Cyber-Security Challenges with SMEs in Developing Economies: Issues of Confidentiality, Integrity & Availability (CIA)

Yeboah-Boateng, Ezer Osei

Publication date:
2013

Document Version
Early version, also known as pre-print

Cyber-Security Challenges with SMEs in Developing Economies:

Issues of Confidentiality, Integrity & Availability (CIA)

Ezer Osei Yeboah-Boateng

Supervised by Reza Tadayoni, Associate Professor

Co-Supervised by Henrik Legind Larsen, Associate Professor

CYBER-SECURITY CHALLENGES With SMEs In DEVELOPING ECONOMIES:

Issues on Confidentiality, Integrity & Availability (CIA)

Ezer Osei Yeboah-Boateng

Supervised by Reza Tadayoni, Associate Professor

Co-Supervised by Henrik Legind Larsen, Associate Professor

This Thesis is submitted to the Aalborg University
for the Degree of Doctor of Philosophy (Ph.D.)
in Information & Communications Technology (ICT)

Department of Electronic Systems, Aalborg University

Center for Communications, Media & Information Technologies (CMI),

Aalborg University, Copenhagen

Submitted in July, 2013.

Dedicated to:

My parents - Papa & Maama, who saw the need to send me to school;

My wife - Dee, who had to make many sacrifices and endure long unending hours of studying;

My only sister - Naomi Sandra, who is probably thinking of following my footsteps;

My children - Elsa, Nana, Erhard & Eion, who had to endure talking to Daddy via Skype.

Acknowledgement

"If I've seen farther than others, it's because I stood on the shoulders of giants."

Sir Isaac Newton

I wish to express sincere appreciation to the center for Communications, Media & Information technologies (CMI) for the immense long-term support and especially to all the diverse comments received during CMI seminars.

Associate Professor Reza Tadayoni deserves a special mention for first having faith in me to accept to supervise my work, and his vast reserve of patience, support and knowledge. I am also grateful for the support and direction from Associate Professor Henrik Larsen, my co-supervisor for keeping me on my toes with fuzzy equations.

Many thanks to my colleagues in the Ph.D. program for being each other's keeper. I am thankful for various supports from Aalborg University, Ghana Technology University College (GTUC), National Communications Authority (NCA), the Ghana Internet Service Providers Association (GISPA), Nigerian Internet Exchange Association, Danish Computer Emergency Response Team (DK-CERT), LimeSurvey web portal, Survey Gizmo web portal, MATLAB and Camo Software - The UnScrambler.

Finally, this thesis would never have been completed without the encouragement and devotion of my family and friends.

ABSTRACT

SMEs today continue to use networks and the Internet as vital business tools. SMEs are utilizing the opportunities offered by advances in ICTs to adopt innovative business operations, to offer user-friendly and competitive products and services, and to develop customer-centric strategies.

While connectivity is indispensable for achieving business success, being connected also implies being exposed to a myriad of cyber-security challenges, such as vulnerabilities which when exploited can violate confidentiality, integrity and availability (CIA) security properties.

As vulnerabilities are exploited by the numerous threats, SMEs are adversely impacted which in some cases may lead to business closure. The extent of cyber-attacks have increased in recent times and experts believe that if nothing is done about it, the severity of future attacks could be greater than what has been observed to date. The pace with which these vulnerabilities are introduced and dealt with is uncertain. This situation has necessitated the need for SMEs to have frequent vulnerability assessment.

This study discussed the perceived uncertainties in cyber-security vulnerabilities and threats, and used fuzzy linguistic variables to represent the real-life business environment decision-making approach to model assessment techniques.

To address the increasing risk to SMEs in developing economies, the traditional risk equation is re-contextualized into a fuzzy risk relational function, with fuzzy arguments of vulnerabilities, threats and asset value, to assist SMEs make better informed decisions.

SMEs were surveyed and strategically interviewed on various cyber-security and business metrics. The elicited experts' opinions were used to model the risk function, using neuro-fuzzy techniques, that combines the human inference style and linguistic expressions of fuzzy systems with the learning and parallel processing capabilities of neural networks to analyze the cyber-security vulnerability assessment (CSVA) model.

The results show that the CSVA model is simple and intuitive, and can be used by SMEs to assess vulnerabilities in their assets and associated threats that confront them. With available sample datasets, the CSVA model was verified and validated using adaptive network-based fuzzy inference system (ANFIS) tests. Fuzzy similarity measures approach was used to rank taxonomies of vulnerabilities and threats, which are benchmarked to assist SMEs to be proactive. Finally, fuzzy cognitive map (FCM) approach is also used to evaluate the existence and possible implications of vulnerabilities amongst SMEs asset disposal policies. It was established that vulnerabilities due to policies or the lack thereof, can have adverse impact on others.

DANSK Resume

SMV'erne i dag fortsætte med at bruge netværk og internettet som afgørende forretningsmæssige værktøjer. SMV'erne udnytter de muligheder, som fremskridt i ikt til at vedtage innovative forretninger, for at tilbyde brugervenlige og konkurrencedygtige produkter og tjenesteydelser, og til at udvikle kunden i centrum strategier.

Mens tilslutning er en forudsætning for at opnå forretningsmæssig succes, er forbundet indebærer også at blive udsat for et utal af cyber-sikkerhedsmæssige udfordringer, såsom sårbarheder, som, når udnyttes kan overtræder fortrolighed, integritet og tilgængelighed (CIA) sikkerhedsmæssige egenskaber.

Da sårbarheder udnyttes af de mange trusler, er SMV'erne negativt påvirket som i nogle tilfælde kan føre til virksomhedslukninger. Omfanget af cyberangreb er steget i den seneste tid, og eksperter mener, at hvis der ikke gøres noget ved det, kan sværhedsgraden af fremtidige angreb være større end hvad der er blevet observeret til dato. Tempoet, hvormed disse sårbarheder indføres og behandles, er usikkert. Denne situation har nødvendiggjort behovet for SMV'er at få hyppig sårbarheden.

Denne undersøgelse drøftede den herskende usikkerhed i cyber-sikkerhedshuller og trusler, og bruges fuzzy sproglige variabler til at repræsentere den virkelige liv erhvervsklima beslutningsproces tilgang til modelvurdering teknikker.

For at løse den voksende risiko for SMV'er i udviklingslande er den traditionelle risiko ligningen igen kontekstualiseret i en fuzzy risiko relationel funktion, med fuzzy argumenter sårbarheder, trusler og indre værdi for at bistå SMV'erne træffe bedre informerede beslutninger.
SMV'er blev undersøgt og strategisk interviewet om forskellige cyber-sikkerhed og business målinger. De fremkaldte eksperters udtalelser blev brugt til at modellere risikoen funktionen, ved hjælp af neuro-fuzzy teknikker, der kombinerer den menneskelige inferens stil og sproglige udtryk for fuzzy systemer med læring og parallelle databehandling af neurale netværk til at analysere cyber-sikkerhedsbrist vurdering (CSVA) model.

Resultaterne viser, at CSVA modellen er enkel og intuitiv, og kan anvendes af SMV'er til at vurdere sårbarheder i deres aktiver og tilhørende trusler, som konfronterer dem. Med tilgængelige prøve datasæt, blev CSVA modellen verificeret og valideret ved anvendelse af adaptiv netbaserede fuzzy inferens-system (ANFIS) tests. Fuzzy lighed foranstaltninger fremgangsmåde blev brugt til at rangere taksonomier af sårbarheder og trusler, som benchmarkes at hjælpe små og mellemstore virksomheder til at være proaktiv. Endelig er fuzzy kognitive kort (FCM) tilgang også anvendes til at vurdere eksistensen og mulige konsekvenser af sårbarheder blandt SMV'er aktiv bortskaffelse politikker. Det blev fastslået, at sårbarheder grund politikker eller mangel på samme, kan have negativ indvirkning på andre.

Table of Contents

List of Figures

List of Tables

Chapter 1 INTRODUCTION

"Dear Small Business Owner:
More small businesses today use networks and the Internet as vital business tools than ever before. While connectivity is indispensable for achieving business success, being more connected also means being more vulnerable to outside threats. Larger companies have security experts at their disposal, but small business owners must make their own decisions about how to secure their networks."[1]
Donald Wilson, President & CEO
Association of Small Business Development Centers (USA) **www.asbdc-us.org**

The above quote can be said to be a synopsis of this thesis. Indeed, more and many more Small and Medium sized enterprises (SMEs)[2] today are utilizing the opportunities offered by recent advances in information and communications technologies (ICTs) as vital business tools than ever before. SMEs are adopting innovative business operations, user-friendly products and services, and customer centric strategies. Unfortunately, a myriad of challenges threaten the SMEs, especially the issues of *confidentiality, integrity and availability (CIA)* vulnerabilities, as those weaknesses are exploited by threat agents. Whenever they are attacked, SMEs are adversely affected by way of loss of revenues, loss of customer confidence, loss of investor confidence, loss of resources, loss of credibility, cost related to dealing with the security breaches, cost of mitigation as well as possible business closure, etc.

Most SMEs operate on a PC and a server network, which store critical company information. To ensure smooth daily operations this information must be both available and secured. In business, confidentiality is to protect the privacy of a business entity, including its critical or sensitive information, and to safeguard intentional or unintentional disclosure. For effective operations, SMEs "*must grant the right access to the right people at the right time*" [1]. There is also the need to prevent the wrong people from gaining access.

As SMEs connect to the Internet and/or correspond with their stakeholders, concerns are raised over some cyber-security challenges associated with Internet patronage. Some of the issues are:

- How do SMEs ensure that the intended recipients have their correspondences intact, safe and at the right time?
- What could possibly go wrong?; and

[1] *"Security Guide for Small Business", Microsoft Corporation, 2005.*
[2] *This research defines SMEs as businesses with less than 10 employees as Micro Enterprises, between 10 and 50 as Small Enterprises, and between 50 to 250 employees as Medium sized enterprises. This definition falls within those applied in Ghana and Nigeria, which are the case studies for this research, and it is also consistent with similar research works in ICT* [29].

- To what extent would these affect the business, if unauthorized persons or entities got their data sheets or pricing strategy?

Risk is perceived to be increasing as technology continues to advance. The threats to information and business assets have increased in sophistication in recent times [2]. A number of techniques could be employed in addressing the concerns raised above or to mitigate the risks.

Traditional risk theory presumes the randomness of cyber-attacks, and estimates risk by probability products. For instance, Gibson [3] defines risk as the probability of threats exploiting vulnerabilities to cause a loss. Accordingly, the loss is a resultant of compromises of business functions and business assets, which in turn, drive business cost up. The probabilistic assumption may lead to risk-free evaluations; situations which can be erroneous and potentially misleading [4].

Another technique, which happens to be the crust of this study, addresses the concerns by bringing out the inherent uncertainties associated with the exploits as well as the susceptibilities. Indeed, this perceived uncertainty and the risk involved with the use of the Internet, be it for business operations or for communications, is the significance of this study.

This study shares the view of Zadeh's possibility theory [5] which espouses that the information needed in human reasoning or decision-making is essentially, possibilistic in nature, rather than probabilistic. The theory also asserts that natural languages or the day-to-day communications are fraught with subjectivity or vagueness. This form of uncertainty, which is intrinsic or inherent in natural languages, is what Zadeh calls fuzziness [6]. Human decision-making is uncertain and cannot be modeled by crisp set, but rather with fuzzy set theory. The utilities of fuzzy set and possibility theories are appropriate for modeling complex, non-linear, linguistic-based everyday decisions. This study seeks to assist SMEs to proactively take decisions aimed at mitigating risks associated with doing business on the cyber-market.

The notion of cyber-risk assessment is complex and has lots of uncertainties. So any strategy or solution to assess cyber-risk with probability is like avoiding risk complexities and uncertainty measures, and instead render the probabilistic risk assessment model "a process that attempts to guess rather than formally predict the future on the basis of statistical evidence" [7].

Even though the probability assessment is said to be based on sound mathematical theory of probability, it undoubtedly uses some subjective and qualitative guesstimates [8]. Shaurette

[8] posited that these qualitative risk values may be appropriately estimated based on rules, such as fuzzy inference rules, that capture the "consensus" opinions of cyber-security experts.

In this study, cyber-risk is seen as the possibility for loss of *confidentiality, integrity and availability* due to a specific threat on a given asset [9]. By definition, cyber-risk is a fuzzy measure of the adverse effects that can result if cyber-security vulnerability is exploited. In other words, any time any cyber-security property is violated, there is the possibility of risk. Typically, cyber-security objective is to deter, prevent, detect, recover from, and respond to threats in cyberspace.

> *Cyber-security is to safeguard the information assets, the information systems and networks that deliver the information, from damage or compromise resulting from failures of confidentiality, integrity and availability.*

This study focuses on the perceived uncertainties in cyber-security vulnerabilities and threats, and uses fuzzy linguistic variables that represent the real world business situational multifaceted decision-making to model mitigation techniques.

Usually, the CIA attributes are used as the benchmark for evaluating most information systems security or information assurance systems. Though, the ITU-T Recommendation X.805 [10] stipulates eight (8) cyber-security attributes, there have been other attempts at presenting alternatives. Zimmerman's [11] *pretty-good-privacy (PGP)*, Dhillon & Backhouse [12] expanded version of the CIA triad with the *RITE* security attributes, and the Parkerian hexad [13] are examples of security initiatives. Nevertheless, the convention has been the application or utilization of the *confidentiality, integrity and availability (CIA)* attributes as the fundamentals of any viable cyber-security endeavor. This study thus concentrates on these three (3) as well.

Confidentiality: implies that stakeholders expect that the privacy of their correspondences, their passwords, phone numbers, and any other information shared during email interactions will be secured. These are examples of *confidentiality*. Thus, *Confidentiality* is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes, either in storage or in transmission.

Integrity: implies that stakeholders expect that content of the emails are not altered and stock counts received are accurate and any attachments downloaded are authentic and complete. These are examples of *integrity*. Thus, *Integrity* is the property that data has not been altered in an unauthorized manner during transmission or storage.

Availability: implies that stakeholders expect to be able to access or send emails and to place orders when convenient for them, and the Internet connection is expected to be functional

without disruption. These are examples of *availability*. Thus, *Availability* is the property that the system has always honored any legitimate requests by authorized principals or entities. *Availability* ensures that information assets are accessible whenever needed. It is an important property since any disruption of service may adversely affect business operations of SMEs.

The cyber-security infrastructure is multifaceted and it includes information technology, procedures and practices, laws and regulations, people and organizations. According to Denning [14] these areas are interrelated and impact each other.

A thorough assessment of these CIA constructs is beset with subjectivity and perceived uncertainties. The issue is how to estimate the cumulative impact on business, should these vulnerabilities be exploited? These uncertain attributes, which are representations of fuzziness, are suitably described by fuzzy functions[3]. For example, *Confidentiality* impact is estimated by taking the possibilities of the occurrence of breaches due to human errors, transmission errors, data storage, data disposal, etc. leading to or due to unauthorized disclosure.

Perfilieva [15] posits that a "fuzzy function is a special fuzzy relation with a generalized property of uniqueness". This notion is alluded to by Zadeh [16] in his extension principle, which espouses that a classical function can be fuzzified. Accordingly, a fuzzy function is interpreted as a fuzzy result or fuzzy functional values [17]. Similarly, a multi-dimensional fuzzy function is formulated by a "fuzzy bunch parameters" [17].

Typically, it is not uncommon for engineers and scientists to use functions to develop the relationships amongst constructs used in modeling problems or solutions of interest [18]. Throughout this study, a format is adopted to represent the vagueness or subjectivity in relationships exhibited by certain key constructs. Caveat! Though the rigorous mathematics in support of these fuzzified functions may not immediately be available, the associated fuzzy manipulations based on the much touted extension principle are utilized. Thus:

Confidentiality (β) is the assurance of data privacy and it's estimated by

$$\beta \square \tilde{F}(\text{human errors, transmission errors, data storage, data disposal}) \quad [1\text{-}1]$$

Integrity (δ) is the assurance of non-alteration and it's estimated by

$$\delta \square \tilde{F}(\text{human errors, transmission errors, software bugs, HD malfunctions, natural disasters}) \quad [1\text{-}2]$$

[3] A function is a mapping, a transformation, an operation or a relation between a set of inputs, usually called arguments, and each element of a given set of outputs, usually called the value(s). Functions are said to be paramount in investigative research [265]. Literature supports a variety of methods for the representation of functions. The commonest ways are either by a formula or an algorithm, which may describe the relationship existing amongst the outcome and the arguments.

Availability (λ) is the proportion of time a system is in functioning condition and it's estimated by

$$\lambda \approx \tilde{F}(\text{destruction, removal, interruption, human errors, natural disasters})^{4} \quad [1\text{-}3]$$

The arguments of the functions in equations [1-1] through [1-3] are deduced from various literatures [3] [19] [20] [21] [22] [10]. The essence of these formulae is to capture all the possible intrinsic information associated with a particular vulnerability.

To ensure business continuity, SMEs require a model that enables them to proactively analyze the various imperative factors critical to the security and business operations. This multifaceted assessment is beset with subjective considerations and uncertainties. This leads the study in pursuing a more holistic risk assessment which is a complete departure from the traditional notion of risk computations based on simplistic probabilities and dependence on overly binary outlook. That is, this study focuses on assessing a system's degree of susceptibility, instead of it simply being judged whether it is secured or not.

The novelty in this study's risk assessment is the modeling of possibilistic fuzzy risk relational function which has the vulnerabilities, threats and asset value as fuzzy arguments. Thus, the traditional risk equation in probability is completely re-introduced in fuzzy sets and possibility theory, as well as adding the impact due to assets value to the equation.

This study takes a holistic view of cyber-risk and alludes to a combined definition of cyber-risk as:

> *"the possibility of the occurrence or realization of a threat, due to compromises of the confidentiality, integrity and availability (CIA) of the system and the associated adverse impact on business."*

It follows that the cyber-risk can be defined mathematically as a fuzzy relational function:

$$Risk_{\text{threat}} \approx \tilde{F}(\text{Threat}_{\text{asset}}, \text{Vulnerability}_{threat}, \text{Asset Value}) \quad [1\text{-}4]$$

where:

- Asset Value is the summation of contributing values from the CIA utilities as evaluated in respect of the urgency for restoring a compromised asset and/or its criticality to the business;
- Vulnerability is a weakness within and around the system that can be exploited by threat agents; and

[4] It must be noted that these functions may have other variables other than those stated above. Each of the variables have been observed and examined in relation to its contribution to cyber-security vulnerabilities on SMEs from the empirical study.

- Threat is the possibility of exploiting the weakness, given the conditions of motivation or intent, capability, opportunity and attractiveness of the asset.

From equation [1-4], the parameters Threat, Vulnerability and Asset Value can either be convoluted if numerical possibility measures are available or the linguistic terms or semantic labels are "convoluted" using approximate reasoning (intuitionistic) with rules [23]. The value of an asset determines its attractiveness, whereas the vulnerability with the asset serves as an opportunity for possible threat exploitation leading to the extent of cyber-risk [24].

It is noteworthy that the contributions of the CIA attributes towards the asset value evaluation or computation are such that, the confidentiality implies the asset's confidentiality or privacy or authentication requirements; the integrity implies the asset's trustworthy or accuracy; and the availability implies the asset's requirement of communications security, continuous functionality or accessibility.

It must also be noted that there are varied contributions from the CIA properties. For example, confidentiality is assessed in respect of vulnerabilities as inherent weaknesses or the susceptibility of the system being assessed, whereas confidentiality utilities are assessed in respect of the asset value; such as the urgency with which a compromise of an asset ought to be restored and/or its criticality to the business.

These are the fundamental assumptions of this study; the research is so designed to elicit the opinions of cyber-security experts of SMEs in developing economies[5].

The ensuing section deals with the key motivation for the study.

Motivation for the Thesis

Cyber-security has become a critical concern in nearly every facet of business lives, creating a demand for comprehensive research and high-level information security expertise.

The motivation of this research is, thus:

- To proactively identify cyber-security vulnerabilities and to come up with a taxonomy (to enlist) of competing options of cyber-security vulnerabilities in the order of most-to-least critical vulnerabilities as a function of how plausible an option is vulnerable; also, to come up with a taxonomy of threat agents that militate against cyber assets in the order of most severe to minor attacks;

[5] Developing economy is defined variously by various development entities for statistical convenience, which has no definite tenets as regards the stage or status of one's economic development [262] [261]; and is an economy which has undeveloped industrial base, low human development index and with a gross national income (GNI) per capita (based on 2011 data) of up to, and including, $12275 [261].

- To develop a model to assist SMEs to safeguard their business assets and effectively mitigate cyber-security vulnerabilities facing the assets; and
- To contribute to the bodies of knowledge in Information Assurance and Information Security analyses and techno-economic business performance.

This research will also aid SMEs in formulating an effective cyber-security and continuity policies. The research findings of this project will contribute to the cyber-security literature on SMEs in developing countries.

1.1. Problem Formulation

As more SMEs today continue to use networks and the Internet as vital business tools, the need for a secure organization cannot be over-emphasized. SMEs are utilizing the opportunities offered by advances in ICT to adopt innovative business operations, to offer user-friendly products and services, to develop customer-centric strategies, and to reach more global clientele and stay competitive through web presence. SMEs facilitate the provisioning of a variety of interactive applications and personalized services, such as e-government, online banking, social platforms, e-commerce interactions, etc.

It is therefore imperative to ensure that these networks are protected against any kind of failures or attacks. Although, interconnectivity is indispensable for achieving business success, being more connected also implies being exposed to a myriad of cyber-security challenges, such as vulnerabilities of confidentiality, integrity and availability (CIA).

As vulnerabilities are exploited by the numerous threats used by threat agents or attacks, SMEs are adversely impacted which in some cases may lead to business closure. The extent of cyber-attacks have increased in recent times and experts believe that if nothing is done about it, the severity of future attacks "could be greater than what has been observed to date" [25].

Threat agents have become innovative and have the capacity to cause harm with catastrophic impact from afar, while equipped "with only a computer and the knowledge needed to identify and exploit vulnerabilities" [26].

Mansoor [27] posits that the dynamic nature of data in the corporate world has rendered the classical approach to ensuring confidentiality, integrity and availability (CIA) "somewhat less relevant". For instance, some challenges arise out of access control for social networking sites or services, sharing of the same ports, e.g. the use of port 80 for YouTube, flash video for conference calls and meetings, as against the traditional usage of port 80 for HTTP services.

A number of serious concerns ought to be addressed. The key questions arising are:

i. *How do SMEs mitigate the impact of cyber-security compromises of Confidentiality, Integrity & Availability against their assets in developing economies?*
ii. *What risks do compromises of the CIA have on business performance and continuity?*

In order to tackle these questions adequately, the following supplementary questions ought to be resolved:

- Are there elaborate policies to deal with cyber-security vulnerabilities or threats?
- Do SMEs have an idea of vulnerabilities or threats due to asset disposal?
- How do SMEs dispose of corporate information? Do they use outside disposal contractors?
- How do SMEs ensure that the intended recipients have their correspondences intact, safe and at the right time?
- To what extent would these affect the business, if unauthorized persons or entities got their data sheets or pricing strategy?

The essence of this study is first to highlight the cyber-security challenges confronting SMEs in developing economies, and to model a framework for safeguarding their assets, to ensure continued optimal business operations, and to participate and compete securely in the ubiquitous cyber-market. To do this, SMEs were surveyed and strategically interviewed on various cyber-security and business metrics. The key factors which influence vulnerabilities have been identified, including human centric issues and perceived uncertainties of vulnerability attributes. Empirical reasons and underlying causes associated with the deployment of cyber-security solutions are examined.

The following section deals with the synopsis of literature and related works used as the basis of the study.

1.2. State-of-the-Art

This section gives concise overview of the key theoretical underpins used for this study. Mainly the scope of SMEs as target sample population is established as well as its significance. Then, the essential elements of cyber-security and associated risk parameters are stipulated. The fundamental theories of possibility, fuzzy sets and neural networks are briefly introduced. This section concludes with synthesizing the building blocks in a model.

1.2.1. Small & Medium sized Enterprises (SMEs)

Small and medium-sized enterprises (SMEs) consist of varied businesses usually operating in the service, trade, agri-business, micro-finance and manufacturing sectors. SMEs may be innovative and entrepreneurial, and usually aspire to grow; though, some stagnate and remain family owned. The subject of an investigation under this study is the small-and-medium-sized enterprises (SMEs). Who or what are SMEs? It may seem very simple and easy question, but most literatures reviewed have divergent views. There is no consensus on its definition; no single, uniformly accepted definition of small-and-medium sized enterprises (SMEs) [28]. Various definitions exist whereby SMEs are classified by various parameters, including net worth, profitability, sales revenue, turnover, number of people employed, etc.

Depending upon the jurisdiction one operates in and for what purpose one intends, SMEs are defined with specific motivations. The lack of a unified definition presents a significant practical challenge; it seriously hampers the prospects of generalization of some research findings as the scope of discussions may need to be clearly defined to avoid any ambiguities.

This study adopts the following definition, that SMEs are businesses with less than 10 employees as Micro Enterprises, between 10 and 50 as a Small Enterprise, and between 50 to 250 employees as a Medium sized Enterprise. This definition falls within those applied in Ghana and Nigeria, which are the case studies for this research, and it is also consistent with similar research works in ICT [29].

Having defined who SMEs are, the next object is to identify SMEs who use the Internet for business communications and/or operations.

SMEs have been touted as the engine of growth for developing economies. Generally, SMEs are estimated to employ about 22% of the population in developing economies [30] [31]. The SME sector in Ghana (as of 2010) accounts for about 92% of all businesses and contributes about 70% of GDP [32] [33] [34]. Similarly, the Federal Office of Statistics (as captured in [35]) indicated that 97% of all businesses in Nigeria employ less than 100 employees, and the SME is defined under the umbrella term of less than 250 employees.

Whereas cyber-security vulnerabilities pose serious concerns to all businesses, SMEs are usually hardest hit victims and find it very difficult to recover after a cyber-attack. The issues of cyber-security metrics and dimensions are explored in details in subsequent sections.

1.2.2. Essential Elements of Cyber-security

As indicated in the preamble, the ITU-T Recommendation X.805 [10] stipulates eight (8) cyber-security dimensions. In spite of attempts by some authorities to propose alternatives, universally literature accepts the classical cyber-security triad of *confidentiality, integrity and availability (CIA)* as the basic building blocks of any good cyber-security initiative.

This study thus focuses on these three (3) and defines cyber-security as the ability to safeguard computers and network systems and the *confidentiality, integrity and availability* of the data they contain.

The objective of this study is to highlight the challenges confronting SMEs and the need to mitigate the associated risks in order to build a secure business that would ensure business continuity.

It is essential to devise cyber-security solutions or mechanisms that would address the needs of SMEs. For instance, encryption and message authentication mechanisms usually work on the assumption of pre-existing relationships between senders and receivers. But in practice, end-users communicate with people they never met, or buy products online from merchants they have never met. In essence, to encrypt or authenticate all messages would have rendered communications impossible. According to Walker [20], "an open, unauthenticated, risky channel" is however used in establishing communication channels or sessions; cryptography could, at best ensure confidentiality, integrity and non-repudiation between entities which have pre-existing relationships. The communicating entities involved are able to instantiate a session by exercising a relationship to effect communication. This session establishment synchronizes the entities to ensure that appropriate entity credential are exchanged to provide mutual assurance of non-repudiation and confidentiality [20].

As new technologies and services become available, the original uses of local area networks (LANs) and Intranets have also changed. Today's Intranet is said to be a combined web portal and public dashboard. Numerous challenges beg for resolution as well as a balance needed for end-users, utilization of resources, and the policies facilitating their interactions.

Mansoor (2009) posits that the weakest link in security is the user training and awareness. He advocates that new recruits must be given all security policies and be made to sign off before being given access to the network.

The following section deals with the risk parameters.

1.2.3. Risk Parameters

A fundamental assumption being espoused in this study is the fuzzy risk relational function. The function arguments are the vulnerabilities, threats, and asset value. In this sub-section, these risk parameters are briefly reviewed.

1.2.3.1. Assets Value

Generally, an asset is said to be any item of economic value that usually is convertible to cash, owned by an entity, such as an individual, an organization or a society. Ozier [36] defines cyber- assets[6] as an embodiment of an organization needed to conduct or transact business. He distinguished between tangible and intangible cyber-assets. He associated the intangibles as "true" information assets, which include information itself, data, corporate image, goodwill and reputation, intellectual property, services, software programs and applications, corporate emails, wikis, user passwords, regulatory mandated personally identifiable health information. Whereas, tangibles are seen as information supportive and/or enablers, which include printouts, end-users, hardware, storage media, equipment, removable media, USB keys, PCs, laptops, PDAs, web-servers, networking equipment, DVR security cameras, employees' physical access cards, etc.

All assets should be accounted for within the organization, and because of the cyber-security implications, each asset should have an assignee or custodian who is responsible for its security and maintenance. A key question is, "does the SME consider computer systems, software applications, and operating systems as critical assets?"

SMEs must classify assets based on its value, criticality, urgency, sensitivity, governing laws and regulation, business requirements or objectives to the SME, and to provide a commensurate level of protection. These assets or information attributes are necessary as well as the associated impacts if the information is compromised (e.g. lost, stolen, corrupted, disrupted, altered, etc.). Note that, some information or assets may need re-classification after a period of time. A number of factors influence the type and strength of the security measures put in place to protect the assets. They include asset value, the extent and severity of the consequences, the attractiveness of the assets, the perceived threat agents, etc.

For the purposes of this study, a cyber-asset is meant to be any information, data, programs, applications, information processing resources used for media or storage, processes and

[6] Cyber-security assets are sometimes referred to as information and communications technology (ICT) assets, and loosely as information assets. Unless otherwise specified, the use of "information assets" shall encompass all cyber-security or ICT assets.

transmission of the information, and the value at risk that could compromise the confidentiality, integrity and availability of the assets.

Assets are targets of various threats and threat agents, and the goal is to protect the assets from the threats [21].

1.2.3.2. Vulnerabilities

ISO 27005 [37] defines Vulnerability as: "a weakness of an asset or group of assets that can be exploited by one or more threats; where an asset is anything that can have value to the organization, its business operations and their continuity, including information resources that support the organization's mission".

Generally, cyber-security vulnerabilities are weaknesses in and around the systems, networks, infrastructures, applications and processes. Concisely, vulnerabilities are the weaknesses inherent within the system exploited to compromise the confidentiality, integrity and availability (CIA) properties of the system. They are categorized into technical, human, physical, operational and business vulnerabilities [38].

This study takes a holistic view at vulnerabilities by expressing vulnerabilities into fuzzy set of attributes, in order to address all necessary and possible attributes of cyber-security vulnerabilities, rather than the often "overly binary" outlook, whereby something is either susceptible (or vulnerable) or not susceptible (or not vulnerable). For instance, the study evaluates the expert opinions on vulnerabilities by metrics using the quintuple {Extremely-Vulnerable, Highly-Vulnerable, Vulnerable, Slightly-Vulnerable, Not-Vulnerable}.

Vulnerability attributes are defined based on type, source and severity [39] and they are taken into consideration in the design of the empirical study.

1.2.3.3. Threats

A *threat* is any event, condition, or circumstance that could potentially cause harm, loss, damage, or compromise, or pose risk to a cyber-asset. For purposes of this research, threats can be categorized as events that can affect the *confidentiality, integrity, or availability* of SME assets.

Whenever cyber-security vulnerability in a system is exploited, a threat is said to be realized, and thus the system is said to be under cyber-attack. The entity that facilitated or caused the attack is known as a threat agent or an attacker. Some threat agents are human, such as end-users, whose actions may be deliberate or intentional; or whose actions may be accidental or unintentional, may emanate from internal or external sources to the system; due to system

problems, such as hardware failures, software failures, failures of related systems, malicious codes like worms, viruses and Trojan horse; and other environmental problems, such as power outages, natural disasters, etc.

The empirical study was designed taking into consideration the vagueness of the threats [4], threat agent attributes of motivation, capability and opportunity [40] [41], their classification based on type, source and likelihood [39] and the relative impact upon realization.

The study employs a number of threat assessment techniques to evaluate the possibility of an attack against an asset or group of assets [42]. The assessment identifies known and potential threat agents, appraises their threat attributes and evaluates the possibility of maturity and criticality or attractiveness of an asset to the threat agent.

Evaluation of the possibility of an attack is not necessarily intuitive; it is even made difficult by the fact that there often is not enough data available to make a statistical inference on the possibility of an attack. It may be impractical to measure the possibilities of all possible vulnerability attributes and their severity. Usually, experienced analysts who can make educated guesses on the possibility are elicited for their expert opinions.

1.2.3.4. Risk

A number of studies have defined risk in a number of ways. McEachem [43] defined cyber-risk with respect to e-Commerce as the possibility of losses due to compromises of confidentiality, integrity and availability of the e-Commerce systems and the data they contain.

Some traditional risk evaluations are based on accounting principles such as: cost-benefit analysis, return on investment, and total cost of ownership (TCO). The evaluations are usually based on estimates of risk as the likelihood of a threat realized or a successful attack against the system or an asset. These notions presume the randomness of attacks as events and the risk equations are usually given by a probability product.

This approach can lead to situations where there are no risks to valuable ICT assets; a situation which can be erroneous and potentially misleading [4]. The US department of Homeland Security (DHS) recognizes that risk assessment is fraught with lots of uncertainties. In view of that, the DHS defined risk as follows:

> "*Risk is an expression of the likelihood that a defined threat will target and successfully exploit a specific vulnerability of an asset and cause a given set of consequences"* [4].

The DHS [4] posits that the risk of security related assets is best estimated qualitatively. It recommends the use of consensus expert opinions or judgment on the possibilities and possible consequences upon realization of the threats.

Katsikas [7] assets risk on the basis of assets value, the severity and likelihood of threats maturing, the nature and extent of vulnerabilities and its likelihood of exploitation, and the impact and likelihood of a threat succeeding.

Katsikas [7] posits that the risk management model based on probabilistic computations, alone, is simplistic. He asserts that the avoidance of risk complexities and uncertainty measures, render the probabilistic risk management model "a process that attempts to guess rather than formally predict the future on the basis of statistical evidence".

This study takes a holistic view of cyber-risk and alludes to a combined definition of cyber-risk as:

> *"the possibility of the occurrence or realization of a threat, due to compromises of the confidentiality, integrity and availability (CIA) of the system and the associated adverse impact on business."*

The study employs fuzzy set theoretic techniques to evaluate the cyber-risk. The application of fuzzy logic is highly subjective and its treatment takes into account the imprecise and vagueness of cyber-risk metrics [44].

Shaurette [8] posits that though probabilistic risk evaluation "is based on well-established mathematical theory", its ratings are fraught with subjective guesstimates. He asserted that qualitative risk values may be estimated based on rules, such as fuzzy inference rules, that capture the consolidated advice of cyber-security experts. Practically, it may be difficult to estimate the probable losses due to morale, credibility, stakeholder confidence and corporate image, etc.

The impact of a breach or cyber-risk is given by the fuzzy risk relational function in equation [1-4] above.

It is noted that in accounting for the traditional notion of risk, the impact element is covered by the asset value, and the likelihood probability is compensated for within both the threat and vulnerability values [45].

This implies that, for a higher asset value, a higher vulnerability value, and/or a higher threat value lead to a higher risk value [24]. To assess cyber-risks, the value of each asset is evaluated for the importance of the asset (i.e. its urgency and criticality), and vulnerabilities and threats which may cause damage or loss of asset values are also examined. An asset may have more

than one vulnerability. Vulnerabilities may be exploitable in multiple ways through multiple forms of applicable threats. It must be noted that there are vulnerabilities without risk; i.e. when the affected asset has no value.

The succeeding sub-section deals with the theories used in the study.

1.2.4. Theories

This section gives an overview of the key theoretical underpins or frameworks used for the study to model the risk parameters. The section examines the possibility theory or possibility of occurrence, fuzzy set theory and neural network theory.

1.2.4.1. Possibility Theory

Possibility theory was introduced by Zadeh [5] as an uncertainty theory and relating to fuzzy sets theory with the concept of possibility distribution with fuzzy restrictions on the assigned values [5].

Zadeh's [5] seminal work on the possibility theory argued that the fuzziness expressed in natural languages is "possibilistic rather than probabilistic in nature". He posited that an analytical metric concerned with capturing the essence of information, and its intrinsic attributes, should be by means of possibility measures rather than probability measures.

Zadeh [5] underscores the important fact of possibility distribution being distinct from probability distribution. That is, an existence of a possibility of occurrence does not necessarily imply a similar measure of probability of occurrence.

This study utilizes the possibility measures to evaluate its intrinsic metrics of threat agents attacking cyber assets and exploiting existing vulnerabilities, for example. The possibility theory is used in the analysis of uncertainty in fuzziness, rather than the uncertainty in randomness, which is associated with probability [46].

1.2.4.2. Fuzzy Sets Theory

A fuzzy set is a class of elements with a continuum in the domain [0,1] of grades of membership, which is characterized by its characteristic (or membership) function [6] [5]. Fuzzy sets are basically functions that map a value that might possibly be a member of the set to a number between zero and one indicating its actual degree of membership [47]. A membership function μ_A in a fuzzy set A maps real numbers in universal set X to [0,1], such that $\mu_A : X \rightarrow [0,1]$. In essence, each element in the fuzzy set is mapped onto a grade of membership between zero and one (inclusive i.e. [0,1]). A degree of zero means that the value

is not in the set and a degree of one means that the value is completely representative of the set.

Fuzzy sets can practically and quantitatively represent vague concepts.

Human knowledge is generally fuzzy. It is usually expressed in linguistic terms such as "young", "secured", "vulnerable" – which are fuzzy in nature. Fuzzy logic is thought of as a bridge over the precision-based classical crisp logic and the imprecision of the real world and its human reasoning [5].

This study deals with non-numerical quantities, for instance *"Integrity"*, which cannot be measured against a numerical scale. An example of such a universe could be the quintuples {Very-Low, Low, High, Very-High, Extra-High}. The notion of fuzzy sets is highly intuitive and transparent as it captures the essence in which a real world is perceived and described [42]. The fuzzy logic theory is just a prolongation of traditional logic where partial set membership could exist, rule conditions could be satisfied partially, and system outputs are calculated by interpolation [6].

Fuzzy logic is an attempt to represent the human reasoning and to approximate its qualitative linguistic and subjective nature. In order to apply fuzzy logic to model real world problems, the knowledge must be structured. That is, the subjectivity inherent in the knowledge would be "normalized" or made objective. By so doing, the fuzzy linguistic terms are treated with the same standard treatment. The linguistic terms are constructed to form fuzzy sets. Unlike classical crisp sets, fuzzy sets have a degree of belonging or grade of membership in the bounded set of real numbers [0,1].

The input–output mapping of such a fuzzy model is integrated into a system as both quantitative mapping and qualitative linguistic rules. This methodological analysis is vague or ill-defined.

Fuzzy system modeling involves the following four stages; namely, definition of basic building blocks of linguistic variables, fuzzification, fuzzy inference and defuzzification.

A typical fuzzy system is premised on the following basic concepts. It defines basic building blocks of linguistic variables and terms. For example, in the statements "the router is vulnerable" and "the vulnerability is high". Here a fuzzy linguistic variable "Vulnerable" and a linguistic term "high", from the fuzzy set {very low, low, medium, high, very high} are involved.

One key issue with fuzzy set theory is how to define the appropriate membership functions of the fuzzy sets. In practice, a number of approaches are used including, using definitions by the

model expert, using data from the system to be modeled to generate them, or by trial-and-error.

Fuzzification is the process of applying membership functions and numeric values to the linguistic variables and terms, respectively. For each term of an input linguistic variable, a membership value $\mu_{A_{ij}}(x)$ is given.

The next stage is the application of the fuzzy rule bases. This process is commonly referred to as the Fuzzy Inference engine. The fuzzy system is built from formulating fuzzy rule base in the form:

IF (Antecedent) THEN (Consequent).

Here conclusions are drawn from existing facts and available knowledge [48]. The inference engine examines the rules based on a predetermined order. It uses the available knowledge from antecedents to determine the consequent statements. The process is iterative and it goes on until predetermined output values or variables are known.

Kirschfink & Lieven [49] categorized the inference process into three (3); namely *aggregation, implication and accumulation*.

Defuzzification is the process of mapping the resulting fuzzy output set into a crisp set. The results of the inference process are converted from fuzzy linguistic variables or terms into crisp values, for meaningful analysis or interpretation.

The fuzzy output set consists of linguistic variables, which are either the resulting intersection or union of all the linguistic terms. This fuzzy set of outputs is also characterized by a membership function that is computed from the possible membership functions of the various linguistic terms.

1.2.4.3. Neural Networks Theory

The basic tenet of the neural network theory is the ability of the artificial intelligence system unit called the neuron to mimic the learning abilities of humans.

Neural networks are powerful tools for modeling problems for which the explicit form of the relationships among certain variables are not known; for example, the cyber-risk model which is complex and non-linear in nature. Artificial neural networks are generalized models of human cognition, based on the following assumptions, that:

- Information processing occurs at many simple elements called Neurons;

- Signals are passed between neurons over connection links;
- Each connection link has an associated multiplicative weight, which, in a typical neural network, multiplies the signal transmitted to reproduce synaptic effect;
- Each neuron applies an activation function (usually non-linear) to its net input (sum of weighted input signals) to determine its output signals.

It is usually very difficult to write programs to solve or model such uncertainties associated with cyber-security. Especially when most of the parameters are unknown, the rules governing the system are uncertain, and the program itself may be complicated.

Instead of writing a program by hand for each specific task of the algorithm, lots of samples that specify the correct output for a given input are collected and are used by the artificial neural network to learn and model the system of interest.

The model built by the neural network may look very different from a typical hand-written program, as it is usually a black box. The black box consists of neurons with activation functions and weighted inputs. The weights are initialized at the start of the learning process and are updated during the training sessions, until an optimal solution is found.

If the model learns well, it is able to solve new problems as well as the ones that were used for the training. Also, the model has adaptive capabilities to adjust to new datasets by training on those new sets.

The neural network saves time and resources with the massive computational ability that would have been needed to model the problem.

The detailed technical literature is presented in chapters 3 and 5 of this thesis.

1.2.4.4. Neuro-Fuzzy Systems

Generally, fuzzy logic can encode the experts' knowledge or opinions elicited from the empirical study by directly applying the rules with linguistic variables. However, it takes a lot of time to design and tune the membership functions that quantitatively represent these linguistic variables.

Neural networks, on the other hand, have learning techniques that can automate these processes and subsequently reduce development time and cost while improving performance. So by employing a hybrid system of Neuro-fuzzy methodologies to model the system, the parallel processing and learning abilities of neural networks are fused with the fuzzy linguistic and human reasoning of fuzzy systems, for easy interpretation and explanation of the system output. Integrating these two methodologies in modeling can lead to better analysis that take

advantage of the strengths of each methodology and at the same time overcome some of the limitations of the individual technique.

The Neuro-fuzzy model is trained with data sets in the form of input-output mappings, and a specification of the rules deduced from the expert knowledge and/or system generated rules from the datasets, and predefined membership functions of the linguistic variables.

1.2.5. Modeling

The world is full of uncertainties, the information obtained from the environment, the notions used and the data resulting from observation or measurement are, in general, vague and imprecise [50]. Thus, formal description of the real world problems or some aspects of it, is in essence, only an approximation and an idealization of the actual state.

In the modeling processes, concepts are idealized to remove complicated details that are not very essential in understanding the main principles. This abstraction allows for the application of mathematics and to make analogies to other familiar systems.

Since it is sometimes impossible to develop a mathematical model which adequately addresses all aspects of the system, researchers may use over-simplified assumptions which may lead to inappropriate decision making [51] [52].

Cao [53] recommends the use of a fuzzy input-output model, which takes into consideration all factors of complexity, imprecision and vagueness to "accurately and scientifically" model the system.

Cyber-security modeling has the same connotations as in the fields of engineering and science. Modeling the cyber-security vulnerabilities is basically an abstraction used for the consideration of a problem of interest, in this case *Confidentiality, Integrity & Availability (CIA)* compromises in SMEs systems. The model has generally been considered as an aid in analyzing the cyber-security properties of interest. Bell [54] posits that a cyber-security model should have the following characteristics:

- descriptive capability – the ability to describe the situation of interest;
- general mechanism – the analytical tools to aid in the analysis of secure systems;
- specific solutions – the direct synthesis and analysis aid in the consideration of specific systems.

The choice of method is usually dictated by the dataset available for the model. If the data are pairs of numbers, neural method may be most suitable, and if the data are rules, the fuzzy methods may be most suitable. This study has both data pairs and rules deduced from experts'

opinions, which makes it appropriate to the use a hybrid Neuro-fuzzy technique. The neural method provides learning capability, whereas the fuzzy method provides flexible linguistic interpretation [55].

1.3. Overview of Methodologies

In view of the complexities and uncertainties in cyber-security metrics, the study sets off with an extensive literature review and designed a survey questionnaire philosophy which was submitted to five (5) cyber-security practitioners for review and comments. Based on their comments and advice, a pre-test survey was designed and administered to those experts, again for the critique. The actual full scale survey was then launched and administered using LimeSurvey Online facilities (www.limesurvey.com). This approach was adopted in order to target most SMEs in Ghana and Nigeria; and in view of the challenges associated with physically distributing questionnaires in the case-study countries. *To ensure credible results, a cookie was setup in the online survey program to prevent repeated participation.*

The study administered objective-based questionnaire to security functionaries and chief-level (C-level) officers of about 500 SMEs in Ghana and Nigeria. Email messages were sent out to the target population with a preamble and a hypertext link to the online survey website. ICT-based SMEs, financial organizations and government agencies were targeted, and they were selected by a simple random sampling. For instance, the lists of the Ghana ISPs Association, the Nigerian Internet Exchange Association and professional IT experts in Ghana and Nigeria were used. Based on the responses, about 20 cyber-security experts were identified, interviewed and opinions solicited for estimation of the level of impact or risks on the SMEs (via web-based online survey facility www.surveygizmo.com).

Ayyub [18] defines an expert as "a very skillful person who [has] had much training and has knowledge in a specialized field". The expert opinions elicited were appropriately aggregated to estimate the Impact of Vulnerabilities on the SMEs. The techniques of fuzzy set theory [6], including fuzzy similarity measures, were applied on the experts' opinions which are linguistic variables and fuzzy numbers.

First, the linguistic variables were used to represent the relative importance of the experts' opinions and the perceived degree of confidence on each expert as seen by the researcher. Then, the linguistic variables were represented by fuzzy numbers for arithmetic computations. Moon & Kang [56] posit that the primary reason for employing "expert judgments in uncertainty analysis is to assist in estimating the possible values for an uncertain parameter and properly representing the uncertainties associated with it".

1.3.1. Research Methods

Typical research methods involve drawing conclusions, or making inferences about something that has not been observed or measured on the basis of those parameters that have been observed or measured. Most cyber-security endeavors lack historical data or it is difficult to measure security posture metrics of a live system. So by inferential statistics, for example, one can generalize from a sample to a population of interest from which the sample was taken.

To use data to generalize findings, into areas for which there are no data, or to predict an outcome based on a limited data set, requires different techniques and analytical methods. The essence of this study is to model a framework for cyber-security vulnerability assessment based on the empirical data collected.

The model is a relationship among vulnerabilities, threats and the resulting effects of risk or impact on SMEs. Using user-defined fuzzy variables, a number of fuzzy rules were inferred from expert knowledge and empirical data to model the system behavior with easily described linguistic expressions. The input-output datasets are expert knowledge or expert opinions collated from the empirical study on SMEs in developing economies.

The model was evaluated through verification and validation. The out-of-sample accuracy measurement principle is applied to split the data sets, randomly, into 75 – 25% for training and testing data sets respectively. The training data were used for the construction of the model, whilst the testing data were used to ascertain the generalizability or the performance of the model. The purpose of the learning process is to find the set of weights that produces an output which closely matches the actual output. The resultant fuzzy sets are helpful for interpretation and emphasize the user-centric nature of the model.

1.3.2. Research Approach

A key challenge with designing any fuzzy model is to appropriately identify the variables that are suitable to describe the system parameters and represent the extent of fuzziness in the linguistic variables. Structural identification in fuzzy based modeling is the process of determining the variables and membership functions (MFs) used to describe the system abstraction of interest. This could be carried out purely based on expert's knowledge, be it an internal expert (the researcher, in this case) or an external expert whose knowledge or judgment is usually elicited.

Costa Branco et al [57] posit that "if the acquired information is wrong or not enough, the model will be bad." They suggested complementing expert's knowledge with a "more objective knowledge using available" empirical data collected for the system of interest.

There are a number of methods for pre-processing data and preparing them for further analysis. This study uses the Principal Component Analysis (PCA) statistical method from the UnScrambler X.10.1. The PCA method was selected for its simplicity, ease of use and repeatability. The PCA process confirms the latent variables within the dataset as perceived by the researcher. The number of MFs and their positioning are guesstimated by the researcher's own insight and expertise.

The general approach of fuzzy modeling was as adapted from [58] as follows:

i. Define the variables of relevance, interest or importance; e.g. Confidentiality, Integrity & Availability, Threat Agents as Input variables; and Risk Impact as the Output variable.
ii. Define the linguistic terms; e.g. {very low, low, medium, high, very high} or {not vulnerable, slightly vulnerable, vulnerable, very vulnerable, extremely vulnerable}.
iii. Determine the membership functions (MFs) of the linguistic terms and the positions of the tuples; e.g. trapezoidal MFs for say "very low" as [0 0 1 2] or "very high" as [8 9.5 10 10]; and triangular MFs for say "low" as [1 2.5 4] or "high" as [6 7.5 9]; for all MFs range of [0 10].
iv. Decide on the fuzzy Rules; e.g. "IF Confidentiality is LOW, AND Integrity is VERY LOW, AND Availability is MEDIUM, THEN Risk Impact is HIGH".
v. Determine the fuzzy model performance by loading it with test data to verify that the system produces the expected output.

Based on the expert knowledge, the IF-THEN rules for the fuzzy inference system (FIS) are defined. Theoretically, the total number of possible outcomes from the rules is set by the multiplication of all input membership functions; in this case of 5 MFs for 4 variables, the possible outcomes will be $5^4 = 625$ possible rules. In practice, one would either use system generated rules or apply the expert rules (which are usually less).

Once the rules are established, the training data sets are loaded into the ANFIS, with appropriately selected optimization algorithms (e.g. back-propagation and/or hybrid methods), and a pre-set number of epochs to run.

First, the training data set is used, together with the fuzzy inference rules, for the construction of the model, until an optimized error level is reached. Typically, the system "learns" iteratively during the training session by finding the set of weights that produces an output which closely matches the actual output.

Then, the test data set is used to validate the generalizability or the performance of the model. If the model produces a similar output, then the system is said to have been validated, and the

model of interest is thus built. Otherwise, the tuning and testing iterations will go on until a desired result is achieved.

Generally there are a couple of fundamental categories of fuzzy inference systems (FIS), namely, Mamdani FIS and the Takagi-Sugeno-Kang (TSK) or as it is commonly known as Sugeno FIS [59] [60] [61].

The Mamdani FIS was proposed by Mamdani and Assilian in 1975 [59]. It is depicted by both fuzzy inputs and fuzzy output(s). As in most fuzzy inference systems, the crisp input is fuzzified as a set of linguistic variables. The fuzzy inference engine processes the fuzzified variables using related fuzzy IF-THEN rules and draws fuzzy conclusions. These are subsequently defuzzified and transformed on to crisp value(s) as output(s).

Alternatively, the Sugeno FIS, that was first initiated by Takagi and Sugeno in 1985 [61], but later fine-tuned by Sugeno and Kang in 1988 [60], only has fuzzy inputs, but actually provides crisp output, either as a constant or a linear relation. Accordingly, the same fuzzification is actually performed through the inference engine and then a crisp output is provided with no need for defuzzification.

It must be noted that the problem at hand is designed as a Mamdani fuzzy inference system (FIS). However, the MATLAB ANFIS toolbox is limited by processing only Sugeno FIS or system generated from data sets. Thus, the MATLAB command of "*mam2sug*" is used to transform the Mamdani rule-based inference into Sugeno FIS before loading onto the ANFIS.

The detailed texts on the methodologies are covered in chapters 3, 5 & 6.

1.4. Empirical Data & Analysis

This section deals with the empirical data, its analysis and findings which culminate into the key research objective of building a cyber-security vulnerability assessment (CSVA) model and enlisting taxonomies of vulnerabilities and threats.

This study seeks to underscore the cyber-security challenges confronting SMEs in developing economies, and to introduce a mechanism for safeguarding cyber assets, with the view to ensuring continuous optimal business operations, and to enable SMEs participate and compete securely in the ubiquitous cyber-market.

To do this, SMEs were surveyed and strategically interviewed on various cyber-security and business metrics. The key factors which influence vulnerabilities have been identified, including human centric issues and perceived uncertainties of vulnerability attributes. Empirical reasons and underlying causes associated with the deployment of cyber-security solutions are examined.

There are 89 respondents from the main empirical study, which have employees within the 250 limit in accordance with the study's adopted SME definition. So the sample size of 89 is the dataset that is processed for further analysis.

The dataset from the study is one of multivariate data type, having 27 vulnerability metrics, 12 threat metrics and 1 for asset value (business impact or risk). Besides, there are other metrics for business profiling in respect of products and/or services engaged in, as well as perceived annual incident losses, perceived incidents of intrusion, dedicated security positions, existence of security policies and compliance with regulations, etc.

Similarly, the strategic interviews (follow-up survey) have 14 respondents. All 14 responses were within the scope of the study and are evaluated under expert opinion elicitation and fuzzy multi-attribute decision-making (MADM).

The multivariate dataset is pre-processed by principal component analysis (PCA) to ascertain the various correlations, and the dataset is coded into numerals (i.e. 1 through 5), depending upon the variable and its fuzzy linguistic terms at play.

The metrics were structured in a manner such that the selection of a linguistic term to a particular metric precludes other terms in that metric from being selected. It is noted that the linguistic terms and coded values were assigned in a mutually exclusive manner, such that each answer of a sample respondent is appropriately placed into a class or category of fuzzy linguistic terms.

This coding approach prepares and simplifies the data for further analysis with minimal errors, especially as regards missing data. It is noted that though the PCA process identifies and deletes the missing data and outliers (if any), the entire dataset is however used in the further analysis for building of the Neuro-fuzzy model and other statistics. This is in accordance with Meyers et al [62], who posited that when samples with the missing values and outliers are "deleted" from the data set during preprocessing, the remaining data set is actually a sub-sample which in turn affects the generalization to the population.

In any research similar to this, there are voluminous datasets that are collected from the empirical study. There is therefore the need to classify the data into various homogeneous categories for further and meaningful analysis. The obvious classifications are those of the vulnerabilities, threats, asset values and/or business impact groupings, besides the general ones for business profiling, descriptive characteristics and statistics analysis.

Just after data coding and classification, the computation or estimation of the cumulative impacts of vulnerabilities and threats follow, as per the study's assumptions. Fuzzy triangular

mean or fuzzy arithmetic mean [63] [64] are used to aggregate the various opinions for each of the categories.

The datasets resulting from the aggregation are appropriately referenced in the appendices, as they are too elaborate for the main body of this thesis.

The highlights of the key results deducted from this study are enumerated herewith:

- The cyber-security vulnerability assessment (CSVA) model is built with adaptive Neuro-fuzzy inference system (ANFIS) based on MATLAB toolbox;
- The taxonomies of vulnerabilities and threats using fuzzy similarity measures for multi-attribute decision-making (MADM) techniques; and
- The fuzzy cognitive maps (FCMs) evaluation of ICT asset disposal policies and associated vulnerabilities.

The ensuing section presents the summary of the key contributions to the study.

1.5. Contributions

This section summarizes the contributions made in this study. This study contributes to the cyber-security, information assurance and techno-economics bodies of knowledge through empirically based characterization of the risk assessment and information assurance literature. The study re-contextualizes the risk formula using a cyber-security vulnerability assessment model.

The thematic problem being addressed in this study has been "how could SMEs, in developing economies, mitigate the impact of cyber-security exposures or compromises that may result from weaknesses in their assets?"

The use of ICT resources and the Internet, in general, for business communications and operations, has undoubtedly come to stay. Consequent to these innovations, are the myriad of cyber-security challenges that threaten the SMEs and their survivability. If nothing is done, these weaknesses shall be exploited by threat agents. This adversely impacts on SMEs by way of loss of revenues, loss of customer and investor confidence, loss of resources, loss of credibility, cost related to dealing with the security breaches, cost of mitigation as well as possible business closure, etc.

This study, cognizance of the SMEs in developing economies and their budget needs, proposes a cyber-security vulnerability assessment (CSVA) model which takes into account all intrinsic elements and perceived uncertainties associated with risk metrics. The CSVA model is simple

to use, intuitive and requires not a huge budget to apply, as amply illustrated by the example in section 6.3.4. – Model Significance & Applications.

Associated with and paramount to the development of the CSVA model is the fuzzy risk relational function (c.f. equation [1-4]) which has the vulnerabilities, threats and asset value as fuzzy arguments. The traditional risk equation in probability has been completely re-contextualized in fuzzy set theory, as well as adding the impact due to assets value to the equation.

It must be noted that the range of possible threats is almost unlimited. Also, computer systems or ICT resources have numerous vulnerabilities, though not all of them are exploited. Typically, vulnerabilities are inherent in the assets, possibly due to systemic weaknesses, such as product or design weaknesses, incorrectly configured systems, weak passwords, or web site weakness that may enable a visitor to access an unauthorized file, etc.

This study also provides a set of taxonomies of vulnerabilities (as perceived as inherent weaknesses within the assets enlisted) and threats confronting SMEs in developing economies.

The taxonomies of vulnerabilities and threats are as listed below in the order of most critical to the least:

i. {DNS servers > Databases > Email servers > Core switches > Routers > Web servers}
ii. {Natural disasters > Poor authentication > Viruses (Malwares) > Hacking > No Backup > Spywares (Adwares) > Power failure > Un-scanned attachments > Spam > Social engineering}

The taxonomies define sets of vulnerabilities and threats organized in the order of most susceptible to least ICT assets, for the vulnerabilities, and from the most likely or critical to the less likely or minor for the threats. The taxonomies provide a benchmark of cyber-security challenges by which SMEs can assess risks in their systems and networks.

This benchmark offers a common platform about the SMEs assets importance or criticality labels that ought to be appropriately safeguarded.

It must be noted that accurately identifying critical assets can assist with proactive prevention and detection strategies that eventually mitigates the susceptibility of the vulnerability.

Similarly, the threats' taxonomy provides panoramic views of the extent and capability of threats militating against SME assets and resources. It can also assist in the appropriate determination and formulation of mitigation strategies and policies for the SMEs.

Finally, a simple fuzzy cognitive map (FCM) approach used to evaluate cyber-security vulnerabilities with SMEs is also a tool that requires neither specialist skillset nor programing abilities. Basic algebraic matrices and understanding of the inherent attributes of security posture would assist SMEs to identify and mitigate some challenges.

The findings of this study are adduced from a sample population of SMEs in developing economies. This may place some limitations on the generalizability of the study. At the onset of this study, the scope was defined for a population of SMEs in developing economies which characteristically use the Internet for communications and business operations. The study further described the sample set based on the number of employees engaged by the SMEs.

The study ensures that the pre-defined sample population is adhered to and that credible measurement techniques are put in place to ensure validity and reliability. The much touted intrinsic cyber-security metrics measure the security postures of SMEs and various inferences are made.

Though, the inferences or deductions are all empirically based, they are constrained due in part to the SME definition, the web portal facilities used for data collection, the sampling techniques employed, and the analytical tools employed, such as the MATLAB based ANFIS toolbox.

The above notwithstanding, the analysis, findings and deductions are statistically confident with respect to the sampled SME population.

1.6. The Outline

This section presents the structure of the thesis.

- Introduction – Chapter 1. Gives the general background information on the topic and its relevance. Briefly, it endeavored to show how and what has been done in this study.
- Literature Review – Chapter 2. presents the theoretical underpins of this study in relation to the state-of-the-art in modeling cyber-security vulnerabilities. It endeavors to argue out what gaps in the literature exist in terms of fully covering the uncertainties associated with cyber-security vulnerabilities on SMEs in developing economies.
- Cyber-security Metrics & Data Collection – Chapter 3. presents the cyber-security metrics and data collection methods, principles and procedures employed in the cyber-security vulnerability research. It deals with the detailed research design for the metrics, sample selection and approaches employed to gather data for the study.
- Cyber-assets Vulnerability Assessment (CVA) – Chapter 4. presents detailed methods on cyber-security metrics, with emphasis on the key constructs of threat assessment, vulnerability assessment and risk/impact assessment.

- Fuzzy Sets & Neural Networks Theories – Chapter 5. presents the two (2) main theoretical frameworks of fuzzy sets and neural networks, and emphasize on the approach to neuro-fuzzy methodologies as employed in this study.
- Cyber-Security Vulnerabilities Assessment (CSVA) Model – Chapter 6. presents the empirical data, its analysis and findings which culminate into the key objective of building a cyber-security vulnerability assessment model.
- Discussion – Chapter 7. reviews the research objectives vis-à-vis the empirical findings. It endeavors to summarize the discussions and emphasize on the contributions of the study.
- Conclusions - Chapter 8. concludes by indicating areas for further research and implications.

Finally, various references and appendices are included for completeness.

The next chapter on literature review deals with the in depth appraisal of numerous related works and theories used for the study.

Chapter 2 LITERATURE REVIEW

There are few literatures on cyber-security vulnerabilities on SMEs in developing economies. Existing contributions do not examine the associated perception of uncertainties that influence on those vulnerabilities. "Since vulnerabilities in assets and threats that exploit them cannot be completely avoided, it is imperative that both must be appropriately mitigated" [65]. There is the need to have a broad perspective including the dynamics of threat propagation. Seacord & Householder [66] posit that understanding vulnerabilities is critical to understanding the threats they represent.

2.1 Small-&-Medium-sized Enterprises

2.1.1. SMEs Defined

Small and medium-sized enterprises (SMEs) consist of varied businesses usually operating in the service, trade, agri-business, micro-finance and manufacturing sectors. SMEs may be innovative and entrepreneurial, and usually aspire to grow; though, some stagnate and remain family owned. SMEs are often classified by the number of employees, annual revenue and/or the value of their assets.

The thematic research of this study is small-and-medium-sized enterprises. Who or what are SMEs? It may seem a very simple and easy question, but most literatures reviewed have divergent views. There is no consensus on its definition; no single, uniformly accepted definition of small-and-medium sized enterprises [28]. Various definitions exist whereby SMEs are classified by various parameters, including net worth, profitability, sales revenue, turnover, number of people employed, etc. The Bolton committee [67] in an attempt to rationalize the definition came up with two (2) classifications of economic and statistical based SMEs. It, however, compounded the problem with multiple definitions, with some based on industry or sector of operations and others on economic sector. For instance, an SME in the oil and gas sector is likely to have much more capital and sales, and probably more employees than a vehicle mechanic workshop.

The committee's statistical definition of SME recognizes that size is relative to sector of operations. For example, a firm may be considered small in a large market with much competition. Whereas similar sized firms may be deemed to be large in a sector where the market is small and less competitive.

Julien [68] formulated some concepts of SMEs such as the firm being small in size in comparison to large or multi-national corporations; they are said to be characterized by the following:

- Having centralized management,
- Having a low level of labor specialization,
- Having simple, informal and direct internal and external information systems, and
- Having intuitive, implicit and short-term strategy.

The Bolton committee [67] recommended that SMEs may be defined by the number of employees within some sectors and by the annual revenue in other sectors.

In furtherance to the varied definitions, for instance:

- The Federal government in Canada, under the auspices of the Small Business & Special Surveys Division defines SMEs as any business establishment with 0 to 499 employees and less than $50 million in gross revenues. However, the British Columbia Statistics (a province in Canada) defines SMEs as companies with less than 50 employees, without reference to revenues [69];
- The European Union defines an SME by the number of employees, together with the revenue and assets. A medium-sized enterprise is defined as an enterprise which employs fewer than 250 persons and whose annual turnover does not exceed €50 million or whose annual balance-sheet total does not exceed €43 million.
- The U.S. Small Business Administration defines a small business as a firm that has up to 500 employees. This definition is mostly used by US scholars; [70] [71]. The above notwithstanding, the U.S. Better Business Bureau Wise Giving Alliance [72] adopted a definition of a small business as being one with between 4 and 99 employees.
- The Small Office Home Office (SOHO) Business group (Vancouver, BC) which has carried extensive research on SMEs and has by so doing assumed authority, defines SMEs as having about 10 employees [69].

The lack of a unified definition presents a significant practical challenge; it seriously hampers the prospects of generalization of some research findings as discussions scope may need to be clearly defined to avoid any ambiguities. Any definition of SMEs in developing economies involving revenues is likely to embrace a particular set of firms that are subject to significant change within months due to fluctuating currencies.

In view of the foregoing and cognizance of the fact that currencies in both case study countries (and for that matter most developing economies) are not stable, the common denominator is

most likely the number of employees. Thus, this research adopts the definition by size or number of employees only.

The department for Business Innovation and Skills (BIS) [73], of UK and EU governments usually define SMEs as follows:

- micro company: 0 - 9 employees
- small company: 10 - 49 employees
- medium company: 50 - 249 employees
- large company: over 250 employees

This research has adopted the following definition, that SMEs are businesses with less than 10 employees as Micro Enterprises, between 10 and 50 as Small Enterprises, and between 50 to 250 employees as Medium sized enterprises. This definition falls within those applied in Ghana and Nigeria, which are case studies for this research, and it is also consistent with similar research work in ICT [29].

2.1.2. Significance of SMEs

SMEs are one of the principal driving forces in economic development. They help to diversify economic activity and make significant contributions to the economy. They are crucial to most countries' economic stability and constitute the majority of businesses, accounting for over 50% of employment [74].

The International Finance Corporation (IFC) [75] posits that the economies of developing nations is hinged on the SMEs, which is the sector that offers the "only realistic employment opportunity for millions of poor people throughout" the economies.

SMEs have been recognized as the engine of growth for developing economies. They create competitive and efficient markets. SMEs are crucial for poverty reduction strategies in developing economies. The SME sector is the largest provider of employment in most countries, especially of new jobs. They are a major source of technological innovation and new products. Obviously, with many emerging technologies in ICT, SMEs have embraced the Internet and its associated technologies for business operations and communications.

Generally, SMEs are estimated to employ about 22% of the population in developing economies [30] [31]. The SME sector in Ghana (as of 2010) accounts for about 92% of all businesses and contribute about 70% to GDP [32] [33] [34]. Similarly, the Federal Office of Statistics (as stated in [35]) indicated that 97% of all businesses in Nigeria employ less than 100 employees.

2.1.3. SMEs in Developing Economies

SMEs in developing economies are characterized by low and uncertain revenues [76]. Literature reveals that there are "... opportunities that ICT provides for SMEs in developing countries..." [77], [78]. Information systems projects in developing economies are characterized by socio-economic changes or transformations, as they seek knowledge and skillset to the SMEs. Walsham & Sahay [79] examined various literatures on information systems research in developing economies, and underscored their relevance. The emergence of Internet facilities in developing economies have impacted positively on societies and organizations, especially in areas of connection costs, access speeds and end-users utilization [80].

Ellefsen & von Solms [80] posited that developing economies are, in many instances, overwhelmed by the massive and rapid improvements of the emerging technologies in ICTs. For instance, most SMEs do not have any programs in place to harness the increased bandwidth, with its attendant vulnerability challenges confronting their systems and their customers. SMEs in developing economies are said to have unique challenges, and so "direct" importation of existing ICT solutions from the developed economies may not necessarily address the issues effectively [80].

Developing economies have embraced the emergence of ICT technologies to promote their development agenda and to present new opportunities for economic empowerment of its citizenry. In an ITU organized forum in December, 2011, the panelists underscored the need for developing economies to be pragmatic about cyber-security risks, stressing the criticality to emerging economies [81].

ITU-T [82] in the "Guide to Cyber-security for Developing Countries" admits the common areas of cyber-security solutions amongst nation states, but concedes that developing economies have peculiar challenges, requiring customized solutions.

2.1.4. Security Challenges to SMEs

Globalization and the advancement in Internet technologies have spurred SMEs into positioning themselves from small regional based companies to become global, cross-border companies. SMEs are seizing the opportunities offered by globalization to gain access to strategic markets. Whilst, these trends come with many more opportunities for SMEs, they also pose some risks.

Cyber-security vulnerabilities pose serious concerns to all businesses; SMEs are usually hardest hit victims and find it very difficult to recover after a cyber-attack. SMEs are easier

targets than large corporations. Large corporations have, in recent times, strengthened their security systems, either as a response to the increased threats or in compliance with regulations. The issues of cyber-security metrics and dimensions are explored in details in subsequent sections of this review.

Pierre [83] in examining cyber-crime activities indicated that "many SMEs do not consider themselves as having data that is of interest to cyber-criminals and quite often dismiss the need for properly addressing vulnerabilities in their infrastructure". He continued that "the opposite is true; every business today collects data on employees, customers and vendors that are of interest to cyber-criminals".

Sharma et al [84] provide an overview of the cyber-attacks which prospective customers of e-commerce are likely to encounter while carrying out transactions over the web. They provide a detailed account of highly specialized attacks that are aimed at SMEs. Rapid diffusion of e-commerce and a rising number of interconnected networks have resulted in an escalation of security threats [85].

The concept of engaging external resources for information systems management raises some challenges. Today's management information systems are typified by ensuring that data and all corporate assets are properly safeguarded. Though, most SMEs may outsource that important component of its business, some may resort to using internal resources which are not up to speed with most security developments in order to save cost.

Julien's concept of simple external information systems whereby the owner-director is supposed to be in total control of all operations may not be the case in today's cyber-economies. SMEs today, though still small in size relatively, are connected with the rest of the world via the Internet. They may have websites which could have its own vulnerabilities. Customers and vendors, as well as some mobile workers, may log-in remotely, all posing some security challenges to the SMEs.

Contributing to Julien's concepts, Planque [86] posits that "the means of obtaining information are a group of interpersonal and informal relationships which are non-institutionalized and unstructured". Again, SMEs today have established structured and standardized forms of communications and information gathering, such as the use of emails. Invoices and tender documents are submitted via email, meetings are held via Skype, formal and informal communications take place via Instant Messengers (IMs), etc. As long as important business communications take place via the electronic media, the confidentiality of the information or data must be protected, the integrity must be ensured, and that the channels must be available

whenever needed. Any breach or compromise of any of these security properties is the motivation for this research.

This study on cyber-security vulnerabilities inherent with SMEs considers network infrastructure, software and applications used by SMEs without due considerations, key drivers towards ICT investment, outsourcing of ICT services and solutions, especially security solutions, SMEs perception of cyber-security and its accrued benefits, if any, etc. Studies have shown that the main drivers for "ICT investment are to provide better and quality customer service and to stay ahead of the competition" [87]. Many SMEs in developing countries are said to outsource most of their ICT activities, due to lack of in-house security expertise, cost, and adequate resources for planning and implementation of ICT projects [88].

2.1.5. Security: Impact on Business Operations of the SME

Recent advances in ICTs and the need for globalization have persuaded SMEs to seize the opportunities for the adoption and introduction of innovative business operations, user-friendly products and services, and customer centric strategies. Incidentally, these opportunities have their corresponding challenges that threaten the SMEs, especially cyber-security issues relating to abuse of confidentiality, integrity and availability (CIA). The resultant adverse effects or impacts on SMEs are seen as revenue losses, resource depletion, and loss of customer and investor confidence, etc.

Risk is seen as the possibility for loss of confidentiality, integrity and availability due to a specific threat [89]. Typically, cyber-security objective is to deter, prevent, detect, recover from, and respond to threats in cyberspace. Cyber-security is to safeguard the information assets, the information systems and networks that deliver the information, from damage or compromise resulting from failures of confidentiality, integrity and availability. Cyber-security is multifaceted and it includes information technology, procedures and practices, laws and regulations, people and organizations; these areas are said to be interrelated and impact each other [14].

To ensure business continuity, SMEs require a model that enables them to proactively analyze the various imperative factors critical to the security and business operations.

2.2 Cyber-security Model Metrics

The body of knowledge on subjects related to cyber-security vulnerabilities, threats and risk is very large and growing. This review considered nearly 100 sources primarily from academia, computer emergency response teams (CERTs) or cyber-security incident response teams (CSIRTs), security solutions providers, law enforcement agencies and other governmental

sources. The result is a review that details a broad range of cyber-security challenges that confront SMEs in developing economies, though some comparisons with large corporations are rarely made. The review also aided in designing the survey questionnaire as to what vulnerabilities are most likely to confront SMEs in developing economies.

This section of the review deals with cyber-security metrics - how to quantify, classify, and measure cyber-security vulnerabilities on SMEs operations in developing economies. In writing the Foreword to the book, "Security Metrics – Replacing Fear, Uncertainty and Doubt" [90], Daniel Geer likened security measurement with "numbers". He posited that "numbers exhibit vulnerabilities like computer systems in that whether misuse is intentional or inadvertent matters little if misuse is at hand". Indeed, cyber incidents, whether caused by intentional or unintentional entities or processes are immaterial as far as the impact is concerned. Rather the ability to identify the threat agents and to understand the vulnerabilities, and take appropriate steps to mitigate the risks is of paramount importance.

The ITU-T Recommendation X.805 [10] stipulates eight (8) cyber-security dimensions; namely, *authorization, authentication, availability, communications security, confidentiality, integrity, non-repudiation and privacy*. Other authorities have attempted to propose alternative cyber-security properties – Zimmerman's [11] *pretty-good-privacy (PGP)* and Dhillon & Backhouse [12] expand the CIA triad with their *RITE* security principles of *responsibility, integrity*[7]*, trust and ethicality*. Also, the Parkerian hexad proposes six (6) cyber-security attributes of possession (or control), authentication, utility, confidentiality, integrity and availability [13]. However, universally, the classical cyber-security triad of *confidentiality, integrity and availability (CIA)* has become the bedrock of most cyber-security assessment. This study thus focuses on the CIA triad (see Figure 2-1).

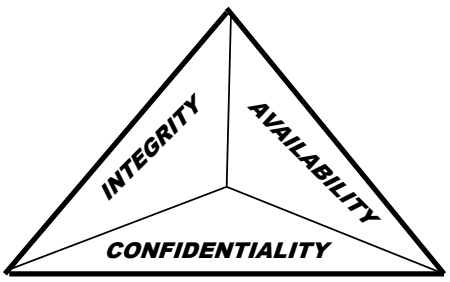


Figure 2- 1: The Cyber-security Triad of Confidentiality, Integrity & Availability (CIA)

Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities or processes. Confidentiality protects data in storage and in transmission.

[7] Integrity in RITE is a requirement of members not to divulge nor reveal any security breach to any "outside" entity [12]

Integrity is the ability to ensure that information has not been altered. It means that data cannot be modified without authorization. Integrity ensures that the data has not been altered in storage and/or in transmission.

Availability ensures that information assets are accessible whenever needed. It is an important property since any disruption of service may adversely affect business operations of SMEs.

For this study, Cyber-security is defined as ability to safeguard computer systems and the confidentiality, integrity and availability of the data they contain.

This study deals with the perceived uncertainty and risk with the use of the Internet and its applications. The thesis employs a risk assessment methodology on randomly selected SMEs in developing economies. The empirical data collated through surveys and strategic interviews are used to build a model that SMEs could use to benchmark vulnerabilities and to proactively mitigate risks.

The proposed model is considered an effective technique in assessing the impact of cyber-security vulnerabilities on SMEs. It combines the human inference style and linguistic expressions of fuzzy systems with the learning and parallel processing capabilities of neural networks to analyze the risks on SMEs.

According to [91] "the role of conceptual modeling in information systems development is seen as an approach for capturing fuzzy, ill-defined, informal "real-World" descriptions and user requirements, and then transforming them to formal, in some sense complete, and consistent conceptual specifications."

Ayyub [18] posits that "classical set theory can efficiently deal with ambiguity by modeling non-specificity, whereas fuzzy and rough sets can be used to model vagueness, coarseness and simplifications". According to [18] engineers use system information as models for the purposes of system analysis and design, to either classify, sort-out, analyze, and/or predict system attributes, variables, parameters and performances. Ayyub [18] admits that uncertainties are attributed to system ambiguities, likelihood, approximations, and inconsistencies in defining system architecture, variables, parameters which are needed to predict the system.

By using models, the study endeavors to measure or quantify uncertainties, such as the vulnerabilities (which are inherent in ICT assets and whose susceptibilities in turn may compromise the confidentiality, integrity and availability properties) or threat, etc. The unique distinction here is that the study measures conceived or abstract notions rather a physical quantity.

2.2.1. Risk Defined

Risk is the likelihood of the occurrence or realization of a threat, with a possibility to adversely impact on business.

Typically, when risk is calculated quantitatively, the functional values of threats, vulnerabilities and assets are estimated from a probability domain [92] [93].

Bernoulli [94] posits that measurement of risk is computed as expected values, in consideration of probabilities of occurrences. He continued that based on this theoretical framework, alternatives are determined and classified into equi-probable cases. Admittedly, this classification is usually subjective, albeit in a quantitative analysis.

Bernoulli's framework is hinged on the assumption that "the risks anticipated by each [entity] must be deemed equal in value". Interestingly, he demanded that no characteristics of the entities should be considered; there shouldn't be the use of judgment, only deliberations. Considerations of risks, especially of networks and associated incidents will have some subjectivity.

Culp [95] defines risk as any random occurrences with adverse impact or effects on a firm. Risks impacting on organizations could be classified as either exogenous (due to weaknesses external to the system) or endogenous (due to weaknesses within the system).

The impact component as evaluated by the traditional notion of risk is herewith compensated for within the asset value. Similarly, the likelihood probability is compensated for within both the threat and vulnerability values [96], as seen in equation [1-4] in the previous chapter.

Risk management entails risk identification, risk analysis and risk mitigation. Bass & Robichaux [97] posited that risk identification has three (3) key components, namely criticality, vulnerability and threat. Criticality here defines the importance of the asset to the organization, which is consistent with this study's mathematical definition of risk in equation [1-4]. In this study, the criticality argument is examined under the classification of the assets, which is an indication of the impact or the extent and severity upon attack on the system.

Srinivasan & Abi-raad [98] in their paper on "Risk factors with e-Business on SMEs", admitted that risk analysis involves both quantitative and qualitative assessments, though a degree of subjectivity is involved in estimating the risk levels. Yazar [45] posits that the qualitative risk analysis is subject to expert's or the assessor's opinion. Generally, quantitative risk analysis is suitable in situations where historical data is available and it is easy to quantify or estimate incidents. Srinivasan & Abi-raad [98] posit that lack of reliable data on security incidents

render the use of statistical models ineffective or at least, with great difficulty. SMEs in most developing economies lack reliable historical data that could be used for any quantitative risk assessment. Hence, qualitative risk assessment with the use of subjective experts' opinions becomes appropriate.

Also, in cyber-security, new vulnerabilities and threats emerge almost on daily basis and so qualitative assessment may be more appropriate. Here the risks are described as either low, medium, high, or very high. For this study, systems are classified as being insecure, secured or highly secured.

The total impact or risk to the SME is not only financial considerations, but also, morale, business output, credibility, investor and customer confidence, corporate image, reputational damage, etc. Shaurette [8] posits that though the conventional probabilistic risk assessment "is based on well-established mathematical theory", its ratings are fraught with subjective guesstimates. He continued that qualitative risk values may be estimated based on rules, such as fuzzy inference rules, that capture the consolidated advice of security experts. The business impact is evaluated with expert knowledge supported by historical data and consists of two main elements [99]. The expert decision must take into account both financial loss due to threat realization and the morale loss on business functionality, as well as the type of business engaged in.

Stajano [100] posits that cyber-security is essentially risk management. He advocates that it entails identifying:

- assets (which are any items of economic value that are to be protected);
- threats (as any agent, condition, or circumstance that can potentially cause harm, loss, damage, or compromise the asset);
- vulnerabilities (as weaknesses that might facilitate the occurrence of a threat);
- attacks (as ways a threat can be made to happen); and
- risks (as the expected loss caused by each attack, corresponding to the value of the asset involved and the likelihood that the attack will occur).

It must be noted that each information has a price tag, and thus, requires a certain degree of protection, which is evaluated through security classification. Information is classified based on a number of factors, including stakeholder's experiences, value of information to the SME, governing laws and regulation, etc. For this research, the following classification shall be applied:

i. Business sector information as: Public, Sensitive, Private, Confidential;
ii. Government sector information as: Unclassified, Sensitive But Unclassified, Restricted, Confidential, Secret and Top Secret.

2.2.2. Perceived Uncertainty

Perceived uncertainty in the context of this study emanates from Knight's [101] definition of risk and uncertainty, and it encompasses data gathering whereby the empirical data to be collected for the study is characterized [102] as follows:

- The measures, metrics, or quantities are assumed to be imprecise, vague or fuzzy;
- The measuring instrument of survey, for example, could be fraught with inaccuracies;
- The metrics could be wrong parameters.

In view of the above, the perceived uncertainties are well taken care of in fuzzy modeling or treatment whether the empirical data is truncated, or noisy data, or erroneous data [102].

Knight [101] posits that lack of data itself leads to uncertainties, which underpins lots of business decisions – which are usually "too unique, for any statistical tabulation" ([101] as cited in [103]). According to [103], "probability is often used as a metric of uncertainty", though with a limited utility, it defines perceived uncertainty. Perceived uncertainty is said to be a form of uncertainty that can be defined operationally. By extension, the presence of risk is assumed as a perceived risk.

Sivanandam, S.N. et al. [104] posit that "uncertainty comes from a number of sources such as ignorance, chance, randomness, vagueness (or unclear statements) like fuzziness within our natural language, as well as lack of knowledge".

Friedlob & Schleifer [105] inferred that "risk arises from the lack of information, which in turn leads to uncertainty". They acknowledged the different types of uncertainty and used the potential of fuzzy set theory to facilitate measurement and management of risk. In view of that, all businesses are confronted with uncertainties in their daily operations. Uncertainty arises out of deficiency in information. Friedlob & Schleifer [105] categorized uncertainty into three (3) types, such as:

- Fuzziness;
- Ambiguity – resulting from discord; and
- Ambiguity – resulting from non-specificity.

This study has much interest with the first source of uncertainty. Fuzziness is uncertainty arising out of vagueness. The notion of uncertainty is applicable to situations such as cyber-attacks on SMEs networks. The systems administrator cannot predict when a virus will affect his systems or the susceptibility of his systems, neither can he predict when corporate payroll will be doctored, due in part to loopholes in the organization; - the vagueness of these uncertainties is what Lotfi Zadeh [6] espoused in his Fuzzy Set Theory. Cyber-security

vulnerabilities or challenges, as in most natural language descriptors, are vague and somewhat uncertain [105]. Thus, fuzzy sets are applicable to this study as a number of vulnerabilities are described by fuzzy linguistic terms.

Business executives make various decisions partly based on their scope of knowledge or information available to them. It implies that decision makers take risks in decisions in accordance with the information available to them, with some degree of uncertainty. According to [106] this requires the use of some basic metrics of uncertainties.

According to [107] experts don't use probability theory when assessing the likelihood of uncertain events. They use heuristics or rules. This is in accordance with this study's approach to use fuzzy and neural network methodologies to analyze the linguistic expert opinions about cyber-security vulnerabilities.

Zadeh [6] defines a fuzzy number as an appropriate numerical value whose boundary is not crisp and is characterized by a membership grade function. Let X be a fundamental set with $x_i (i = 1, 2, \ldots\ldots, n)$ elements and mapping unto the unit interval $[0,1]$. Then, an assessment with some lexical, informal or uncertain propositions [17] leads to an assignment of a subset A of X, such that $A = \{(x, \mu_A(x)) \mid x \in X\}$ is referred to as the uncertain subset or fuzzy subset; heretofore referred to simply as fuzzy set. The set X is also called the universe of discourse and $\mu_A(x)$ is the membership function of the fuzzy set.

Milliken [108] adds to the literature on perceived uncertainty by defining three (3) types of perceived uncertainty:

i. Perceived State Uncertainty – here the perceived uncertainty is about the inability to predict the future behavior or state of an organization, given a number of "environmental" or external constructs (to the organization), such as competitors, stakeholders, vendors, suppliers, etc.
ii. Perceived Effect Uncertainty – relates to the inability to predict the impact or extent and severity or effects on the system, should there be a change. That is, the uncertainties associated with the effect of a possible future event. Others view the perceived effect uncertainty as a deficiency of knowledge of cause-effect relationships of the system [109] [110].
iii. Perceived Response Uncertainty – defines "the lack of knowledge of response options", or the likely consequences of a particular choice or option in response to a threat to the system [109] [111].

Kaplan & Garrick [112] posited that determining risk generally amounts to addressing the following questions:

- What could go wrong?
- How many times does it go wrong?
- What is the impact on the organization? Or what are the consequences?

The answer to the first question is a set of threats, presented by exploited vulnerabilities. The second question requires the evaluation of the possibility of occurrences of these threats. The third question estimates the extent and severity of consequences or the impact level of the risk as a result of the exploited vulnerabilities. The issue of how confident or certain the answers to these questions are correct, is dependent upon the inherent uncertainties surrounding the protection of the assets.

In this study, risk is perceived as uncertainty in its subjective assessment with regards to the 'nature, level and source' [113] of vulnerabilities inherent in the cyber assets.

McFadzean et al [114] found that the "decision-makers" perception of both internal and external risks has a major impact on information security. They observed that, "decision-makers' perception of risk will have an impact on their own roles and actions including the development of the organization's information security strategy". It is these attitudes, opinions and values that have an effect on the perceivers' actions and decision making processes [115] [116].

The utility of fuzzy functions become handy for empirical extrapolation and/or forecasting models, even when data is unavailable [117]. Studies on cyber-security vulnerabilities on SMEs in developing economies have little or no historical data, and thus, the use of fuzzy logic is a suitable technique to deal with data beyond what is available or can be measured.

In measuring the vulnerabilities, fuzzy set theory is used in view of its utility to the qualitative and subjective linguistic variables for definition of possible states in concert with appropriate approaches that yields a quantitative equivalent for each state [118] [119] [120]. One-to-one mapping function or membership function is used to relate the possible states with the linguistic variables.

To show the uncertainty in the parameter values, fuzzy number estimators are used, such as the triangular fuzzy number $A(x) = [a, b, c]$, where a is the lowest value of support of x; c is the highest value of support of x; and b is the middle value or modal value of the triangle.

A triangular fuzzy number $A[a, b, c]$ can be represented as

$$\mu_A(x) = \begin{cases} \frac{x-a}{b-a} & ; a \le x \le b \\ \frac{x-c}{b-c} & ; \mathrm{b} \le x \le c \\ 0 & ; otherwise \end{cases} \quad [2\text{-}1]$$

A trapezoidal fuzzy number $A[a,b,c,d]$ can be represented as

$$\mu_A(x) = \begin{cases} \frac{x-a}{b-a} & ; a \le x \le b \\ 1 & ; \mathrm{b} \le x \le c \\ \frac{x-d}{c-d} & ; \mathrm{c} \le x \le d \\ 0 & ; otherwise \end{cases} \quad [2\text{-}2]$$

2.2.3. Confidentiality

Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities or processes. Confidentiality protects data in storage and in transmission. Confidentiality is compromised whenever information can be viewed or read by unauthorized entities or disclosed out of the 'need to know' group or community. This compromise could be either physical or electronic.

The electronic confidentiality compromises include end-users or entities accessing information, data or resources that are not meant for them. For instance, if someone can access one's email messages without the express authorization from the account owner, confidentiality property is said to be breached.

The physical confidential compromises include reading printouts marked 'confidential' or verbal disclosure of confidential information outside the 'need to know' group.

Confidentiality ensures that information is accessed by and disclosed to authorized users only. Confidentiality encompasses the concepts of data privacy, encryption and cipher or cryptography.

2.2.4. Integrity

Integrity is the ability to ensure that information has not been altered. It means that data cannot be modified without authorization. Integrity ensures that the data has not been altered in storage and/or in transmission.

Integrity is breached whenever information is modified without the express authorization by the information owner. This compromise could result in commission or omission of either authorized user or unauthorized entity.

Integrity compromise could be either accidental or intentional and through malicious intent. Malicious integrity compromise could be that an entity intentionally adds, deletes, or modifies database records. This can occur either through an authorized party (someone who has the access to actually modify the record) or by an unauthorized party when the user has access that they shouldn't have.

Accidental integrity compromise is when a system modifies or deletes records that it shouldn't. This can occur when a virus infects a system or when a user does something that he didn't intend to do. This is often why systems will verify that you want a file deleted, before it actually does so. Integrity refers to the trustworthiness of information resources.

It includes the concept of "data integrity" - namely, that data have not been changed inappropriately, whether by accident or deliberately malicious activity. It also includes "origin" or "source integrity" - that is, that the data actually came from the person or entity you think it did, rather than an imposter, e.g. phishing or spam.

Integrity can even include the notion that the person or entity in question entered the right information - that is, that the information reflected the actual circumstances (in statistics, this is the concept of "validity") and that under the same circumstances would generate identical data. On a more restrictive view, however, integrity of an information system includes only preservation without corruption of whatever was transmitted or entered into the system, right or wrong.

2.2.5. Availability

Availability ensures that information assets are accessible whenever needed. It is an important property since any disruption of service may adversely affect business operations of SMEs.

Availability is to ensure that an authorized user or entity or unit can access a system resource when a legitimate request is made. If this resource is a mission critical asset, then availability requires that a backup or redundancy provisions are made to guarantee its availability.

Availability compromise could occur as a result of unintentional actions or accident or by malicious or intentional acts, such as a Denial-of-Service attack or botnets. Availability compromises could also be categorized as technical, human or natural phenomena, such flood, earthquake or power outage.

2.2.6. Impact

The impact on a system is measured by the extent and severity of the loss caused to the asset upon threat realization. The extent and severity of the loss is directly proportional to the operational or business value of the asset compromised or attacked [121].

The impact on SMEs associated with the exploitation of vulnerabilities such as compromises of customer data, or alteration of data in transit, or denial of service to an authorized entity, can be determined quantitatively. Miller [92] evaluates the impact by estimating the annual loss expectancy (ALE) using probabilities. The impact is the obvious manifestation of the extent and severity of a realized threat, i.e. risk is eminent.

In view of the associated catastrophic impact of cyber-attacks, most businesses, especially large corporations, invest in both physical and technical security controls [122]. Some businesses may invest in procuring intrusion detection and prevention systems. The impacts have direct and indirect cost implications, e.g. cost of mitigation techniques, cost of restoration, reputational damage, etc.

In order to justify the need for spending to improve security, one must first carry out risk analysis. Two basic types of risk analysis to consider are quantitative risk analysis and qualitative risk analysis. Quantitative risk analysis attempts to assign independently objective monetary values to the components of the risk assessment and to the assessment of potential losses. Conversely, a qualitative risk analysis is scenario-based [92].

Both Sarbanes-Oxley Act and Basel II Accord emphasize the need for an integral security risk and business risk management as a regulatory requirement. Ayyub & Klir [106] posit that every system is designed purposefully with unknown variables. If the unknown variables can be determined, they are said to be deterministic, otherwise, they are non-deterministic.

Expert opinions are subjective and are said to be perceived "experiences" of uncertainties about an event or a situation. Applications of expert opinions or perceived uncertainty may be used to evaluate subjective probabilities. However, in this study, lots of expert opinions are used in view of lack of historical data on security incident occurrences and metrics. Zadeh's [6] fuzzy set theory facilitated, processed expert opinions and formalized the notions of perceived uncertainty. Fuzzy set and logic with its capability to process linguistic variables and rules are employed.

Ayyub & Klir [106] proposed three (3) uncertainty based criteria used in constructing knowledge based on uncertainty and information synthesis. The principles are:

- The principle of minimum uncertainty – alternatives (to problems) are formulated as solution sets; the only solutions accepted are those which reduce uncertainty to minimum acceptable level or which have minimal loss of information;
- The principle of maximum uncertainty – alternatives drawn from intuitive inference are used to maximize the relevant uncertainty within a given constraint;
- The principle of invariance uncertainty – alternatives are deduced to preserve information as they are transformed from one uncertainty measure to the other; e.g. transformation of probabilities to possibilities.

There is contribution in literature that supports the use of perceived uncertainty measures for eliciting and aggregating expert opinions [123] [124] [125]. In this study, a couple of uncertainty measures [126] [106] are employed to address expert opinions on the impact of cyber-security vulnerabilities on SMEs.

2.2.6.1. Impact: Expert Opinion Elicitation

Most engineering decision making processes are complex and involve uncertainties. One technique that lends itself in the uncertainty analysis is the fuzzy set theory [6]. The degree of membership of the fuzzy linguistic variables can be estimated by various methods such as intuition, inference, rank ordering, inductive reasoning, among others. Intuition is of particular interest to this study and it is said to be based on the human intelligence and understanding of the issue of interest; herewith referred to as Expert Knowledge.

Using Ayyub's [18] definition of an expert, opinions are elicited as either a formal judgment, an advice, a conclusion, or a belief, which is a subjective estimation of the problem. This may seem true, valid or probable in the eyes of the expert [18]. Expert opinion elicitation is used to assess the impact of cyber-security vulnerabilities on SMEs as well as the consequences and severity on the systems.

The impact of cyber-security vulnerabilities on SMEs is assessed, as measures of the perceived risk, by eliciting the expert opinions through structured questionnaire and strategic interviews.

Literature support use of experts to construct knowledge based on available information and data, in what [18] terms as "Expert Opinion Elicitation". The expert opinions are said to be propositions that do not necessarily meet the justified true belief (JTB) requirements of knowledge, and thus may be fraught with some uncertainties. Ayyub [18] advises that, in view of the above, researchers have vested interest in ensuring that the process of expert opinion elicitation optimizes all the available information contents as provided by the experts. The

expert opinions should account for any uncertainties by appropriately aggregating them into useful and acceptable decisions [56].

Lance Hayden [127] posited that there exist other methods of elicitation with high degree of accuracy of decision-making under uncertainty, such as expert calibration and training. These strategies could best leverage on historical data, if available, to make extrapolations.

2.2.6.2. Impact: Aggregation Methods

There are various methods for aggregating expert opinions, such as:

- Similarity measures [126] [128]
- Simple averages [129]
- Bayesian Aggregation [130]
- Analytic Hierarchy Process (AHP) [131].

Cooke [132] and Rowe [133] provided elaborative summaries of various methods employed in aggregating expert opinions. These methods can be classified into Consensus methods and Mathematical methods ([134] & [135] as cited in [18]).

The fuzzy averaging operations, also called AGGREGATION, fall within the gap between the unions and intersections [119] [136].

First, the linguistic variables are used to represent the relative importance of the expert's opinion and the perceived degree of confidence on each expert as seen by the researcher. Then, the linguistic variables are represented by fuzzy numbers for arithmetic computations. Moon & Kang [56] posit that the primary reason for employing "expert judgments in uncertainty analysis is to assist in estimating the possible values for an uncertain parameter [which is the Impact or Risk on SMEs in this study] and properly representing the uncertainties associated with it". Researchers [56] [137] agree that a couple of key questions that beg for answers are:

- How to elicit information from the experts; and
- How to aggregate the various opinions in a group decision-making or with multiple experts.

It must be noted that, experts do express their opinions using vague terms or subjective linguistic terms and phrases or words using everyday expressions such as, very low, very high, slightly secured, highly secured, etc. These vague linguistic terms are modeled using membership functions, as it's difficult to define them with crisp sets. The membership functions are usually constructed subjectively based on experts' experience and opinions and/or that of the researcher's.

Adapting [138] and [56] aggregation methods, the steps applied are illustrated in the ensuing sections.

Experts Elicitation

Assume n expert opinions E_i $(i = 1,2, \ldots\ldots, \text{n})$ are elicited, with m criteria for evaluation, C_j $(j = 1,2, \ldots\ldots, \text{m})$. The preference rating ρ_{ij} is a set for the experts and associated criteria for evaluation, such that ρ_{ij} has linguistic variable x, with linguistic term tuples $\rho_{ij}(x)$, representing the preferences ratings of linguistic variables and associated membership functions. Let also w_j be the preference ratings for each criterion C_j such that the fuzzy confidence level or index of optimism, α_i for the experts is computed by aggregating ρ_{ij} and w_j.

Using "importance" mean operator [63],

$$\alpha_i = \tfrac{1}{m} \sum_{j=1}^{m} \rho_{ij} w_j \qquad [2\text{-}3]$$

So, the fuzzy confidence levels for experts E_1 and E_2 are given by

$$\alpha_1 = \frac{1}{m}\left(\rho_{11}w_1 \oplus \rho_{12}w_2 \oplus \ldots\ldots\ldots \oplus \rho_{1m}w_m\right) \qquad [2\text{-}4]$$

and

$$\alpha_2 = \frac{1}{m}\left(\rho_{21}w_1 \oplus \rho_{22}w_2 \oplus \ldots\ldots\ldots \oplus \rho_{2m}w_m\right) \qquad [2\text{-}5]$$

respectively[8].

Upon computing the confidence levels of the experts, each expert is associated with a triangular fuzzy number A_i with corresponding membership functions μ_{A_i}. The triangular fuzzy numbers represent the fuzzy estimates ranked by the experts for a given criterion and alternative. By the extension principle, an approximate fuzzy number, R_i is deduced [64] [56] as an aggregated ranking: $R_i \cong (X_i, Y_i, Z_i)$, where triangular fuzzy numbers $\rho_{ij} = (\text{q}_{ij}, \text{r}_{ij}, \text{s}_{ij})$ and $w_j = (\text{t}_j, \text{u}_j, \text{v}_j)$, such that $X_i = \frac{1}{m}\sum_j \left(q_{ij}t_j\right)$; $Y_i = \frac{1}{m}\sum_j \left(r_{ij}u_j\right)$; $Z_i = \frac{1}{m}\sum_j \left(s_{ij}v_j\right)$ for all $i = 1,2,\ldots\ldots,n$ and $j = 1,2,\ldots\ldots,m$.

[8] $\oplus$ is a bounded sum

Estimation of Confidence Level or index of optimism

The confidence levels or indices of optimism for each expert are estimated.

Let $A \subset R$ be a subset of the set of real numbers; for a fuzzy number A defined as $A = [a,\ b,\ c;\ \mathrm{w}]$ with a membership function $\mu_A(x)$ given by

$$\mu_A(x) = \begin{cases} \mu_A^l(x) & ;\ a \le x \le b \\ 1 & ;\ x = b \\ \mu_A^r(x) & ;\ \mathrm{b} \le x \le c \end{cases} \qquad [2\text{-}6]$$

This generates a graph that is bounded by $-\infty < a \le b \le c < \infty$ and $0 < w \le 1$. Assume $\mu_A^l(x) : [a,b] \to [0,w]$ is a continuous and strictly increasing function; whereas $\mu_A^r(x) : [b,c] \to [0,w]$ is a continuous and strictly decreasing function. By definition, when $w = 1$, the fuzzy number A is said to be normal.

Let α be a confidence level or an index of optimism [138], then α takes its values from the unit interval; i.e. $\alpha \in [0,1]$. In essence, the confidence level or index of optimism is an indication of the decision-maker's assessment of ranking of the attributes [138].

Liou & Wang [138] showed that the left and right integral values, $I_l(A)$ and $I_r(A)$, respectively reflect the decision-makers' levels of pessimistic and optimistic on the rankings; and given by

$$\begin{aligned} I_l(A) &= \int_0^w \mu_A^l(y)dy \\ &\text{and} \\ I_r(A) &= \int_0^w \mu_A^r(y)dy \end{aligned} \qquad [2\text{-}7]$$

It follows that the total integral value is given by

$$\begin{aligned} I_t^\alpha(A) &= (1-\alpha)I_l(A) + \alpha I_r(A) \\ &= (1-\alpha)\int_0^w \mu_A^l(y)dy + \alpha\int_0^w \mu_A^r(y)dy \end{aligned} \qquad [2\text{-}8]$$

It can be shown [138] that the left, right and total integral values at confidence level or index of optimism α are:

$$I_l^{\alpha}(A) = \frac{w}{2}(a+b)$$

$$I_r^{\alpha}(A) = \frac{w}{2}(b+c) \qquad [2\text{-}9]$$

$$I_t^{\alpha}(A) = \frac{w}{2}\left(\alpha c + b + (1-\alpha)a\right)$$

As an illustration, assuming *n* experts are consulted for expert opinions on cyber-security vulnerabilities confronting SMEs in developing economies; i.e.
$E_i = \{E_1, E_2, ..., E_n\}$; i = 1,2, ..., n. Then, the criteria for evaluation, C_j is given by
$C_j = \{C_1, C_2, ..., C_m\}$; j= 1,2, ..., m.

For this study, C_j could be elements such as {education (Edu), experience (Exp), ethics (Eth), independence (Ind), management (Mgt), responsibility (Res), etc. }

There are two key linguistic "concepts" variables defined as "importance" and "confidence" with respective quintuples:

W = {Very-Minor, Minor, Important, Vital, Critical} representing the relative importance or criticality of each criterion; and

C = {VeryLow, Low, Medium, High, VeryHigh} representing the confidence levels on each expert.

The corresponding membership functions are then defined using triangular fuzzy numbers. Then the weights would be computed from equations [2-4] & [2-8].

2.2.6.3 Security Impact Assessment:

The impact of a security attack can be financially significant. SMEs lack the resources available to large enterprises, and they often find it harder to recover from an attack. Carnegie Mellon University [139] estimates that 99% of all reported intrusions "result through exploitation of known vulnerabilities, for which countermeasures are available". Cashell et al [25] asserted that SMEs in particular lack the security expertise necessary to fend off cyber-attacks.

There are very few studies about security audits and solutions on SMEs in developing countries. Most security audit researches have either been on specialized protocol and systems or on enterprises in the developed countries [140] [141] [142].

According to [143], "many previous studies have attempted to quantify financial losses resulting from [cyber-security] breaches, reliance on self-reported survey data has undermined the credibility of their results." They posit that "using an event-study methodology" to analyze the financial impact of cyber-breaches yields a better result. "While carrying out the impact analysis of security vulnerabilities seems a daunting task, increasing possibility and scope of cyber-security breaches due to increasing interconnectivity makes it imperative" [144]

2.2.7. Possibility Theory

Possibility theory, as introduced by Zadeh [5], is an uncertainty theory devoted to the handling of incomplete information. Zadeh meant to use possibility theory to handle "graded semantics of natural language statements" [145]. It is based on set functions just like probability theory, but differs by the use of dual set functions of possibility and necessity measures [145]. Possibility theory relates to fuzzy sets theory as a concept of possibility distribution with a fuzzy restriction on assigned values [5]. It compliments fuzzy set theory by way of explaining the concepts of fuzziness.

Zadeh's [5] seminal work on the possibility theory argued that the fuzziness expressed in natural languages is "possibilistic rather than probabilistic in nature". He posited that an analytical metric concerned with capturing the essence of information, and its intrinsic attributes, should be by means of possibility measures rather than probability measures.

Probability is conceptually a representation of the occurrence of events in random space [47]. The notion of randomness presumes the capability of employing probability theory to "measure and order the random space [47]. Whereas, fuzziness associated with possibility theory has inherent attributes, linguistic terms in "probability have no underlying semantics"; they are arbitrary [47]. In essence, probability (through probability distribution functions) tells of a population; it is said that probability evaporates with individual instances [47].

Consider the statements "it is probable that Ezer's laptop will get a virus" and "it is possible that Ezer's laptop will be infected with virus". First, the probability of virus infection is predicated on a number of laptops in similar conditions as Ezer's. As soon as the laptop gets infected, the probability vanishes at that moment, because it has already occurred. On the other hand, in view of Ezer's laptop's disposition, such as no or outdated antivirus, the possibility of virus infection remains with the "insecurity" of the laptop. This intrinsic property of the laptop enshrined in the vagueness of "insecurity" is what is known as fuzziness; and it doesn't dissipate with time.

Zadeh [5] underscores the important fact of possibility distribution being distinct from probability distribution. He illustrated the point with the infamous "Hans can eat μ eggs for breakfast" example. Though it might be highly possible for Hans to eat, say 6 eggs for breakfast, the probability may be very small. In the same vein, it might be possible for someone to eat a dozen eggs, but its chances may be improbable. That is, an existence of a possibility of occurrence does not necessarily imply a similar measure of probability of occurrence.

Dubois [145] posited that possibility theory is not additive and it handles ordinal structures appropriately. According to [145], possibility and necessity measures can handle partial beliefs. He asserts that, both possibility and necessity measures have their respective degrees of beliefs. Whereas, possibility degree of disjunction events is given by the maximum of the possibility degrees of the events (maxitive), the necessity degree of conjunction events is given by the minimum of the necessity degrees of the events (minitive).

Possibility theory also thrives on the notion that any hypothesis not known to be impossible cannot be ruled out. This study focused on plausibility of threats maturing to exploit vulnerabilities that exist in assets giving rise to exposures of different impacts to the SMEs.

Possibility theory in its qualitative treatment finds application in ranking or comparative assessment (c.f. fuzzy similarity measures used in assessing the taxonomies of vulnerabilities and threat agents. It is applicable to decision making under uncertainty with multi-attribute qualitative criteria. For example, if U is a universe of discourse and $X \subset U$ is a fuzzy set, then for uncertainty states $x \in X$, the following axioms hold true [146]:

- $\mu(x) = 0 \Rightarrow$ a complete rejection of the state;
- $\mu(x_1) > \mu(x_2) \Rightarrow x_1$ is preferred to x_2;
- $\mu(x) = 1 \Rightarrow$ an absolute preference of the state;

where $\mu(x)$ is a possibilistic qualitative utility function or a membership function (in fuzzy set theory). Possibility theory is an alternative to probability theory, with applications in uncertainty situations, where data sets are not large and the lack present constitute uncertainty in itself. Note that, possibility distributions are represented by fuzzy numbers. Dubois & Prade [146] posit that for "any possibility measure Π, there exists an equivalent fuzzy set A, such that $\mu_A(x) = \pi(x)$ where $x \in X$ in A with $\mu_A(x) \in [0,1]$."

Shenoy [147] took the definition of possibility measures to another dimension. First, he referred to the possibility function as a consistent possibilistic state. Then, he posited that

propositions in a possibilistic state are "either possibly True (or simply, possible) or possibly False (or simply, not possible) [147].

Suppose X is a fuzzy linguistic variable in the set $A(x)$, then the following axioms (conditions) must be consistent with Shenoy's [147] possibilistic state:

a. For any proposition X_i, one and only one state holds true:
   i. X_i is possible; or
   ii. X_i is not possible.
b. $A(x)$ is possible, and Ø is not possible; where is Ø the null set;
c. If X_i is not possible and $X_i \subseteq X_j$ then X_j is not possible;
d. If X_i and X_j are not possible, then $X_i \cup X_j$ is not possible.

Possibility theory allows for the graduation of a many-valued logic such as fuzzy logic, rather than the classical crisp binomial logic. Fuzzy logic is compositional in respect of its union and intersection operators, whereas possibility logic is indeterminacy. For example, when a router (or firewall) is said to be vulnerable by 50% or at level of 0.5, it can be interpreted to mean the level of truth of the proposition "the router is vulnerable" is 0.5. The word "vulnerable" is a fuzzy linguistic term which describes the extent of cyber-security vulnerability with the router. That is, the linguistic term "vulnerable" has a membership function value of 0.5.

In respect of probability theory, the router is thought of as either completely "vulnerable" or "not vulnerable". The proposition "the plausibility (possibility) that the router is vulnerable is 0.5" describes a degree of belief. Here, 0.5 is interpreted to mean that the security of the router can be guaranteed 50% of the time.

Lee [148] computed the possibility of occurrence using fuzzy relations based on rules, for example. Given the fuzzy relations $R \subseteq AxB$ and $S \subseteq BxC$, such that the fuzzy sets A, B and C represent fuzzy events; e.g. the realization of attacks on a system or the occurrence of a virus infection on a system.

The possibility of occurrence is given by a fuzzy matrix relation $M_{(R,S)} \square \min(\mu_R(A), \mu_S(C))$ if there exists the possibility of occurrence R such that B occurs after A, and S such that C occurs after B [148].

This study utilizes the possibility measures to evaluate its intrinsic metrics of threat agents attacking cyber assets and exploiting existing vulnerabilities, for example. Possibility theory is used in the analysis of uncertainty in fuzziness, rather than utilizing probability which is associated with the uncertainty in randomness [46].

2.2.8. Consequence & Severity (Extent & Severity)

There are limited literature on consequence & severity in the area of cyber-security or information assurance. However, risk related literature abound in the areas of building construction and health [149] [150]. The realization of threat or cyber-attack incidents on systems could be catastrophic and require risk/impact assessment to determine the extent and severity. Impact/risk consequences are the assessment of business impact should assets be compromised, and the risks resulting from such breaches. The risk/impact severity is the quality or condition or state or intensity of the realized threat to the system.

Ayyub [151] posits that the extent of "damage inflicted by a loss is a measure of the severity". He continues that severity has uncertain measures and that it is usually defined in monetary or utility terms. Severity uncertainty is dealt with using random probability measures. Maximum Possible Loss (MPL) and Probable Maximum Loss (PML) are two (2) such measures used in assessing severity [151].

Consequences and severity are estimated using expert knowledge, or historical data, or expert guesstimate. Each cyber-attack is assigned a level of consequence and severity to compute the overall impact or risk. Cyber-attacks affecting SMEs could impact on their business operations, such as productivity loss, personnel loss, or public confidence loss, or corporate image loss or reputational damage. It is therefore difficult to assign numerical values to consequences and severity. Ayyub [151] recommends that assessing the impact of risk to a system requires using special logic based on fuzzy sets and pattern recognition.

Most contributions [152] [153] [154] [155] [156] to literature recognize the following four (4) levels of severity:

i. Catastrophic – impact caused by multiple or major system losses or failure;
ii. Critical – impact caused by single but major system loss or failure;
iii. Marginal – impact caused by minor but severe system loss or failure;
iv. Insignificant – impact caused by single minor system failure.

2.3. Cyber Threats & Vulnerabilities

The world is full of uncertainties, the information obtained from the environment, the notions used and the data resulting from observation or measurement are, in general, vague and imprecise [50]. Thus, formal description of the real world problems or some aspects of it is, in essence, only an approximation and an idealization of the actual state.

Cyber-security modeling has the same connotations as in the fields of engineering and science; that of an abstraction used for the consideration of a problem of interest. Cyber-security

models have generally been considered as an aid in analyzing security properties of interest. Bell [54] posits that a cyber-security model should have the following characteristics:

- descriptive capability – the ability to describe the situation of interest;
- general mechanism – the analytical tools to aid in the analysis of secure systems;
- specific solutions – the direct synthesis and analysis to aid in the consideration of specific systems.

2.3.1. Understanding Threats & Vulnerabilities

2.3.1.1 Vulnerabilities

By definition, cyber-security vulnerabilities are weaknesses in the systems, networks, infrastructures and applications. ISO 27005 [37] defines vulnerability as a weakness inherent within an asset or group of assets; which usually are exploited by threats agents. An asset is any resource which is value to the organization for purposes of business operations and continuity.

Vulnerabilities could be categorized into technical, human, physical, operational and business and compliance.

Technical vulnerabilities are such flaws as found in the design, implementation and/or configuration of software and/or hardware components of the systems.

Human related vulnerabilities are those associated with end-user vulnerability, gaps in awareness and training, gaps in discipline, unauthorized elevation of privileges, improper termination of access, etc.

Physical and environmental vulnerabilities are insufficient physical access controls, poor citing of equipment, inadequate temperature and humidity controls, inadequately conditioned electrical power, etc.

Operational vulnerabilities are the lack of change management, inadequate separation of duties, lack of control over software installation, lack of control over media handling and storage, lack of control over system communications, inadequate access control or weaknesses in access control procedures, inadequate recording and/or review of system activity records, inadequate control over encryption keys, inadequate reporting, handling and/or resolution of security incidents.

Business continuity and compliance vulnerabilities are the misplaced, missing or inadequate processes for appropriate management of business risks; inadequate business

continuity/contingency planning; inadequate monitoring and evaluation for compliance with governing policies and regulations.

Most vulnerability methods are "overly binary" in outlook, i.e. something is either vulnerable or it is not. This study looks at the fuzzy aspects of vulnerability so as to address necessary and possible attributes of cyber-security vulnerabilities. It must be noted that there are vulnerabilities without risk; i.e. when the affected asset has no value and, equally, when the identified vulnerability is not pertinent to that particular asset.

The attack can be active when it attempts to alter system resources or affect their operation, so it compromises *Integrity or Availability*. A "passive" attack attempts to learn or make use of information from the system but does not affect system resources, so it compromise Confidentiality.

In assessing vulnerabilities that may exist in an asset, the following attributes may be used – their Type, Source, Compromise path and Severity:

- type - a weakness in a system that can be exploited to violate the system's intended behavior relative to confidentiality, integrity and availability;
- source - vulnerabilities that are inherent in the design, operation, or operational environment of a system;
- compromise path - vulnerabilities resulting from errors of omission, error of commission, and operational errors during the life of a system;
- severity - the classification or ranking of the vulnerability due to the consequent business impact should that vulnerability be exploited.

2.3.1.2. Threats

Threats are any events or situations or actions that may cause harm or pose risk to an asset [37]. Whenever a cyber-security vulnerability or weakness in a system is exploited, a threat is said to be realized, and thus the system is said to be under cyber-attack. The entity that facilitated or caused the attack is known as a threat agent or an attacker. Some threat agents are human, such as end-users (legitimate or illegitimate, intentional or unintentional), often times called hacker or cracker. The other is nature, such as natural disasters.

Some threats may be due to threat agents such as:

- Deliberate actions by people, be they internal or external to the system;
- Accidental actions by people, be they internal or external to the system;
- System problems - hardware failures, software failures, failures of related systems, introduction of malicious code; and

- Other problems e.g. power outages, natural disasters.

Threats include unauthorized access to or use of information or assets, cyber-threats that deny, disrupt, degrade or destroy information and assets. They also include the theft of information and computer, viruses, websites defacement, denial-of-service (DoS) attacks, system penetrations, and alteration of data.

Cyber-threats come from many different sources. Wright et al [157] wrote that security threats and vulnerabilities may lead to malicious and unanticipated system behavior. Both of these security challenges impact business continuity and performance.

2.3.2. Vulnerability & Threat Analysis

Any effective cyber-security program or initiative includes performance of vulnerability and threat analyses. Hermann's [39] vulnerability and threat analyses framework entails the following:

- To select appropriate cyber-security analysis techniques ;
- To identify vulnerabilities, their type, source and severity;
- To identify threats, their type, source and likelihood; and
- To evaluate transaction paths critical to threats zones and risk exposure.

According to Johnston [158], adversarial vulnerability assessment transcends "formalistic, unimaginative, semi-quantitative, linear methods" to view the cyber-security problem from the perspective of the adversary. He emphasized that effective vulnerability assessment requires a "psychologically pre-disposed" expertise with "hands-on hacker experience" and an intrinsic psychological disposition "to think, see, and feel what the adversaries think, see, and feel". He concluded that understanding the SME's security objectives, attributes, culture, human capital and environment is imperative [158].

What techniques are used to authenticate users? For example:

i. No authentication
ii. Single factor (e.g. user ID + password)
iii. Software second factor (e.g. digital certificates + tokens)
iv. Hardware second factor (e.g. smartcards)
v. Third factor (i.e. biometrics).

A vulnerability audit is a fact-finding audit, and non-fault-finding one, which involves:

- A search for vulnerabilities through information collection and analysis; and
- A way to identify leaks, sources and indicators potentially exploitable by an adversary.

Cyber–security vulnerabilities and threats ought to be identified and some counter measure put in place to mitigate risk. The performance of vulnerability and threat analyses recognize intentional as well unintentional acts, or commissions or omissions. Hermann [39] posits that events and a series of other events could lead to different levels of compromises.

Chapter 3 Cyber-Security Metrics & Data Collection

This chapter on Cyber-security Metrics and Data Collection is about the process of measurement as much as it is about the metrics of cyber-security. The chapter presents the cyber-security metrics and data collection methods, principles and procedures employed in this research. It deals with the detailed research design for the metrics, sample selection and approaches employed to gather data for the study.

Cyber-security Metrics

Researchers collect data about the constructs being studied. Since the world is full of uncertainties, the data collected may be fraught with uncertainties in various ways [102]. For example, the researcher can only collect finite data, whereas the data of interest may be infinite. Also, the metrics used may not necessarily measure the desired constructs or the approaches and/or equipment used in data collection may be faulty, thus rendering the data inaccurate.

The question is, how do researchers ensure that the uncertainties associated with the metrics and data collection are reduced to the barest minimum? An attempt at addressing these issues is one of the contributions of this chapter.

Hayden [127] posits that cyber-security metrics involve "local[9] and tactical" elements that are largely correlated. He emphasizes that metrics should generate the needed results and that collected data through measurement must also be analyzed aimed at understanding the security posture of the organization. In essence, "measurement without analysis and action, wastes time and money and contributes to uncertainty and risk rather than reducing them" [127]. He asserts that "any empirical measurement that helps an organization to reduce uncertainty is a good metric".

It must be noted herewith that this thesis deals with the metrics of cyber-security which is intangible. Measuring cyber-security properties is not done in the same manner as a physical property is experimentally measured or observed. Cyber-security metrics and indicators are applied to assess security processes and to find the means by which the security posture can be improved and/or managed proactively. Cyber-security metrics must be aimed at effective data collection and data analysis with good understanding of its effects on security and business operations.

[9] Local here means that measurement process starts from within one's systems, networks or organization with thorough understanding.

Hayden [127] made this corollary "you cannot measure what you do not understand" to the mantra "you cannot manage what you do not measure".

The purpose of the measurement process is to transform metric data through data analysis into security knowledge to support risk decision-making; which must be inferred or referenced in respect of its sources, such as perceptions of cyber-security functionaries or perceived expert's opinions.

> *One of the contributions of this study is the extent of exposition made on cyber-security metrics. As already indicated, cyber-security is an intangible concept and so are its elements of risk, vulnerabilities and threats. This thesis endeavors to emphasize on the intrinsic properties of the confidentiality, integrity and availability (CIA) for which a model is proposed as guidance to SMEs in developing economies to assist them stay secured in today's ubiquitous and indispensable cyber environment.*

Typical cyber-security research methods involve drawing conclusions, or making inferences about metrics that have not been observed or measured on the basis of those parameters that have been observed or measured. Besides, most cyber-security endeavors lack historical data or it is difficult to measure security of a live system. So by inferential statistics, for example, one can generalize from a sample to a population of interest from which the sample was taken.

To use data to generalize findings, into areas for which there are no data, or to predict an outcome based on a limited data set, requires different techniques and analytical methods.

Statistics is categorized into two main branches [159]:

i. Descriptive statistics – involves the collection, organization, summarization and presentation of data;
ii. Inferential statistics – involves the generalizations from samples to populations, the estimation and hypothesis testing, the determination of relationships between various constructs, and the inferential decision-making, such as predictions.

Both descriptive and inferential methods are implemented in this study. Descriptive statistics method consists of two approaches: qualitative and quantitative. To sum up, this study has used the multi-method approach of both quantitative and qualitative analysis. This is necessitated by the fact that cyber-security metrics and data analysis is "purely" techno-economic; i.e. it is intrinsically "a social process as much as a technical one" [127].

The population for this study is SMEs in developing economies. In view of the obvious limitations in accessing the population, a sample of SMEs were selected from two developing

economies, i.e. Ghana and Nigeria. Strategically, Ghana and Nigeria have had economic booms spurred by the Internet developments and usage with their SMEs claimed to be the engine of growth for their economies [160] [161] [33] [162]. It is important to select the samples such that they have the same or similar characteristics as the population. *The key characteristic of SMEs in this study is the firm which uses the Internet for communications and business operations*.

Both quantitative and qualitative methods are used in this study, with emphasis on qualitative statistics.

Fundamentals of Qualitative Statistics

As quantitative statistics is associated with quantities, qualitative statistics is associated with qualities and meanings. Quality is used as a measure of relative worth or relative value [163]. This is based on the inherent attributes of what is being evaluated; called meanings – which are semantics to communicate the inherent attributes.

It must be noted that sometimes numbers can contain or communicate meanings; e.g. car tag or address of a building may be used as descriptors of quality or manipulated for convenience [163]. In essence, qualitative research uses concepts to describe data, all-be-it their characteristics or "qualities" – these are categorized to prescribe meanings to a group of objects, characteristics or attributes. Dey [163] admits that these categories used to describe qualitative data may be vague or ill-defined; they are "fuzzy" and "overlapping", but are suitable as long as they "meet" the preset objectives. Dey [163] goes on to define the categories as implicit classification of observations, which by implied contrast with other observed concepts may not be characteristic of the current observations.

Qualitative approaches are easily adaptable to the environment from which data is being collected, and can be repetitive. For instance, the analytical process can be continuously refined whilst further investigation is on-going. Qualitative research facilitates the normal measurement of constructs without necessarily tampering with the environment [164].

Variables are classified as either qualitative or quantitative. Qualitative variables are those characterized by distinct qualities or attributes. Quantitative variables on the other hand, are numerical by nature and may be in particular order or ranking [159].

Latent variables are those constructs which are not directly measured or observed, but inherently inferred from the measured variables [165]. Meyers et al [164] posit that latent variables are by nature composites of multiple observed variables, called variates, though useful, but are not directly measured or observed due to limitations in measurements. This

empirical study deals with such latent variables or multivariate data in respect of vulnerabilities whose exploitation will lead to breach of the Confidentiality, Integrity and Availability (CIA) properties.

Ritchie et al [166] posit that relatively small sampled qualitative studies can be used to draw inference about the wider population, as long as the tenets of qualitative research are adhered to. Qualitative research approaches are typically assortment of empirical investigation and creative discovery.

Qualitative data are any non-numerical data, presented in the form of linguistic or semantic terms and may be described in nominal categories in tuples, such as {very low, low, moderate, high, very high}.

Qualitative research is characterized by the following attributes:

- Naturalistic – inquiry into real world situations, rather than manipulative settings [167];
- Flexible nature of research design;
- Volume and richness of qualitative data;
- Distinctive approaches to analysis and interpretation;
- Not based on means of quantification [168];
- Grounded theoretic in nature by the analytical and interpretative manner, with the characteristics of inherent theories rather than a priori categorization [168] [167]; and
- Purposively selected samples based on preset objectives.

Qualitative research employs methods that seek to offer holistic understanding of the sampled population's perceptions of the problem of interest. Qualitative research has the capability of diversity with perspectives, which add richness to the understanding of the phenomenon of interest [167]. It is noted that qualitative and quantitative statistics complement each other, hence, the compelling reason of using both in this study.

Research Design

Research design is a process of planning and implementation in research aimed at gathering information or eliciting data on the thematic area of interest by asking questions. It includes the process of inference from the respondents' results to generalize on the population.

Research design consists of the following five processes of research; scope, questionnaire development, sampling, data collection and data analysis, as depicted in Figure 3-1.

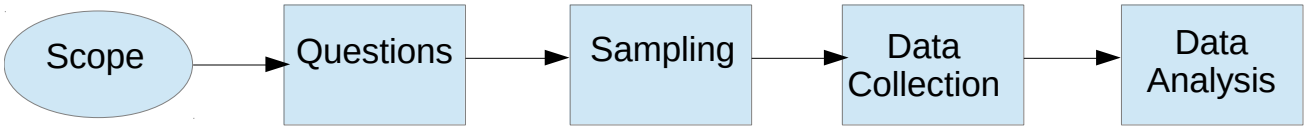


Figure 3- 1: Research Design Process

The ultimate design approach is influenced by the mode of distribution or administration (be it printed matter, email messages, or web interactions), the format of questionnaire (be it written or oral) and as well the mode of documentation, such as by hard-copy or soft-copy.

Research design is the strategic plan of a study aimed at stimulating effective and efficient manner of data collection in order to guarantee credible results [169].

The following sections discuss each of the components of the research design approach as shown in Figure 3-1.

3.1. Scope

Scope defines the processes and procedures leading to the realization of the set outcomes or objectives. The research design set off with quite extensive review of literature, primarily from academia, computer emergency response teams (CERTs) or cyber-security incident response teams (CSIRTs), security solutions providers, law enforcement agencies and other government sources.

The review detailed a broad range of cyber-security challenges confronting SMEs in developing economies. The scope involves the methodological approaches needed to carefully construct this study; and dependent upon the particular parameters in respect of the research questions raised and the objectives defined, as well as the theoretical basis and limitations of the available data. It aided in the design of the survey questionnaire as to what are the likely vulnerabilities that SMEs face in developing economies.

The review first evaluated the numerous definitions of SMEs across developing (as well as developed) economies, and adopted an appropriate definition that best suits the characteristics of the SME population of interest. Besides the criteria for the definition, one key characteristic of the sample SME was an SME that utilizes email and the Internet for business communications and operations. For example, if an SME does not have, say an email account – a very typical "brick-and-mortar" company – such SME is automatically excluded from the study's population. An associated challenge with this sample is the possibility of inactive or wrongly spelled email addresses, as the samples are selected from a pool of SME contacts.

The adoption and use of the online survey facilities was one way of ensuring that the sample was within scope.

The scope also defines the parameters of the study, including limitations, such as challenges in getting accurate data or full answers, lack of resources, time, data, equipment used and location. For instance, the www.limesurvey.com online facility required that the researcher has a web hosting account or a website, and also had to be familiar with MySQL database functionalities. These can pose some challenges to some researchers.

In view of the above, the www.surveygizmo.com online facility was adopted for the expert's opinions elicitation due to its simplicity. It does not require web hosting account and MySQL expertise. That notwithstanding, the elicitation was carried out within the trial window of 14 days; though full functionalities or solutions of the facility are available for the trial version or period. Being mindful of the limited period, the questionnaire and necessary preparatory work were carried out prior to launching the survey. This ensured that the trial period was adequately utilized to gather enough responses from the experts.

The study was targeted at cyber-security functionaries and chief-level (C-level) officers of about 500 SMEs in Ghana and Nigeria. (Based on this researcher's local knowledge and industry contacts in the two countries, about 100 respondents were expected). The survey targeted ICT-based SMEs, financial organizations and government agencies, which use the Internet for business communications and/or operations, and they were selected by a simple random sampling. Based on the respondents, 20 SMEs were identified for further strategic level interviews as expert opinions elicitation.

3.2. Designing the Research Questions

As noted in preceding sections, extensive literature review was performed to identify the state-of-the-art of the discussions and the main challenges; and that formed the basis for the design of the empirical study.

In view of the complexities and uncertainties in cyber-security metrics, the designed survey questionnaire philosophy was submitted to five cyber-security practitioners for review and comments. Based on their feedback and advice, a pre-test survey was designed and administered to those experts, again for critique. The actual full scale survey was then launched and administered using online web portal interactions from *LimeSurvey* Online (www.limesurvey.com); an approach that was aimed at reaching out to the right target sample population. *To ensure credible results, a cookie was setup in the online survey program to prevent repeated participation.*

The questionnaire were structured and mainly self-completion in nature; that is, the respondents were required to answer the questions themselves unaided (independently). The study adopted and administered a set of mixed closed and open-ended questions. Though most of the questions were the closed-ended type, in few instances it was necessary to ask for the open-ended "independent opinions" of the respondents. The closed-ended types are straight forward to complete and analyzed than the open-ended types [170].

The empirical study had a preamble and 4 thematic areas; the following briefs cover the questionnaire (c.f. detailed questionnaire is attached in Appendix – C1):

The Preamble: The Philosophy underlying the study:

ISO 27005 [37] defines vulnerability as: a weakness of an asset or group of assets that can be exploited by one or more threats; where an asset is anything that can have value to the organization, its business operations and their continuity, including information resources that support the organization's mission". Most vulnerability assessment methods are "overly binary" in outlook, i.e. something is either vulnerable or it is not. This study looks at the fuzzy aspects of vulnerability assessment so as to include necessary and possible attributes of cyber-security vulnerabilities. It must be noted that there are vulnerabilities without risk; i.e. when the affected asset has no value. Attack is active when it attempts to alter system resources or affect their operation. A "passive" attack attempts to learn or make use of information from the system but does not affect system resources, which makes it harder to detect, hence may go unnoticed; e.g. eavesdropping on a communication or conversation.

To obtain the best outcome, the questionnaire was structured in four thematic areas as follows:

Business Profile:

These set of questions sought to profile the SME businesses aimed at documenting SME products and services, and their sectors of operations, e.g. banking and finance, ISP, public sector, etc. The set of metrics gauged the level of compliance, ICT governance and ultimately, the risk impact associated with cyber-security policies and procedures.

Security Posture:

These set of metrics mainly evaluate the cyber-security threats and threat agents confronting SMEs. The metrics are meant to assess the likelihood of threats and the SMEs preparedness or otherwise in respect of susceptibility to attacks.

Assets categorization:

Assets are any entities or elements that have value. Cyber-security assets include software, hardware, human capital, information assets, such as trade secrets, intellectual property, business objectives, future business projects, employee security. It also encompasses the security of the business structure, be they tangible or intangible. It is important to classify assets appropriately in order to provide appropriate level of

protection or security based on the value, criticality, sensitivity and importance to the business. These assets or information attributes are necessary as well as the associated impacts if the information is compromised (e.g. lost, stolen, corrupted, disrupted, altered, etc.).

The following define the level of criticality, value and importance of assets:

Critical – greatest impact (with extreme disruption) on business; must be present for the business to operate;

Significant – necessary in order for the business to resume operations beyond contingency recovery stage;

Important – minimal near-term impact on business if disrupted, but essential for normal operations;

Minor – no real impact to business over the near-to-mid-term;

Very Minor – insignificant impact and considered as non-essential services.

Possibility of Occurrence:

These set of metrics assess vulnerabilities and their possibilities of being exploited by threats. The metrics also assess the extent of severity and levels of exposure to the SMEs.

The following summary are in respect of the www.surveygizmo.com online questionnaire (expert's opinions elicitation):

There was a preamble to the email with a summary of the purpose and solicitation, as well as a statement on confidentiality.

The survey first sought to profile the experts based on qualifications and experience in ICT security. Level of responsibility is also gauged aimed at ranking the experts' importance and criticality weightings.

The actual questions were matrices with strategic assets as rows and 10 threat agents as columns. The answers involved 5 multiple choice drop-down answers per asset-threat-agent mapping.

Lastly, the strategic assets were mapped with perceived criticality (impact level) and the urgency with which these assets ought to be restored, in the event of a compromise or exploitation (c.f. detailed questionnaire is attached as Appendix -C2).

The following rankings (or ratings) shall apply to the Importance or Criticality and Urgency metrics:

Table 3- 1: Experts Opinion Elicitation Rankings

Points	Criticality or Importance Ranking	Urgency Ranking
5	Critical	Restore Immediate
4	Vital	Restore Within 48 hrs.
3	Important	Restore Within 7 days
2	Minor	Restore Within 2 weeks
1	Very Minor	Restore Within 1 month

3.3. Design & Selection of Samples

This section deals with the selection of samples, sample size and its relations to producing credible and reliable results.

3.3.1. Sampling Techniques

Once the target population is defined, then a criteria or strategy is devised to survey them. However, if the population is wide and diverse, as is the case with SMEs in developing economies, a sampling process is usually used in selecting a subset, called target samples of the population. A good target sample can improve the quality of the data collected. These selection criteria define the sampling techniques employed in the study.

The essence of sampling techniques is geared towards studying a subset of the population of interest which is characteristically representative to merit appropriate generalization of the outcome [171]. This study selected the target samples of SMEs by random sampling. That is, a pool of SMEs which have access to email accounts and/or use the Internet were selected from a number of sources, such as the Ghana Internet Service Providers (ISPs) Association (GISPA), Banking institutions in Ghana and Nigeria, Nigerian Internet Exchange Association, Ministries-Municipalities & District Assemblies (MMDAs), industry associations (such as Association of Ghana Industries (AGI), Chamber of Commerce, etc.), Opportunities Industrialization Communities (OICs) and other business-related networks.

For this study a couple of sampling techniques are employed. For instance, with the main empirical survey, using the www.limesurvey.com online facility, random sampling is used in the selection of the SMEs; that is, based on chance, in view of the fact that all the SMEs sourced

are firms with access to the Internet and use emails for basic business communications and operations. On the other hand, as regards the experts opinions elicitation, using the www.surveygizmo.com online facility, deliberate sampling is used, where a few SMEs are purposively selected and interviewed (briefed on the role of the experts in the study), and followed up with a couple questions that would be evaluated for the fuzzy rule base and experts opinions aggregation.

The sample of experts for the opinion elicitation is selected by systematic sampling. First the original sample for the empirical study is revisited using their email contacts. It must noted that random samples can be selected by using either chance methods or random numbers [159]. A shortlist of 40 ICT experts is collected by random sampling; i.e. a starting point email contact is picked by closing of the eyes [159] [172] and placing the finger anywhere on the general contact list. Then, the next 39 contacts following are selected.

Using the shortlisted experts, every fourth contact is systematically selected and briefed (interviewed) via either conventional telephone or Skype. Finally, of the remainder 30 contacts, every third is selected starting from the first, thus creating a total list of 20 expert contacts. Email messages with a brief preamble and the link to www.surveygizmo.com web-based survey are sent to each expert. It is noted that a couple of the emails bounced back and so they are replaced with the next available contact.

By definition, a cluster sampling is a sample selection from an existing association or group within the population [159]. It is also noted that part of the sample in the main empirical study chosen by random sampling, is cluster sampling. For example, the AGI and GISPA are clusters within the SME population.

Finally, the sample population of SMEs are selected to meet the following criteria:

- SMEs with number of employees not exceeding 250;
- SMEs must be in Ghana and/or Nigeria;
- SMEs must use the Internet and email for business communications and operations; and
- SMEs must have at least one employee in charge of ICT or technical operations or a chief-level officer responsible for operations.

3.3.2. Sample Test Size

In view of the obvious limitations with studying the entire population, generalizing the findings from the sample to the population raises delicate concerns. One such key issue is the test of significance. According to Meyers et al [164], the test really is purported to be based on the

sample data collected, whereas in actual fact it tests "a certain hypothesis concerning the population". They assert that the null hypothesis of the population is such that:

- The sample averages are representative of the population; or
- The variables of the study have no relationship.

In other words, the alternate hypothesis is that there will be significant differences amongst given conditions, or that there is significant correlation amongst any given variables.

The other issue of concern, according to Meyers et al [164] is that of missing values in the case of multivariate data analysis (such as the case of this study). Here the argument is that when samples with the missing values and outliers are "deleted" from the data set during preprocessing, the remaining data set is actually a sub-sample which in turn affects the generalization to the population.

Visser et al. [173] found out that low response rates (RR) near 20% yield more accurate results than those of high response rates near 60% (or 70%). A statistic called the standard error of the mean measures a reflection of how far the answers are from the "truth" in terms of percentage points; and it is inversely related to the number of respondents.

A key assumption on the sample size is that it must be greater than or equal to 30; i.e. the size $n \geq 30$ or the population must be normally or approximately normally distributed, if $n < 30$. The caveat is that, non-parametric statistics does not require normal distribution [159].

The minimum acceptable sample size necessary to make accurate estimation depends on the margin of error, the population standard deviation, and the degree of confidence [159].

The formula for the sample size is derived from the margin of error; i.e.

$$E = Z_{\alpha/2}\left(\frac{\sigma}{\sqrt{n}}\right) \qquad [3\text{-}1]$$

$$\Rightarrow \quad n = \left(\frac{\sigma . Z_{\alpha/2}}{E}\right)^2 \qquad [3\text{-}2]$$

Where, $Z_{\alpha/2}$ is the critical value on the standard normal distribution such that for a significance of α, there exists a confidence interval given by $\overline{X} - Z_{\alpha/2}\left(\frac{\sigma}{\sqrt{n}}\right) < \mu < \overline{X} + Z_{\alpha/2}\left(\frac{\sigma}{\sqrt{n}}\right)$ and σ is the standard deviation, $\overline{X}$ and μ are the sample and population means respectively. Note that the concept of confidence interval is always associated with a significance α or a

confidence level (usually quoted as (1-α)%) and implying that for a given population, a number of samples taken for a particular study is likely to yield (1-α)% (e.g. 95%) of similar results.

It is noted that, in computing the sample size, the size of the population is irrelevant, when the population is large or infinite [159].

When the population standard deviation, σ, is unknown, the sample standard deviation, ***s***, is estimated and used in the computation of the sample size, n. Bluman [159] posits that using ***s*** requires that critical values greater than the values for $Z_{\alpha/2}$ are used for the reasonably acceptable confidence intervals. These values are taken from the Student *t distribution* (a.k.a. *t-distribution*).

DePaulo [174] argues that sample size matters in qualitative studies, but in a different setting. He asserts that quantitative research estimates sample size with respect to marginal sampling error, whereas qualitative studies, on the other hand, seeks to minimize the "chances of discovery failure" due to inadequate samples. He then assumed that for a random sampling qualitative study, a sample size greater than 30 can have confidence of 95% (this supports the statistical theory as stated in [159]).

A number of assumptions and propositions for sample size in a qualitative research exist. Some suggestions are for specific areas of qualitative studies, whereas others are for generic qualitative studies. For example, 15 is said to be the minimum acceptable sample size [175] and [176] as cited in [177]. Mason [177] investigated the concept of saturation with over 2500 Ph.D. Theses, amongst other factors, as a key determinant of most qualitative studies. He asserts that respondents in a qualitative study usually express divergent views. This presumes that the sample size must be large to "include" all relevant perceptions on the subject, even though too large is likely to be full of repetitions and the information rendered superfluous. Interestingly, he concluded that though the skills of the researcher can impact on the quality of data collected, the sample size per se is irrelevant compared with data quality in qualitative studies.

3.3.3. Validity

It must be noted that cyber-security metrics are used to measure constructs that cannot be directly observed. Therefore, the metrics should be well thought-through, must have theoretical basis, and must have reliability and validity. The validity of the study is measured by the representativeness of the sample population and its inclusiveness which culminates in the extent of credible results received. Validity is about the need to ensure that the metrics are

measuring the constructs intended by the study's objectives. The structure of the survey was to inform the sample population the research objectives and the framework for evaluating their responses.

In most non-parametric studies, the issue of validity is addressed by "out-of-sample" accuracy measurement [178]. Here, the dataset is divided and one part is used for the estimation of model parameters that setup the system (or model) for forecast. The other part is then used to test for accuracy or verification of the system performance. This approach is used in this study under the neuro-fuzzy system modeling using MATLAB ANFIS toolboxes (c.f. Chapters 5 & 6).

Reliability is about the need to ensure that the sample population will give the same results if the survey was repeated. A preamble to the survey is important to ensure reliability of the study.

3.3.4. Ethical Considerations

To ensure full disclosure and candid answers from the respondents, the study preamble included statements of anonymity and confidentiality in respect of participation in the study. They were also assured that responses were for academic research, though the intended findings are likely to be applicable to business and industry.

3.4. Choice of Data Collection Methods

This section gives an overview of the data collection methods used for the study.

The essence of good data collection is to assist and inform the population in making better decisions. Data can be collected through various methods. Survey happens to be one of the commonest means by which data is collected. The usual approaches may be through questionnaire distribution, or questionnaire via conventional post mail, or email, or via telephone calls, or via interviews, or via online web portal interactions.

Throughout this study, four (4) collection methods were utilized in survey or data collection. For instance,

i. Online web portal (www.limesurvey.com) is used in collecting data for this thesis, towards building a cyber-security vulnerability assessment (CSVA) model; the participants are invited to answer the questions via email messages;
ii. Online web portal (www.surveygizmo.com) is used as a follow-up in the strategic interviews conducted to elicit experts' opinions in formulating fuzzy rules and fuzzy experts opinion aggregation; the participants are invited to answer the questions via email messages;

iii. Printed questionnaire were distributed in the data gathering for the "Cyber-security: Implications on SMEs on Developing Economies – the case of Ghana" – a paper presented with the main Supervisor, at the 21st European Regional ITS conference, in September 2010, in Copenhagen, Denmark;
iv. Printed questionnaire were distributed in the data collection for the "Cyber-crime: The Mindset of Sakawa Perpetrators" – a paper that was presented at a colloquium in Ghana and is yet to be published.

Online web portal survey has wider geographical coverage; email messages vis-à-vis web portal are appropriate since all the population of ICT functionaries in SMEs have access to email and the Internet. This means that everyone has equal chance of being surveyed. Bluman [159] posits that to ensure unbiased samples, any of the four basic methods of sampling must be adhered to. They are random, systematic, stratified and cluster sampling methods.

The essence of the study is to collect credible and useful data that would be analyzed and informative inferences could be drawn from it. Though literature does not stipulate an expected minimum response rate [179], useful conclusions are likely to be drawn with more adequate data.

For cyber-security, there are 4 main data sources that can be used in analysis [127], which are:

i. System data, such as system and event logs, system configurations, etc.;
ii. Process or organizational data, such as business process diagrams, compliance monitoring, operational activities, etc.;
iii. Documentary data, such as security policies and procedures, corporate records, customer records, etc.; and
iv. People data, such as direct observations, staff meetings, surveys, training and awareness sessions, etc.

The challenge in collecting and analyzing people data is the concern on how to do it methodically and scientifically so that the results are as credible and reliable as possible [127].

3.5. Data Analysis

This is section deals with data analysis – the principles and processes involved, with specific emphasis on multivariate data analysis and fuzzy data analysis.

3.5.1. Data Analysis Principles

Upon completion of the data collection, a number of actions take place such as categorization, coding or grouping of raw data, tabulation and inferences computation.

Succinct and consistent processes and procedures in organizing survey results cannot be over-emphasized. The survey design philosophy must capture or address the mode of coding and analysis of the results.

Data analysis involves data descriptions, contextualizing and breaking down of the data into bits, thereby showing its inter-relationships and inherent concepts represented by the data [163]. Dey [163] posits that the hallmark of qualitative analysis is the emphasis it places on the perceptions attributed by observers to the same concepts or situations.

When dealing with multivariate and complex data as is the case in this study, presenting the data in pictorial (or schematic diagrams) form is useful in data analysis, and to communicate the results clearly. Intricate relationships amongst variables as well as the gaps existing amongst them can easily be revealed in diagrams. It should also facilitate systematic and logical analysis of the data [163]. The pictorial forms may be in matrices and/or maps.

For this study, matrices have been used extensively in the data analysis. For example, matrices are used for cross-tabulation of data, two-way contingency table analysis and with fuzzy cognitive maps (FCMs). Also, the FCM represents relations amongst constructs with directed graphs or di-graphs.

Dey [163] noted that categorization of concepts does not exclude other concepts per se, but only discount them, with the possibilities being included by another categorization. That is, the categories are “inclusive rather than exclusive”. This phenomenon is best understood with the fuzzy concepts of membership functions, where a member of a fuzzy set (or category) has only “inclusive” grade of membership, rather than an “exclusive” crisp binary set.

Capra [180] posits that numbers and meanings are mutually dependent or complementary; that is, in dealing with numbers (quantitative analysis) the associated meanings cannot be ignored, neither can the numbers (enumeration) be ignored in dealing with meanings (qualitative analysis). In summary, in any research, numbers are based on conceptual meanings, as conceptual meanings are informed by the numbers. Meaning is foremost in qualitative data analysis. Meaning is inspired by latent information that is discovered or uncovered or extracted during the analysis.

As part of the analysis, missing values are appropriately addressed. These are taken care off by the data preprocessing.

3.5.2. Data Pre-Processing

There are methods for pre-processing data that helps prepare them for further analysis. Principal Component Analysis (PCA) is a way of identifying patterns in data, and expressing the data in such a way as to highlight their similarities and differences. Since patterns in data can be hard to find in data of high dimension, PCA becomes a powerful tool for analyzing data [181]. PCA is used in this research as a preprocessor to prepare SME online survey data for further analysis.

This study uses the Principal Component Analysis (PCA) statistical method from the UnScrambler X.10.2. The PCA method is selected for its simplicity, ease of use and repeatability. The PCA process confirms the latent variables within the dataset as perceived by the researcher. The number of membership functions (MFs) and their positioning are guesstimated by the researcher's own insight and expertise.

The survey questionnaire consisted of over 20 items which represent more than 20 variables of interest. Since some of the variables may be measuring the same construct, for example *Confidentiality*, and so correlate with each other, by using PCA, the number of variables can be narrowed down to the 3 key latent variables of *confidentiality, integrity and availability (CIA)* without much loss of generality. The PCA identified a number of correlated patterns amongst the variables. After the preprocessing, the 3 variables are used as predictor or criterion variables in the adaptive neural fuzzy inference system (ANFIS) analysis.

3.5.3. Data Description & Exploratory Analysis

Data is analyzed to gain useful information from raw data by organizing them into descriptive statistical measures and other graphical representations.

The most common measures are the measures of central tendency, such as the average or mean, which invariably describe the general characteristics of the samples. There are other measures like those of central dispersion (e.g. standard deviation and variance) and measures of relative standing or position (e.g. percentiles), which are used to describe the samples [159].

Some of the data (especially the few quantitative ones) are analyzed and summarized by traditional statistics. For example, in analyzing some metrics under the business profile section, descriptive statistics become handy; such as the number of dedicated security positions amongst the SMEs, or the computation of annual security losses amongst the SMEs, etc.

Another statistical technique used is the exploratory data analysis, to explore the data to confirm some conjectures and to discover some aspects of the data. Multivariate non-graphical exploratory data analysis technique in the form of cross-tabulation and two-way contingency table are used as well to show some relationships existing amongst variables.

The primary purpose of exploratory data analysis is to examine data and to discover other characteristics of the data. This facilitates uncovering any mistakes in data capture and/or input, patterns or trends in data, and any deviations from any hypothesis or assumptions.

3.5.4. Model Building

Using the data to generalize findings, and to compute possible outcomes based on a limited data set, requires employing appropriate techniques and analytical methods. This study models a vulnerability assessment framework based on the empirical data collected.

The model is a relationship between the vulnerabilities in assets which can compromise the CIA properties, the threats emanating when vulnerabilities are exploited, and the resulting impact or risk to SMEs. Using user-defined fuzzy variables, a number of fuzzy rules are inferred from expert knowledge and empirical data to model the system behavior with easily described linguistic expressions.

The three vulnerabilities categories measured through the empirical study are those susceptibilities in assets that are likely to compromise the Confidentiality, Integrity and Availability (CIA) properties; these are coded from the various metrics and used as inputs into the neuro-fuzzy model. For example, a Confidentiality construct can have possible values in the quintuple fuzzy set {*very low, low, medium, high, very high*}. The MATLAB toolbox of Adaptive Neural Fuzzy Inference System (ANFIS) is used to construct the model from the empirical datasets. Fuzzy rules are extracted from numerical datasets and combined with fuzzy knowledge acquired from the experts.

A key challenge with designing any fuzzy model is to appropriately identify the variables that are suitable to describe the system abstraction of interest and parameters, which represent the extent of fuzziness in the linguistic variables. This could be carried out purely based on expert's knowledge, be it an internal expert (the researcher, in this case) or an external expert whose knowledge or judgment is usually elicited.

Branco et al [57] posit that "if the acquired information is wrong or not enough, the model will be bad." They suggested complementing expert's knowledge with a "more objective knowledge using available" empirical data collected for the system of interest.

The general approach of fuzzy modeling was as adapted from [58] as follows:

i. Define the variables of relevance, interest or importance; e.g. Confidentiality, Integrity & Availability, Threats as Input variables; and Impact as the Output variable.
ii. Define the linguistic terms; e.g. {very low, low, medium, high, very high} or {not secured, slightly secured, secured, very secured, extremely secured}.
iii. Determine the membership functions (MFs) of the linguistic terms and the positions of the tuples; e.g. trapezoidal MFs for say "very low" as [0 0 1 2] or "very high" as [8 9.5 10 10]; and triangular MFs for say "low" as [1 2.5 4] or "high" as [6 7.5 9]; for all MFs range of [0 10].
iv. Decide on the fuzzy rules; e.g. "IF Confidentiality is LOW, AND Integrity is VERY LOW, AND Availability is MEDIUM, AND Threat is HIGH, THEN Impact is HIGH".
v. Determine the fuzzy model performance by loading it with test data to verify that the system produces the expected output.

Based on the expert knowledge, the IF-THEN rules for the fuzzy inference system (FIS) are defined. Theoretically, the total number of possible outcomes from the rules is set by the multiplication of all input membership functions; in this case of 5 MFs for 4 variables, the possible outcomes will be $5^4 = 625$ rules. In practice, one would either use system generated rules or apply the expert rules (which are usually less).

Once the rules are established, the training data sets are loaded into the ANFIS, with appropriately selected optimization algorithms (e.g. back-propagation and/or hybrid methods), and a pre-set number of epochs to run. The out-of-sample accuracy measurement principle is applied to split the data sets, randomly, into 75 – 25% for training and testing data sets respectively.

First, the training data set is used, together with the fuzzy inference rules, for the construction of the model, until an optimized error level is reached. Typically, the system "learns" iteratively during the training session by finding the set of weights that produces an output which closely matches the actual output.

Then, the test data set is used to validate the generalizability or performance of the model. If the model produces a similar output, then the system is said to have been validated, and the model of interest is thus built. Otherwise, the tuning and testing iterations will go on until a desire result is achieved.

It must be noted that the problem at hand is designed as a Mamdani fuzzy inference system (FIS). However, the MATLAB ANFIS toolbox is limited by processing only Sugeno FIS or system generated from data sets. Thus, the MATLAB command of "*mam2sug*" is used to transform the Mamdani rule-based inference into Sugeno FIS before loading onto the ANFIS.

Chapter 4 Cyber-assets Vulnerability Assessment (CVA)

Cyber-assets vulnerability assessment (CVA) is a methodical course of actions aimed at evaluating the possibility or likelihood of a threat being realized against ICT assets and appraising or estimating the extent and severity of consequences on business systems.

This chapter presents the detailed methods on cyber-security metrics which were employed in assessing vulnerabilities, threats and risk/impact to SMEs in developing economies.

The objective of this chapter is to provide security best practices for SMEs to manage their cyber-security assets and to enhance business continuity. The methods are intended to assist SMEs to proactively mitigate against the potential risks due to cyber-security vulnerabilities. Often, SMEs think that they have nothing that would interest the threat agents or hackers. But, any unprotected system or asset is potentially at risk.

To ensure cyber-security, SMEs require proactive measures coupled with the right expertise that is utilized consistently to assess the security posture and business resilience of the systems. The cyber-assets vulnerability assessment (CVA) methodology commences with the appropriate review of the three (3) key parameters of cyber-risk (c.f. equation [4-4]), which are assets, vulnerabilities and threats.

One benefit of the CVA is to identify and come up with taxonomy of vulnerabilities and threats. CVA is used for risk decision making and it facilitates the identification and understanding of vulnerabilities, threats and level of impact to the SMEs assets.

Cognizance of the frequency of vulnerabilities that are identified by software vendors, and the short time interval at which cyber-security vulnerabilities are exploited, any good mitigation metrics must endeavor to minimize the windows of exposure to newly identified vulnerabilities [182].

Literatures on cyber-security assessment techniques are available, spanning different industries and sectors. But, there are limited contributions in literature on SMEs in developing economies. Similarly, the focus of existing contribution on SMEs in developing economies are not on providing an assessment methodology for understanding vulnerabilities in a holistic fashion. This may be due to the fact that very few studies have been undertaken in this area. One of the contributions of this study is by first taking a holistic approach to the assessment and accounting for the subjective, imprecise and vague aspects of vulnerabilities affecting the SMEs.

A key challenge with cyber-security measurement is that most metrics are overly binary; usually defined quantitatively. Though, it is easier to assess, compare and analyze crisp numbers and probabilities, such quantities are fraught with imprecision and vagueness in its assessment and metrics. Patriciu et al [182] posit that the metrics must be "obtainable and feasible to measure". They admitted that appropriate methodology should be applied in order to cover all dimensions of security in respect of "organizational, technical and operations, and to minimize biases as possible".

Though, Patriciu et al [182] applied quantitative probabilities in their assessment of cyber-security vulnerabilities, they inadvertently alluded to the subjective nature of the metrics. For example, their base metrics of *Confidentiality Impact* defined as "the impact on confidentiality of a successful exploit of the vulnerability on the target system, [was evaluated either as] {none, partial or complete}". This is in line with this study's metrics of fuzzy linguistics terms of "{extremely-vulnerable, very-vulnerable, vulnerable, slightly vulnerable, not-vulnerable}".

This chapter establishes the guidelines for risk assessment by first identifying and classifying the cyber assets, their characteristics and value to the SME businesses. Then, vulnerabilities that may exist in the SMEs assets are assessed based on their type, source and severity of impact. CVA evaluates the potential impacts on business operations and services, such as financial implications, compliance with industry regulations and governance. This is followed by threat identification and assessment. Finally, cyber-risk is modeled using fuzzy multi-criteria decision making techniques.

4.1 Cyber Assets

An asset is any item of economic value that usually is convertible to cash, owned by an entity, such as an individual, an organization or a society. Accountants may define assets into categories, such as current assets (e.g. cash), long term assets (e.g. buildings, plant and equipment), deferred assets (e.g. insurance, rent, interests), and intangible assets (e.g. trademarks, intellectual property (IP), patents, goodwill, etc.)[10].

Ozier [36] defined a cyber-asset or ICT asset as an embodiment of an organization needed to conduct or transact business. He distinguished between tangible and intangible ICT assets. He associated the intangibles as "true" information assets, which include information itself, data, corporate image, goodwill and reputation, intellectual property, services, software programs and applications; whereas tangibles are seen as information supportive and/or enablers, which include print-outs, end-users, hardware, storage media, machines and equipment.

[10] **www.investorwords.com/** (accessed in May, 2012)

A number of factors influence the type and strength of the security measures put in place to protect the assets. They include asset value, the extent and severity of the perceived consequences, the attractiveness (or interest in) of the assets, the vulnerabilities at stake, and organization risk tendencies or outlook.

For the purposes of this study, an ICT asset is meant to be any information, data, programs, applications, information processing resources used for media or storage, processes and transmission of the information.

4.1.1. Assets Classification

Cyber-security assessment identifies both real and possible vulnerabilities confronting the systems. Notwithstanding the metrics in use, there should be a balance in defending valuable assets so that lots of resources are not allocated to less valuable assets. It is in this vein that appropriate and accurate assets classification is imperative.

Assets classification involves the categorization or assignment of information criticality or importance labels to the ICT assets. The values assigned are usually based on the level of impact on the business upon the asset being compromised, lost, unlawfully disclosed, disrupted, corrupted, intercepted or denied access. The asset classification incorporates policies in its definitions and assignments. For example, policies such as data confidentiality policy, asset custodian or responsibilities policy, asset disposal and destruction, data handling and acceptable Internet use policies, as well as end-user security awareness programs, incorporate explicit asset classification assignments for effectiveness.

ICT assets classification must be based on business risk, asset value, sensitivity, criticality, governance and compliance requirements. For instance, a health sector SME would have to ensure adequate data confidentiality of its customer's data as per regulations like HIPAA[11] or PIPEDA[12]. Appleyard [183] posits that one of the benefits of an explicit asset classification is to enhance data usability and to ensure confidentiality, integrity and availability properties across the enterprise. This is because the organization's limited resources would have been utilized in effective protection mechanisms, instead of being "wasted" on non-critical assets.

Assets classification can enhance the operations and business output of an SME. The following are some of the important attributes of assets classification:

- To provide a framework for the use, handling and disclosure of information assets;
- To conform or comply with industry regulations and governance requirements;

[11] HIPAA stands for Health Information Portability and Accountability Act.
[12] PIPEDA stands for Personal Information Protection and Electronic Documents Act.

- To safeguard confidentiality of information from unauthorized access, use, or disclosure;
- To facilitate smooth business operations with the access, use and disclosure of information.

Appleyard [183] advocates that an organization must first have an information security policy framework in place, before an appropriate asset classification policy can be implemented. It must be perceived as an invaluable asset of the organization. Included in an effective asset classification program is the assignment of roles and responsibilities. In practice, an individual can be responsible for a number of assets, but each role must be explicitly defined. For example, an information owner is usually a senior executive who is charged with the responsibility of corporate-wide information assets. This role could also be responsible for asset classification, and it ensures that appropriate mitigation mechanisms are employed, and that the policy is periodically reviewed to ensure its currency and alignment with overall business objectives [183].

The accuracy of the asset classification forms the basis for an effective vulnerability assessment and its associated metrics. In practice, this exercise is a continuous process as new assets are added throughout the lifetime of the business.

Another benefit of assets classification is to facilitate and establish the business value of each asset, which can be used in designing commensurate mitigation plans. The degree of protection associated with a particular asset is evaluated through proper cyber-asset classification.

This study distinguished between government and private sector asset classification schemes are classified as follows:

i. Private sector information:
   - Public – information, usually made available to all stakeholders, that can be used, divulged or disclosed in public domain without harm and adverse impact on the business and/or its stakeholders;
   - Private – information restricted to internal use on “need-to-know” basis, but that cannot be divulged or disclosed into public domain, and has the possibility to hurt or harm the organization and/or its stakeholders in the event of such disclosure;
   - Sensitive – information that is sensitive to the organization, usually made available based on specific roles and responsibilities, and requiring careful handling, with the possibility of adverse impact on the business and/or its stakeholders upon compromise;

- Confidential – information that is highly sensitive to the organization and/or its stakeholders, and requiring "restricted" observation, with the possibility of major adverse impact on the business and/or its stakeholders upon compromise.

ii. Government sector information are usually that maintained in confidence in order to protect national security:

- Unclassified – information that has significant doubt on its impact in the event of a compromise;
- Restricted – information restricted to internal use on "need-to-know" basis, but that cannot be divulged or disclosed into public domain, and has the possibility to hurt or cause harm to its government in the event of such disclosure;
- Confidential – information, the unauthorized disclosure of which could result in damage to the national security
- Secret – information, the unauthorized disclosure of which could result in a serious damage to the national security
- Top Secret– information, the unauthorized disclosure of which could result in a major catastrophe or damage to the national security, and bilateral instability between nations.

Information is classified based on a number of factors, including stakeholder's experiences, value of information to the SME, governing laws and regulation. The utility of the asset classification is applied in the expert's opinion elicitation of this research.

4.1.1.1. Assets Identification

Assets identification involves assessment of the assets and their criticality to the organization. Apart from assisting in physical inventory of assets, assets identification facilitates the valuation of the assets. Each asset is identified based on its importance and then labeled or tagged. Next, the purchased price or acquisition cost is recorded before applying the appropriate depreciating rules to estimate the asset value.

In today's ubiquitous business world, some stakeholders (e.g. sales force, field engineers, vendors and consultants) use corporate assets remotely. This places enormous responsibility on the organization as remote access poses one of the most vulnerable points on the security chain. It also implies that lots of corporate information and data are external to the premises of the organization. Assets identification can facilitate the proper accounting for these assets. For example, the value placed on a Remote Access Dial-In User server (RADIUS) may be more than the cost of the server alone.

4.1.1.2. Assets Criteria & Characteristics

According to [24] assets have attributes used in its characterization, in the form of elements and properties, as well as interactions with other related assets. Ye [24] posits that different assets have different attributes and are categorized differently.

ICT assets can be categorized into resources, processes and end-users. These include software, hardware, human capital, information assets, such as trade secrets, intellectual property, business objectives, future business projects, employee security. It also encompasses the security of the business structure, be they tangible or intangible. It is important to classify assets appropriately in order to provide proportionate level of protection or security based on the value, criticality, sensitivity and importance to the business. These assets attributes are necessary as well as the associated impacts if the information is compromised (e.g. lost, stolen, corrupted, disrupted, altered, etc.).

Upon asset classification, the next task it to categorize the assets into levels of impact and/or extent of severity should the asset be compromised. In this study assets are characterized as {critical, vital, important, minor, or very minor}. In practice, these characteristics depend upon the nature of business engaged by the entity in question. For instance, the notebooks used by the sales force could be classified as important, whereas applications or programs used for direct production or income generation would be classified as critical to the business.

The assets classification framework stipulates various criteria for safeguarding the ICT assets [24]. For example, labeling of ICT assets; email containing confidential must be labeled "confidential" in, say, the subject line. The criteria used for the assets classification must take into consideration the CIA triad properties as well as the assets value.

The following define the level of criticality, value and importance of assets:

- Critical – greatest impact (with extreme disruption) on business; must be present for the business to operate;
- Vital – necessary in order for the business to resume operations beyond contingency recovery stage;
- Important – minimal near-term impact on business if disrupted, but essential for normal operations;
- Minor – no real impact to business over the near-to-mid-term; and
- Very Minor – insignificant impact and considered as non-essential services.

4.1.2. Assets Value

This sub-section introduces the concepts of criticality in classifying the ICT assets. Paul Garvey [184] lends a hand with the concepts of value, utility and risk functions used in decision analysis to rank assets amongst a set of competing options.

Garvey [184] defined a value function as "a real-valued mathematical function defined over an evaluation criterion (or attribute) that represents an option's measure of "goodness" over the levels of the criterion. A measure of goodness reflects a decision-maker's judged value in the performance of an option across the levels of a criterion (or attribute)".

A value function, $V(x_i) \in [0,1]; \forall i = 1, 2, \ldots\ldots, n$ where x is a criterion and n is the number of options being evaluated. Practically, $V(x_i) = 0,$ if $i = 1;$ i.e. x_1 is the least preferred criterion level; and $V(x_i) = 1,$ if $i = n;$ i.e. x_n is the most preferred criterion level.

There are various approaches employed in the application of value functions, such as value increment approach, direct preference rating approach, and exponential value functions [184].

It must be noted that the value function does not make any references to uncertainty measures. In other words, it assumes that each of the criteria is deterministic. Garvey [184] noted that the value function alone is applicable to decisions in which there's certainty amongst the competing alternatives or options. However, most real world problems are fraught with uncertainties. So, the use of utility and risk functions are explored, in addition to the value function. Asset value of certain types may be estimated by quantitative assessment using value function or direct financial value (e.g. operating license, patent, or design) or any asset "bought" on the market or by using the production value [185]. Most ICT assets may be difficult to estimate by the value function alone, even if the contributing effect is clear. The asset value may be derived from the asset's importance to the organization.

M'Pherson [186] defines value as a measure assigned by an expert or observer in respect of an object's or asset's qualities such as purpose, pleasure and ideals. He further defined monetary value as a perceived value with an agreed monetary indicator in a given time.

The asset value of a given ICT resource is, by extension, a measure or degree of its importance to the organization [187]. According to Fisch & White [187] the asset value is a function of its cost, time required for its maintenance and administration, its sensitivity and criticality to the organization. In practice, it may be very difficult to estimate the asset value of data, for example, and so the time value (which is utility value) required to restore a corrupted data may be used instead.

The asset value can be evaluated based on the CIA triad [187]. Here, the confidentiality gives an indication of the asset's confidentiality or privacy requirements; the Integrity gives an indication of the asset's trust and accuracy; whereas the availability indicates the asset's requirement of continuous functionality or accessibility.

Algebraically, the Asset value, A_v, is given by the value and utility (disutilities) function

$$A_v = \sum(Confidentiality, Integrity, Availability) \quad [4\text{-}1]$$

i.e. the summation of the contributing values of the CIA parameters. It is noted that each of the parameters is proportional to the asset value, such that a higher ranking of a property, is a positive indication of the degree of importance or higher asset value. For accuracy in asset valuation per equation [4-1], the rankings of the parameters must be of the same scale or normalized values.

The asset value has positive correlation with the impact on SMEs. The impacts in turn are reflections of revenue loss, financial loss, cost, loss of investor and customer confidence, loss of reputation and possible lawsuits.

4.2. Vulnerability Assessment

4.2.1. Vulnerabilities

Vulnerability has been well defined in ISO 27005 [37] as a weakness inherent within an asset or group of assets. Cyber-security vulnerabilities are weaknesses in the systems, networks, infrastructures and applications. Vulnerabilities are the weaknesses in systems or the susceptibility of the systems to attacks.

Vulnerability is said to be a weakness that can be exploited by a threat agent to compromise a security property or pose a threat to the system or asset [4]. Vulnerabilities are evaluated by carefully assessing the possible exposures upon exploitation and by estimating the effects of multiple and sequential incidents.

Within the context of this study on cyber-security, *vulnerability is defined as*

> *a flaw or weakness inherent within the system that can be exploited to compromise the system's objectives in respect of information technology, information systems, associated communications networks and systems, and the business processes*.

Vulnerabilities can be categorized into technical, human, physical, operational and business weaknesses [38].

- Technical vulnerabilities are the weaknesses inherent in the design, implementation and/or configuration of system elements, such as applications, software and hardware.
- Human related vulnerabilities are the weaknesses associated with end-user vulnerability, gaps in awareness and training, gaps in discipline, unauthorized elevation of privileges, improper termination of access, etc.
- Physical and environmental vulnerabilities are weaknesses such as insufficient physical access controls, poor citing of equipment (e.g. on the ground floor of a building in flood prone area), inadequate temperature and humidity controls, inadequately conditioned electrical power (no uninterruptible power supply (UPS)), etc.
- Operational vulnerabilities are the weaknesses due to ineffective separation of duties (SoD), ineffectual monitoring, ineffective logging systems, lack of change management, lack of control over software installation, lack of control over media handling and storage, lack of control over system communications, inadequate access control or weaknesses in access control procedures, inadequate control over encryption keys, inadequate reporting, handling and/or resolution of security incidents.
- Business continuity and compliance vulnerabilities are the misplaced, missing or inadequate processes for appropriate management of business risks; inadequate business continuity/contingency planning; inadequate monitoring and evaluation for compliance with governing policies and regulations.

In this study, these vulnerabilities metrics were measured from the empirical survey under the security posture, critical assets and possibility of occurrence sets of questions. The fuzzy aspects of these vulnerabilities were utilized to address the necessary and possible attributes of the CIA security properties.

4.2.2. Vulnerabilities: Source, Type & Severity

Hermann [39] classified vulnerabilities into three (3) categories, namely Type, Source & Severity and defined them as follows:

- Type: refers to how the vulnerability is manifested; be it intentional, unintentional, omission, or commission;
- Source: refers to the mode by which the vulnerability is exploited; be it direct or indirect, active or passive in respect of the threat agent's involvement;
- Severity: refers to the extent of impact upon the exploitation of the vulnerability or upon the realization of the threat; be it of critical, vital, major or insignificance.

The empirical study on vulnerabilities took cognizance of those attributes in the design and evaluation of the metrics based on the following:

- a weakness in a system may be exploited to violate the system's intended behavior relative to confidentiality, integrity and availability;
- vulnerabilities are inherent in the design, operation, or operational environment of a system;
- vulnerabilities may result from errors of omission, error of commission, and operational errors during the life of a system.

4.2.3. Evaluation of Vulnerabilities

Threat agents succeed in their attacks to assets, which often times cause adverse impacts whenever the assets are vulnerable or susceptible. Vulnerability types, source and severity are taken into consideration in vulnerability assessment. The aim of an effective vulnerability assessment is to ensure that the identified critical assets are adequately protected. Proactive prevention and detection techniques are put in place to minimize the susceptibility of vulnerabilities.

This study sought the expert opinions of cyber-security functionaries on vulnerability metrics used in this research. The experts assessed the vulnerabilities of their SMEs systems by rating perceived critical assets as either vulnerable or not vulnerable, using the quintuple {Extremely-Vulnerable, Highly-Vulnerable, Vulnerable, Slightly-Vulnerable, Not-Vulnerable}. The study also impact on the assets upon compromise or breach, using the quintuple {Very-Minor, Minor, Important, Vital, Critical}.

It must be noted that threats and vulnerabilities are two (2) fundamental challenges confronting SMEs today. These challenges are characterized as being "unavoidable – present in most assets", and "increasing – growing incidents" [65]. Since vulnerabilities in assets cannot be completely avoided, it is imperative to appropriately mitigate the risks [65]. Seacord & Householder [66] argued that understanding vulnerabilities is critical to understanding the threats they represent.

4.3 Threat Assessment

4.3.1. Threats

Threats are any events or situations or actions that may cause harm or pose risk to an asset. Whenever a cyber-security vulnerability or weakness in a system is exploited, a threat is said to be realized, and thus the system is said to be under cyber-attack. The entity that facilitated or caused the attack is known as a threat agent or an attacker. Some threat agents are human, such as end-users, whose actions may be deliberate or intentional, accidental or unintentional, may emanate from internal or external sources to the system; or it may be due to system

problems, such as hardware failures, software failures, failures of related systems, malicious codes like worms, viruses and Trojan horse; and other environmental problems, such as power outages, natural disasters, etc.

The study was designed in conformity with the above notions of threats. Diverse metrics were used including unauthorized access to or use of information assets, cyber-attacks that deny, disrupt, degrade or destroy information assets. Also measured were issues relating to the theft of information, laptop or PCs, viruses, websites defacement, denial-of-service (DoS) attacks, system penetrations, and alteration of data.

Indeed, cyber-threats come from many different sources; which could be malicious or due to unanticipated system behavior [157]. Either of these security challenges could impact heavily on business continuity and performance.

Threat assessment is a step-by-step comprehensive review, identification and prioritization of potential threats to ascertain the possibility and severity when it happens. A significant challenge of threat assessment is that the information available or used for the evaluation is often times vague, imprecise or non-specific [4].

Vidalis & Jones [40] in claimed that a number of factors give rise to threat realization. Their definition of threat can be estimated as a fuzzy function; i.e.

$$Threat \sim f(\text{Motivation, Capability, Opportunity, Impact}) \qquad [4\text{-}2]$$

where

- Motivation is the degree to which a threat agent is prepared to implement a threat; e.g. {attributed motivational factors such as personal, individualistic challenges, including extreme advocacy – espionage & terrorism, monetary};
- Capability is the degree to which a threat agent is able to implement a threat; e.g. {availability of tools and necessary skillset to use the tools};
- Opportunity is the ease with which the target is vulnerable or the degree of susceptibility in order to utilize the capabilities and make the intended impact;
- Impact is the resultant effect or output upon threat realization [40].

It must be noted that the extent and severity of the impact is very relative. For example, the loss of a network address translation (NAT) server to an ISP may be catastrophic, but probably to a marketing consulting SME, the effect may be just minor. This is why it is important that every organization carries out a business impact assessment to determine and assign business impacts to systems.

4.3.1. Threat Agents Identification & Classification

A threat can be identified as the possibility to cause harm or the capability to cause harm with reasonable opportunity and intent. Threats agents or sources in cyber-security are many, such as:

- criminal hackers (crackers) who are skillful and have the motivation to break into someone's system;
- a hacker who deliberately hacks into a corporate network to steal intellectual property;
- an amateur techie who inadvertently misconfigured a server or a firewall;
- a disgruntled ex-employee who seeks revenge;
- a nation-state espionage activities on another;
- an innocent end-user who inadvertently opens an un-scanned email attachment; etc.

In the normal course of operations, threats may be identified when system activities "change". For instance, sudden system crashes or slow processing of browser requests, or the presence of unusual filenames and/or extensions, and so on.

Threat agents are classified based on locality to the assets, such as internal (as insiders) and external (as outsiders). Though some outsiders could pose a very high risk to the system, the risks posed by insiders are particularly severe.

By definition, an insider is an authorized entity or end-user of the resource or asset, who can pose a threat to the system. By virtue of the permissive accessibility, they can use their training and knowledge of the system (or the lack of it), coupled with deception or dissatisfaction (e.g. disgruntled end-user) within the system to facilitate an attack against the system.

Vidalis & Jones [40] were not particularly enthused about the distinction between insiders and outsiders. Rather, they admonished that once a threat agent has been identified (and recorded), it must not be down played or deleted. They focused on the status attributes of threat agents as being either {active, inactive, dormant or dead}. Threat agents are said to "mutate over time, acquiring new capabilities" [40].

The study was designed based in part on Hermann's [39] classification of threats by Type, Source and Likelihood as follows:

- Type: - refers to the kind of action that can trigger the threat;
- Source: - refers to the nature of action that can trigger the threat;
- Likelihood: - refers to the possibility of occurrence of the threat.

4.3.2. Assets Attractiveness

Threat assessment is a systematic process used to evaluate the possibility of an attack against a given asset or group of assets. It is a decision analysis technique aimed at identifying threats and prioritizing resources allocation to mitigate possible risk. Pedrycz & Gomide [42] posited that a threat assessment is a process of evaluating the possibility of attacks against an asset or resource. Its purpose is to identify and prioritize threats based on attributes such as the motivation or intent, capability, opportunity and extent of impact (or attractiveness of the asset) [42]. It also involves evaluating historical data, if available, to appraise an indication of possibility of a missed or undetected attack. The threats identified are used to form a baseline or benchmark for the SMEs. The study was designed based in part on the threat assessment processes as follows:

i. To identify known and potential threat agents;
ii. To appraise the motivation, capability, opportunity and severity of threat agents as metrics against assets;
iii. To evaluate threats in respect of their possibility of maturity and attractiveness to the threat agents.

4.4 Cyber-Risk & Impact Assessment

This section evaluates risk and impact upon realization of threats, and also estimates the possibility or maturity of attacks through exploitation of vulnerabilities by threat.

4.4.1. Risk Defined

Studies have defined risk in a number of ways. With regards to cyber-risk, different treatments have been offered in the literature [43] [188] [189] [44].

Cyber-risk is said to be the possibility of losses due compromises of confidentiality, integrity and availability of computer systems and associated data contained therein [43]. Other definitions, and in particular Viehlandm [190], emphasize on risk as the impact on business operations, productivity, corporate image, etc., in the event of compromises on the systems.

Traditional risk theoretic estimates risk as the likelihood of a threat realized or a successful attack against the system or an asset. This notion presumes the randomness of attacks as events and the risk is usually given by a probability product (based on Cartesian product); i.e.

$$Risk = P_i \otimes C_j$$

where P_i are the probabilities of occurrence; C_j are the consequences of the attack, give as a dimenionless variable. [4-3]

Evaluation of risk based the above approach can lead to situations where there are no risks to valuable ICT assets; thus, leading to an erroneous and potentially misleading evaluation [4]. To cure this potential anomaly, the department of Homeland Security (DHS) [4] recognizes that uncertainties in risk assessment may exist. In view of that, the DHS defined risk as follows:

> "*Risk is an expression of the likelihood that a defined threat will target and successfully exploit a specific vulnerability of an asset and cause a given set of consequences"* [4].

The DHS [4] argues that cyber-risk may be best assessed and estimated qualitatively. So, the use of consensus expert opinions or judgment on the possibilities and possible consequences upon realization of the threats are recommended.

This study takes a view of cyber-risk and defines as:

> *the possibility of the occurrence or realization of a threat, due to compromises of the confidentiality, integrity and availability (CIA) of the system and the associated adverse impact on business.*

The study employs fuzzy set theoretic techniques to evaluate the cyber-risk. This application is highly subjective and its treatment takes into account the imprecise and vagueness of cyber-risk metrics [44].

A number of studies have employed fuzzy set theory in risk analysis, such as [44] [18] [189] [191] [9] [192].

For this study, cyber-risk is mathematically given by the fuzzy relational function, as previously defined in equation [1-4] in chapter 1 of this thesis; thus:

$$Risk_{\text{threat}} \square f(\text{Threat}_{\text{asset}}, \text{Vulnerability}_{threat}, \text{Asset Value}) \qquad [4\text{-}4]$$

where the fuzzy arguments are $Threat_{asset}$, $Vu\ln erability_{threat}$ and Asset Value.

It follows that, a higher asset value, a higher vulnerability value, and/or a higher threat value lead to a higher risk value [24]. To assess security risks of a computer and network system, the value of each asset is evaluated for the importance of the asset, and vulnerabilities and threats which may cause damage or loss of asset values are also examined. An asset may have more than one vulnerability. A vulnerability may be exploitable in multiple ways through multiple forms of applicable threats.

M'Pherson [186] posits that combining value and utility functions, requires the expression of both metrics in the "same units within a logically proper combinatory space". Using M'Pherson's [186] approach for estimating the business value modeling (BVM), the risk

function can be expressed as the combined value of threat and vulnerability utility functions, the relative values of assets and a given combinatorial fuzzy linguistic rule that specifies the logic combining the value and utility functions.

This study adopted the approach used by [44], which was also supported by [193] [194] [195]. The approach is as follows:

i. Carry out risk identification;
ii. Perform fuzzification of risk constructs;
iii. Use fuzzy risk assessment and aggregation;
iv. Perform fuzzy weighted mean computation; and
v. Perform defuzzification.

This approach culminates into a cyber-security vulnerability assessment (CSVA) model, which will assist decision-makers on available risk options. The essence of the CSVA model is to offer SME decision makers a plausible and pragmatic approach to assessing risks against ICT assets. Kaplan & Garrick [112] posited that determining risk amounts to addressing the following questions:

- What could go wrong?
- How many times does it go wrong?
- What is the impact on the organization? Or what are the consequences?

The answer to the first question could be interpreted as the assets being compromised. The second question requires the evaluation of the possibility of occurrences of these threats. The third question estimates the extent and severity of consequences or the impact level of the risk as result of the exploited vulnerabilities.

4.4.2. Risk Identification

Risk identification deals with the question "what can possibly go wrong?" It involves identifying which risks could impact the business significantly as well as determine their characteristics. Risk identification is said to be highly subjective and may be iterative in nature [106].

Here, the key constructs of threats and vulnerabilities are identified and enumerated. For example, threats were compiled from the "Possibility of Occurrence" section of the survey, whilst vulnerabilities were assessed from the "Security Posture" section.

For each of the categories, the constructs were sub-divided based on whether the compromise was a breach to confidentiality or integrity or availability. Exploratory analysis was carried out on the data to classify them, indicating their contributing factors per each metric.

4.4.3. Fuzzification

As indicated earlier, traditional risk analysis estimates the likelihood of occurrences or probabilities and the severity of consequences as a probability product [c.f. equation 4-2].

The extent and severity of an impact was measured by the susceptibility of the assets or systems. That is the impact due to vulnerabilities and threats indicated by the quintuple {VeryMinor, Minor, Important, Vital, Critical}.

Similarly, the vulnerabilities and threats components were measured and indicated by the quintuples {Extremely-Vulnerable, Very-Vulnerable, Vulnerable, Slightly-Vulnerable, Not-Vulnerable} and {Very-Low, Low, Medium, High, Very-High} respectively.

For simplicity, fuzzy triangular membership functions were used for all fuzzy linguistic terms. These are depicted in Figures 4-1, 4-2 & 4-3 below.

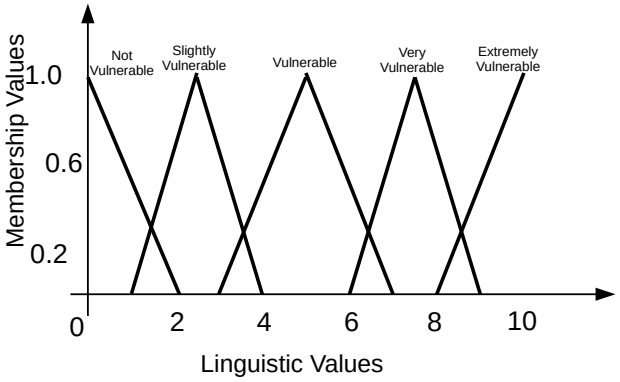


Figure 4- 1: Vulnerabilities

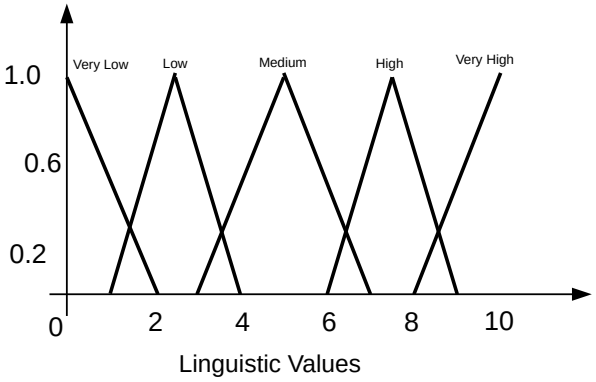


Figure 4- 2: Threats

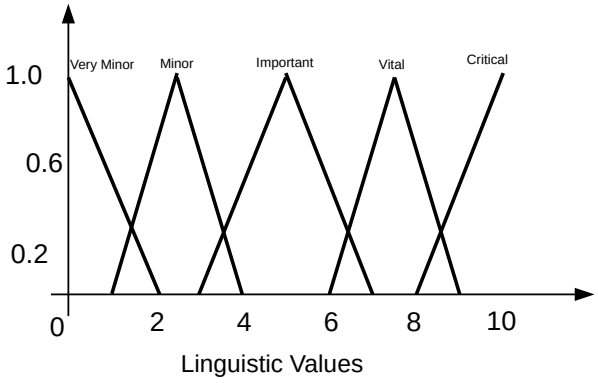


Figure 4- 3: Critical Assets

4.4.4. Fuzzy Risk Assessment & Aggregation

Expert opinions of cyber-security functionaries and chief-level officers of SMEs in developing economies were elicited for the survey. By aggregating their opinions (or responses), "a more objective and unbiased result can be obtained" [44].

Following Ngai & Wat [44] and Bojadziev & Bojadziev [196] examples, the fuzzy triangular average formula is used to aggregate the expert opinions. That is, given n experts (or respondents) with corresponding fuzzy triangular numbers, $x_i = (x_l^i, x_m^i, x_h^i)$ where $i = 1,2,.....,n$; and x_l is the lowest value of support value of x; x_h is the highest value of support of x; and x_m is the middle or modal value of the triangle. Then, the fuzzy triangular mean or fuzzy arithmetic mean [63] is given by

$$\begin{aligned}\overline{X} &= \frac{X_1 + X_2 + ... + X_n}{n} \\ &= \frac{(x_l^1, x_m^1, x_h^1) + (x_l^2, x_m^2, x_h^2) + ... + (x_l^n, x_m^n, x_h^n)}{n} \\ &= \overline{X_l}, \overline{X_m}, \overline{X_h} \\ &= \left(\frac{1}{n}\sum_{i=1}^{n} x_l^i,\ \frac{1}{n}\sum_{i=1}^{n} x_m^i,\ \frac{1}{n}\sum_{i=1}^{n} x_h^i\right)\end{aligned} \qquad [4\text{-}5]$$

4.4.5. Fuzzy Weighted Mean Calculation

Statistically, averages are computed in one of two ways, the mean value and the weighted mean value. The mean is used whenever the data has no frequencies or counts; otherwise, the weighted mean is used. The weighted mean is the ratio of the total data values multiplied by the respective frequencies, to the total frequencies.

Mathematically, the weighted mean or the "importance" weighted arithmetic mean (WAM) [63] is given by

$$\overline{X} = \frac{\sum_{i=1}^{n} W_i . C_i}{\sum_{i=1}^{n} W_i} \qquad [4\text{-}6]$$

where

W_i are the weights assigned to compromised assets or measures of relative importance of assets; it is noted herein that the W_i's are normalized fuzzy weights, which address the

uncertainties with partial fuzzy evaluations [197]; practically, these could be simply deduced from the relative frequencies of the choices made by experts with regards to a given criteria or set of attributes;

C_i are the compromises of vulnerabilities exploited by threats.

By extension, the fuzzy weighted mean (FWM) with respect to the fuzzy sets $\mathbf{W}_i$ and $\mathbf{C}_i$ is given by

$$\overline{\mathbf{X}} = \frac{\sum_{i=1}^{n} \mathbf{W}_i.\mathbf{C}_i}{\sum_{i=1}^{n} \mathbf{W}_i}; \ \exists \ \mathbf{W}_i, \mathbf{C}_i \in \left[0,1\right], \mathrm{i} = 1,2, ..., \mathrm{n}. \qquad [4\text{-}7]$$

Again [44], [198], [193], [199], [200], [197] are amongst a number of studies employing FWM to risk and/or multi-criteria decision making models.

4.4.6. Defuzzification

Upon calculating the fuzzified weighted mean, the resultant fuzzy set has to be converted into a crisp set (or value) that has appropriate interpretation or meaning in the real world. In essence, the fuzzified cyber-risk decision has to be applicable decision criteria. This process of conversion from fuzzy set to the crisp set is known as Defuzzification.

By definition, Defuzzification is the process of mapping the resulting fuzzy output into a crisp set. The results of the inference process are converted from fuzzy linguistic variables to crisp values, for meaningful analysis or interpretations.

A number of defuzzification methods exist in literature and/or in applications, such as center of gravity (or Centroid), mean of maxima, basic defuzzification distribution (BADD), bisector, [201], [202], [203]. The Centroid method is the most commonly used, but requires enormous computation power. The choice of a defuzzification method is highly dependent upon the attributes of the application [201]. Hellerdoorn & Thomas [204] provide a number of defuzzification criteria, such as continuity, dis-ambiguity, plausibility, computational simplicity, all of which are dependent on the type of problem being solved.

For example, the maxima method or mean of maximum (MoM) evaluates the mean of all maximum values as the defuzzified crisp value. The disadvantage is that, certain maxima may dominate the evaluation, thus skewing the results.

This study utilizes the weighted mean defuzzifier for simplicity and problem application. Here, the defuzzified weighted mean is computed from the maximum membership values of the output fuzzy set(s) [205]. That is, defuzzifier weighted mean

$$\bar{\mathbf{Z}} = \frac{\sum_{i=1}^{n} \mu_z(z_i).\overline{\mathbf{z}_i}}{\sum_{i=1}^{n} \mu_z(z_i)} \qquad [4\text{-}8]$$

Consider, for example, the fuzzy triangular output set depicted in Figure 4-4.

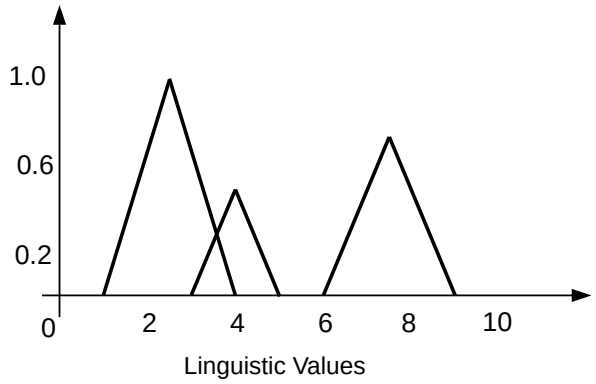


Figure 4- 4: Output Fuzzy Set

Then the defuzzified weighted mean is given by

$$\bar{\mathbf{Z}} = \frac{(1.0 * 2.5 + 0.5 * 4.0 + 0.75 * 7.5)}{(1.0 + 0.5 + 0.75)} \qquad [4\text{-}9]$$

$$= \frac{2.5 + 2.0 + 5.625}{2.25} = \frac{10.125}{2.25} = 4.5$$

4.4.7. Risk Assessment Modeling

Risk assessment is the process of identifying both actual and potential (perceived) threats to the ICT assets, and to determine the possibility of occurrence and associated impact. It must evaluate the threats and vulnerabilities to the assets, possible consequences on business operations and performance, and prioritizes the measures needed to mitigate the possibility of compromises to the CIA security properties. Risk assessment provides the metrics in estimating the threats to the assets, the vulnerabilities of the assets, and the extent and severity should vulnerabilities be exploited.

Risk management is a corporate decision-making process. It involves the evaluation of consequences, resulting from threats and vulnerabilities and in addition to protection. Looking at risk from the decision science perspective, risk can be deemed as a single-criterion or a multi-criteria decision-making. This study involves multi-criteria attributes.

Multi-criteria decision-making (MCDM) techniques can be categorized into multi-attribute decision-making (MADM) and multi-objective decision-making (MODM).

In MODM, a predefined or pre-determined mathematical model is identified for the problem. Each option is subjected to the model, and evaluated of its test "performance" (or "satisfaction") in respect of an objective or multiple objectives.

MADM, on the other hand, chooses the decision criteria based on their attributes, usually involving sorting and ranking. Some commonly used techniques of MADM are fuzzy Analytic Hierarchy Process (AHP), fuzzy TOPSIS, fuzzy out-ranking methods, fuzzy similarity measures and fuzzy weighting methods [206].

This study on cyber-security vulnerabilities with SMEs involves evaluating multiple criteria of threats, vulnerabilities and asset values. Multi-attribute utility functions were therefore explored especially in evaluating asset values.

The multi-attribute utility function [62] consists of two (2) key concepts. i.e.

- The multiplicative complement measure, which complements each construct in the form of an AND condition or ANDness [63]; and
- The implicative compensate measure, which compensates for each construct in the form of an OR condition or ORness [63].

Meyers et al. [62] posited that there is a third category of the multi-attribute utility function called the additive utility function. This is a special case of both complementary and compensatory utility functions.

In evaluating risk with equation [4-4] above, two key functions are computed. The asset value is computed by the value function, whereas the utility values of both vulnerabilities and threats are computed by the utility function.

Using utility theory applications to evaluate vulnerabilities and threats, a low utility value of say, 0.20, indicates a high vulnerability of an asset, whereas a high utility value of say, 0.90, indicates that the asset is less vulnerable. This is made possible because the risk function is dimensionless.

The risky characteristics of ICT assets can be modeled by the concept of fuzzy utility functions. The fuzzy utility functions have the following attributes:

- Objective factors – tangible, e.g. physical security, hardware;
- Subjective factors – intangible, e.g. interests, preferences, goodwill;
- Susceptibility function is a fuzzy concept which describes the risk attributes or variables appropriate for evaluating the various attributes of susceptibility, such as {Very-Minor, Minor, Important, Vital, Critical}.

Given a utility function $U(x)$ of consequences of successful attacks; then for possible consequences x_1 and x_2, $U(x_1) > U(x_2)$, if and only if x_1 consequence is preferred to x_2 consequence. In cyber-security, the risk is evaluated as a detrimental consequence or negative impact on cyber-assets or ICT systems; i.e. the risks involve "*disutilities*" [189].

Assume U_i is a fuzzy utility function, and X_i as any linguistic variable for susceptibility, then

$$U_i : X_i \to U_i; \exists\ U_i \to 1\ \forall X_i \to \infty, \text{ and } U_i \to 0\ \forall X_i = 0.$$

For example, the asset value of a system could be $A_v = 1$ if the estimated compromised cost is say \$100K, in comparison with compromises estimated at \$1000; then \$100K is far greater than \$1000 (i.e. \$100K ≫\$1000).

4.4. 8. Modeling Risk & Impact

Business impact assessment is a process aimed at evaluating the extent of tolerance or operational continuity in the event the business suffers substantial loss or consequences.

As part of the CSVA initiative, SMEs can stipulate appropriate policies to protect the confidentiality, integrity and availability of all ICT assets. ICT assets are invaluable to SMEs and it is paramount to ensure that information is not compromised or lost or corrupted. The information assets are usually sensitive and thus require adequate and appropriate protection.

Cyber-security policies are to ensure that appropriate access to ICT assets are granted to only authorized entities on the principle of the need-to-know basis, role based access and least privilege, such as end-users, vendors, contractors, consultants, processors and systems. These initiatives include measures to deter, detect, prevent, preserve, and at the least, minimize, malicious and unauthorized access and usage.

Cyber-security policies are meant to ensure business continuity. They stipulate the rules and procedures used in ICT assets gathering, dissemination, distribution, processing, storage and transmission. The policy frameworks also ensure that firms adhered to best practices and complied with laid down regulations and laws.

Applications of decision theoretic models and measurement methods to solve real world problems date as far as the 1930s [189] [207]. Since then, there have been desire towards applying preference and value metrics to problems which were traditionally dominated with probability treatment.

A multi-criteria decision problem generally involves making a choice amongst a number of options or alternatives based on a predefined objective or criteria or attribute. These attributes or criteria are usually rated or ranked based on level of relative importance or relative weight or contributing factors or influence, and they are aggregated. The ordering of the options based on their rates or ranks gives an indication of an attribute's preference over others.

The assignment of the rating or ranking is done by a value function. Typically, a simple linear value function would have suffice, but a utility theoretic non-linear value function is more appropriate in taken care of the human reasoning or fuzzy linguistic aspects of decision making. This approach, though may be complicated or complex, offers an advantage of independence from the approach which has merely the relative importance of options or attributes.

Chapter 5 Fuzzy Sets & Neural Networks Theories

This chapter presents the two main theoretical frameworks of fuzzy sets and neural networks theories, with emphasis on the neuro-fuzzy methodologies employed in this study.

5.1 Fuzzy Sets Theory

This section deals with fuzzy sets and logic, its operations and relations, fuzzy implications and rule-based systems. Fuzzy sets are characterized by numerous intrinsic properties which define the attributes and operations within fuzzy systems [47]. The treatment given hereunder are the basic properties employed directly in this study; though in few cases, an extended treatment is presented for cohesion and comprehension of the thesis. The detailed explanations are offered in many literature, especially [6] [148] [47] [196] [208], with some supporting literature included in the Appendix D.

5.1.1. Fuzzy Sets & Logic

Set Theoretic

Fuzzy sets are extensions of classical sets, where elements of the fuzzy sets have graded characteristic functions, called membership functions. Fuzzy sets theory was introduced by Zadeh [6] to deal with uncertainties associated with vagueness. Fuzzy sets and logic are utilized to represent vague concepts quantitatively. They have applications in engineering and science. Especially, its utility is applied to fuzzy data used in expressing subjectivity in natural languages and human reasoning.

Fuzzy logic, unlike classical Aristotelian logic, is multi-valued, and has graded memberships which capture most of the system attributes and constructs. The notion of fuzzy sets is transparent and highly intuitive as it captures the essence in real world of what is perceived and described [42].

Cox [47] defines fuzzy sets succinctly as “functions that map a value that might be a member of the set to a number between zero (0) and one (1) indicating its actual degree of membership. A degree of zero means that the element is not in the set, and a degree of one means that the value is completely representative of the set”. An element belonging to a fuzzy set must satisfy the following axioms:

- It must lie within the defined domain of the set;
- It must have a non-zero membership value; and

- It must lie above a currently defined α-cut threshold[13].

Fuzzy sets and logic are used to handle the perceived uncertainties in the metrics of everyday systems such as the computer systems and networks providing ubiquitous services and products.

In essence, fuzzy logic theory is a prolongation of the (classical set theory) conventional logic whereby members of a fuzzy set could have partial membership, and defined by rule conditions which can be partially satisfied [6].

Fuzzy logic is used to approximate the qualitative linguistic and subjective aspects of human reasoning. This is done by a structured representation of real world vague and imprecise knowledge. That is, the inherent subjectivity in the natural language is "normalized" or made objective and used appropriately to model a real world abstraction.

For instance, the linguistic terms or semantics used in describing the security conditions of computer systems, such as "vulnerable", "secured", or "susceptible" are all vague terms or fuzzy in nature. A fuzzy system modeled with, say, security abstraction variables or metrics have fuzzified parameters estimated by the degrees of "contributions" of each variable [209].

Membership functions define the degree of compatibility of fuzzy linguistic variables with a particular fuzzy concept [47]. Different approaches are available to assign appropriate membership functions to a fuzzy set. These approaches are in practice ill-defined; it can be done by model expert, or by using system generated data or by trial-and-error. An approach adopted may be due to a model expert's interpretation of fuzziness as a concept [210]. (Detailed explanations of different fuzzy view concepts are offered in [210]; and some brief illustrations are offered in Appendix D).

It must be noted that membership functions can be defined by neural network modeling techniques as with the use of adaptive neural-based fuzzy inference system (ANFIS)[14]. In this study, membership function elicitation is carried out by either one of the likelihood, utility or measurement views. For example, in estimating the membership values of vulnerabilities in ICT asset disposal policies, the likelihood view was appropriately applied. Cyber-security functionaries were polled (surveyed) to declare the perceived vulnerabilities in their systems.

[13] The fuzzy α-cut set concepts are made clearer with more definitions in subsequent sections.
[14] ANFIS which was first introduced by Jang in 1993, is discussed under section 5.3.3.

5.1.2. Fuzzy Set Operations

Fuzzy set operations are used for the computation of linguistic terms within the fuzzy variables. There are many fuzzy set operations and nomenclature in literature. The relevant operators and their key nomenclature on fuzzy sets theory used in this thesis are included in Appendix D. Apart from a few unavoidable instances, relevant definitions are given in Appendix D.

5.1.3. Fuzzy Relations & Graphs

A fuzzy relationship between two or more sets is an expression of association, interrelationship, interconnection, or interaction amongst the sets [18]. Accordingly, there is a degree of presence (or belief about the existence) or absence (or non-existence) of such relations [211]. That degree of presence in the relationship $\mathbf{R}$ between two constructs $\mathbf{A}$ and $\mathbf{B}$, is given by $\mathbf{R(A,B)}$ or $\mu_R \in [0,1]$ such that $\mu_R(a, b) \in [0, 1]$.

In this study, fuzzy relation is used in evaluating, for example, the possibility of occurrence of threats x_1 and x_2, such that the possibility of occurrence of threat x_1 maturing after threat x_2 is, say, 0.7.

Fuzzy relations can be represented in graphs just like classical crisp set relations. Notable amongst them are bipartigraph, coordinate diagram, matrix and directed graph (or Digraph).

For this study, the last two methods are employed. For instance, fuzzy matrices and fuzzy digraphs are useful tools in the analysis using fuzzy cognitive maps (FCMs). FCMs are treated and applied in detail under section 5.3.2.

It must be noted that some literature treat fuzzy matrix multiplication as what is called max product [148] in which case $X \square Y = \max(\min(X_{ij}, Y_{ij}))$. This study employs the min-max matrix product approach, unless it is explicitly stated otherwise.

5.1.4. Fuzzy Rule-based Systems

Fuzzy logic is concerned with the inherent imprecision of describing the fuzzy concepts themselves, rather than the inaccuracies or noise associated with the metrics [47].

Fuzzy systems consist of a series of conditional and/or unconditional fuzzy statements, correlation, implication, and aggregation methods and decomposition or defuzzification techniques. The fuzzy statements (or rules) are fired in “parallel processing paradigm”, except

that some rules have no significant degrees in their premises and so fail to contribute to the outcome [47].

Fuzzy rules or propositions are typically correlated and evaluated for their various contributions to the overall model solution in a process called Fuzzy Implication [47]. As an illustration, given any fuzzy sets A and B, the rule-base is viewed as "fuzzy implication function" [148] written as $\mu_R(x,y) = f(\mu_A(x), \mu_B(y))$; where f is the fuzzy implication function, x ∈ A and y ∈ B such that $(x,y) \subseteq A \text{ x } B$. This study utilizes two(2) typical fuzzy implication functions described in [148] as the Mamdani fuzzy implications functions (which interprets the relations with the minimum operator) and the Larsen fuzzy implications functions (which interprets the relations with the dot product operator).

Fuzzy Modeling:

This study endeavors to model and represent the abstractions of real world cyber-security vulnerabilities and associated cyber-risk by using fuzzy constructs; and by using fuzzy linguistic variables to reduce the system complexity with semantic labels in a systematic and computationally by efficient manner. The imprecise empirical data and the vague experts opinions are modeled to represent the human reasoning of cyber-risk and vulnerabilities challenges confronting SMEs in developing economies.

Fuzzy rules and inferences are deduced from the elicited experts opinions based on the notion that modeling cyber-security vulnerabilities is fraught with subjectivity, imprecision, and vagueness. Also, cyber-security vulnerabilities system is complex and lacks historical data.

Cognizant of the above, traditional mathematical modeling approaches are typically inadequate to model such non-linearity and uncertainties. But fuzzy modeling is appropriate as it takes into consideration all inherent attributes resulting from the system uncertainties.

Upon appropriate representation of the cyber-security vulnerabilities system with fuzzy variables, a fuzzy relational output is generated as a solution. The fuzzy relational output is then subjected to a fuzzy implication function which evaluates the consequent propositions, based on a set of antecedents. The various system membership values are correlated and aggregated by either AND or OR connectors, as the implication transfer function is updated to create the output solution [47].

The fuzzy output set consists of linguistic variables, which are the resulting union of all the linguistic terms. This fuzzy set of outputs is also characterized by a membership function that is computed from the possible membership functions of the various linguistic terms through aggregation process.

The resultant model solution from the inference is a fuzzy set or space that has to be converted into a crisp value for meaningful analysis and interpretation. This process of decomposition is called Defuzzification.

5.2 Neural Networks Theory

Artificial neural network (ANN) or neural network is an information processor with capability to learn, adapt and automatically classify similar classes together [208]. ANN has the capability to receive, process and transmit information signals and to apply its cognitive abilities to predict solutions [212]. It is usually applied in modeling cases where there is meaning or patterns in data and it can handle massive and complex datasets [213] [214].

The neural networks are powerful tools for modeling problems, such as the cyber-security vulnerabilities study, for which the explicit form of the relationships amongst the key variables are not known.

The empirical dataset is presented in an input-output array (or mapping) to the neural network. The neural network learns by associating the inputs with corresponding target output responses, as the model runs. By so doing, an error is computed from the difference(s) of the target output response and that of the real system output.

The error information is fed back into system which makes all adjustments to its parameters in a systematic fashion which optimizes a criterion, commonly referred to as the Learning Rule. This process is repeated until the desired output is acceptable.

Note, appropriate sections of Appendix D contain literature on the ANN characteristics and structures, as well as the transfer functions and learning modes (i.e. supervised and unsupervised learning). In this study, the ANN assumes a multi-layer neural network structure; (for most applications a 3-layer multi-layer neural network, consisting of an input layer, a hidden layer and an output layer, would be sufficient). It must be noted that the more hidden layers there are, the more complicated the network would be.

The problem of modeling cyber-security vulnerabilities is one of non-linearity and so the linear neural network would not be suitable to resolve. This study uses a simple feed-forward 3-layer neural network with a back-propagation neural (BPN) algorithm in a supervised neuro-fuzzy system.

A treatise on the back-propagation neural algorithm (BPN) is given with detailed mathematical explanations in Appendix D.

5.3. Hybrid Neural & Fuzzy Systems

The choice of methodology is usually dictated by the dataset available for the model. In this study, the datasets consist of input-output data pairs as well as the fuzzy linguistic rules generated from the experts' opinions. The numerical input-output mappings are best modeled with neural network techniques, whereas the fuzzy inference rules are best modeled with appropriate fuzzy techniques. The neural network methods provide the learning capability and the fuzzy methods provide flexible semantic interpretations [55]. So by integrating these two techniques in modeling can lead to better analysis that take advantage of the strengths of each techniques, whilst overcoming some of the limitations of each technique.

Fuzzy logic is used to encode the expert knowledge directly using rules with linguistic variables. In practice, this may take a lot of time to design and tune the membership functions that quantitatively represent the linguistic variables. The learning capabilities of neural networks are employed to automate this process and subsequently reduce development time and cost while improving system performance. This hybrid process also makes it easy to interpret and explain the resulting output as a typical fuzzy system.

5.3.2. Fuzzy Cognitive Map (FCM)

Fuzzy Cognitive Map (FCM) is a signed directed graph with concepts such as policies, events, etc., represented as nodes or vertices and causalities represented as edges or arcs [215]. FCMs are used for the abstraction of real world problems, knowledge representation and computational inference, by representing the key constructs as concepts or nodes, and linked with concurrently active causal relations [201] [202] (as cited in [215]). Its basic framework uses vector-matrix operations to infer causative fuzzy concepts relations.

The concepts take fuzzy numbers from the unit interval [0, 1]. The causal relations between concepts are represented by the signed directed edges or links, which are indications of the relational impact or influence [215].

The utility of fuzzy sets expressed in the membership functions, make fuzzy set theory suitable for uncertainty metrics and most importantly gives meaning to the representation and interpretation of vague concepts in simple human reasoning [202] (as cited in [215]). FCM is simple, works well with expert's opinion, and it's able to handle unsupervised data to unearth the latent characteristics or correlation of variables [215].

"This study used Fuzzy Cognitive Map (FCM) approach to evaluate the possible vulnerabilities of ICT asset disposal policies and the associated impact on SMEs in developing economies. The evaluation of vulnerabilities resulting from indiscriminate ICT assets disposal involves limited

historical data sets and imprecision" [215]. This situation is due in part to lack of literature in security analysis of vulnerabilities in SME assets [216] as well as inherent uncertainties associated with intra-uncertainty and inter-uncertainty[15] of expert opinions and fuzzy metrics, in general. This situation results in as a type of uncertainty and techniques using fuzzy set theory emerge as convenient. The FCM technique examined the policies (as concepts) making use of expert's appraisal and fundamental fuzzy matrices to represent the possible knowledge intrinsic in discovering cyber-security vulnerabilities. By using fuzzy matrices and directed graphs resources the relationship amongst the diverse asset disposal policies and vulnerabilities were determined [215].

According to Kandasamy et al [202] (as cited in [215]), FCM theory is solidly grounded when there are more experts' opinions. This facilitates the application of combined FCM using those experts' opinions. That notwithstanding, Kandasamy et al. [202] assert that the key disadvantage is when there exist conflicting opinions, the combined FCM could be sum to zero, in which case the experts' opinions would have been rendered worthless.

Another disadvantage with FCM is the encoding nature of expert's opinion or biases which could render the model inaccurate. This issue is mitigated by deriving this study's expert's opinion partially from the dataset [215].

In spite of its simplicity, this FCM approach can be applied to almost any techno-economic endeavor which require assessment of cause-and-effect analysis.

Siraj et al. [217] (as cited in [215]) used FCM to model a decision support system that utilized causal knowledge for intelligent intrusion detection system (IIDS). This was an innovative model where fuzzy rule-base was applied, just as in a similar risk assessment study by Smith & Eloff [218] (as cited in [215]). This study however, employs simple FCM modeling with matrix operations.

FCM has been used for expert judgment elicitation and then innovatively transformed into a fuzzy inference system that was used to predict the discount rate for a venture capital valuation of firms [219] (as cited in [215]).

[15] Uncertainty with fuzzy terms used in evaluating the expert opinions has two (2) forms; intra-uncertainty, which is uncertainty that an expert has about a fuzzy term, and inter-uncertainty, which is uncertainty that a group of experts have about a fuzzy term [60].

5.3.3. ANFIS

The Adaptive-Network-based Fuzzy Inference System (ANFIS)[16] is a form of feed-forward neural network with the ability to learn from data in a supervised mode. It's adaptive nature implies that the nodes (neurons) give outputs based on some predefined parameters, such as the weights and learning rate, which keep changing or updating based on an optimized error metric [220].

ANFIS employs the gradient descent and chain rule algorithm as the learning rule. A disadvantage of the gradient descent method is its slowness and possible tendency to be trapped in local minima [220].

ANFIS is a hybrid modeling tool that utilizes the back-propagation neural (BPN) algorithm. Its training session is iterative such that the predefined error metric is evaluated as the sum of squared difference between the targeted and calculated outputs, as well as reducing the error. The training session ends upon achieving either of the predefined error metric or number of epochs [220] [221].

The neuro-fuzzy model is trained with a set of data in the form of input – output tuples, and a specification of the rules, including a preliminary definition of corresponding membership functions. A typical approach is to assume a certain shape for the membership functions so that the membership functions depend on parameters that can be learned by the neural network [222]. This study assumed triangular membership functions for the inner-most linguistic terms, whilst trapezoidal membership functions were used for the outer terms, and the parameters were in turn learned by the neural network. The aim of the training procedure is to minimize the error, which is the difference between the calculated output and the target value. The adaptation of the weights during the training process can lead to a so-called over training. This means that the neural network can reproduce the training data quite well but has lost its ability to generalize.

In this study, the MATLAB toolbox of Adaptive Neural Fuzzy Inference System (ANFIS) was used to develop the cyber-security vulnerability assessment (CSVA) model with the survey dataset to determine if indeed it is supported or refuted by the data collected from the field.

The ANFIS toolbox uses fuzzy rules extracted from the numerical data sets and combined with fuzzy knowledge acquired from the experts. Based on the expert knowledge, the IF-THEN rules were defined for the fuzzy inference system (FIS). Theoretically, the total number of possible

[16] ANFIS was developed by Roger Jang, a protégé of Prof. L.A. Zadeh. Jang titled his seminal paper on ANFIS as Adaptive-Network-based Fuzzy Inference System in [220]. However, other literatures use Adaptive Neural Fuzzy Inference System and Adaptive Neuro-Fuzzy Inference System for ANFIS interchangeably.

outcomes from the rules is set by the multiplication of all input membership functions; in this case of 5 MFs for 4 variables, the possible outcomes were $5^4 = 625$ rules. In practice, one would either use system generated rules or apply the expert rules (which are less).

Once the rules were established the training data set were loaded into the ANFIS, with the selection of appropriate optimization algorithms (e.g. back-propagation and/or hybrid methods), and set the number of epochs to run. The FIS rules were loaded into the ANFIS and start the training until an optimized error level is reached. After that the system is re-loaded with test data sets to validate the system.

It must be noted that the problem at hand was designed as a Mamdani fuzzy inference system (FIS). However, the MATLAB ANFIS toolbox is limited by processing only Sugeno FIS or system generated from data sets. Thus, MATLAB command of "*mam2sug*" was used to transform the Mamdani rule-based inference into Sugeno FIS before loading onto the ANFIS.

Chapter 6 Cyber-Security Vulnerabilities Assessment (CSVA) Model

This chapter presents the data, its analysis and findings which culminate into the key research objective of building a cyber-security vulnerability assessment (CSVA) model and enlisting taxonomies of vulnerabilities and threats.

The chapter has been structured into six distinct, but intertwined sections, besides the preamble. It discusses the introductory background with key assumptions and research questions of the study.

The succeeding section covers the data presentation as utilized for the analysis of the study. This is followed by the CSVA model itself, primarily, built with the MATLAB adaptive neuro-fuzzy inference system (ANFIS) toolbox, together with its key constructs and applications.

The taxonomies of vulnerabilities and threats are evaluated using fuzzy similarity measures with multi-attribute decision-making (MADM) techniques to rank the constructs. Further, cyber-security vulnerabilities are analyzed using fuzzy cognitive maps (FCMs) approach.

Preamble

The key motivation for this study has been a focus on the cyber-security challenges that threaten the survivability of SMEs businesses in developing economies. The research has been about finding a model by which SMEs can mitigate against cyber-risks and also to facilitate their secured and reliable participation in today's cyber-market.

SMEs expert opinions on various cyber-security and business metrics were solicited and efforts were made at identifying the key vulnerabilities as well as their associated perceived uncertainties about those vulnerability attributes. Upon careful examination of the inherent causative factors, appropriate cyber-security solutions are recommended.

Assumptions

The following are key assumptions made for this study:

- That, the risk (due to threats) is proportional to the value of the vulnerable assets.
- That, a cyber-security vulnerability based conceptual model is an approach used in capturing vague, imprecise and real-world linguistic descriptions and system requirements, for the transformation of its constructs into recognized and consistent conceptual metrics [91].

- That, fuzzy sets can be used to model vagueness and coarseness in a system. That, models are used for the purposes of system analysis, to either assess, describe or prefer system attributes, constructs and metrics [18].
- That, the cumulative impact of vulnerabilities is estimated based on the following formulae, afore-mentioned in chapter 1 of this thesis, i.e. the vulnerability constructs as fuzzy relational functions with human and system attributes as fuzzy arguments as per equations [1-1] through [1-3]:
- That, a threat is a fuzzy function with a number of fuzzy arguments, such as motivation, capability, opportunity and impact [41] [40], as defined per equation [4-4] in chapter 4 above.
- That, the culmination of this study is on the basis that mathematically, cyber-risk is given by the fuzzy relational function as per equation [1-4] in chapter 1 of this thesis.

These assumptions which are mainly based on state-of-the-art literature led to the research questions as per Chapter 1 of this Thesis.

The ensuing section attempts to recap the key methodologies in order to bring flow and comprehension to the treatise herein.

6.1. Recap Methodology

This section recaps on the process of measurement as much as the metrics of cyber-security used in gathering the perceived opinions of the sample experts for the study. Though detailed descriptions are given in chapters 3, 4 and 5, brief overviews are presented herein for comprehension.

First, the methods employed are presented and then followed by the approaches adopted.

6.1.1. Overview of Methods

The assessment of cyber-security was based on the assumption that the constructs are intangible. In other words, cyber-security properties are not directly measured or observed in similar manner as a physical property is experimentally measured. Essentially, cyber-security metrics and indicators are employed to assess a firm's security posture and apply measures to improve security.

As noted in the preceding Chapters, the survey design was based on extensive literature review that solicited experts opinions, which constitute the datasets of this study. The datasets were analyzed to assess the perceived vulnerabilities, threats, and key assets, as constructs of interest.

The following section dilates briefly on the approaches and tools used in the study.

6.1.2. Overview of Materials

The main approach adopted for this study is the use of structured questionnaire-based online survey. The sample SMEs were reached via email messages sent to them with a preamble explaining the import of the study and a URL link to the web portal. Two specific web portals have been utilized for the study – one for the main study (www.limesurvey.com) and the other for the follow-up strategic interviews (www.surveygizmo.com).

Online web portal survey has wider geographical coverage; email messages vis-à-vis web portal were appropriate since all the population of ICT functionaries in SMEs in the case study have access to email and Internet. This means that everyone has equal chance of being surveyed.

Concise overviews of both metrics and the approaches used in collecting data have been presented. The next section deals with the data presentation.

6.2. Data Collected

There were 94 respondents from the main survey, of which 5 had employees more than 250 employees and so were disqualified (excluded from further analysis – even though some "minor" comparisons are made occasionally) in accordance with the study's adopted SME definition. That means the sample size of 89 is the dataset being analyzed herewith.

The breakdown of the 89 respondents is as follows:

- Less than 10 employees (or micro firms): - 11
- 10 – 49 employees (or small firms): - 24
- 50 – 99 employees (or medium firms): - 19
- 100 -250 employees (or medium firms): - 35

The main study had 27 vulnerabilities metrics, 12 threat metrics and 1 set of metrics for asset value (business impact or risk). Besides, there were other metrics for business profiling in respect of products and/or services engaged in, such as perceived annual incident losses, perceived incidents of intrusion, dedicated security positions, existence of security policies and compliance with regulations, etc.

Similarly, the strategic interviews (follow-up survey) were targeted at 20 cyber-security experts, of which 14 responded. All 14 responses were within the scope of the study and were evaluated under expert opinion elicitation and fuzzy multi-attribute decision-making (MADM), described in later sections.

All responses were then coded for ease of data analysis.

6.2.1. Data Coding

It is noted that the dataset is one of multivariate[17] dataset. So after the principal component analysis (PCA) pre-processing on the dataset to see the correlations, the dataset were coded into numerals (i.e. 1 through 5), depending upon the variable and its fuzzy linguistic terms at play.

For instance, the following coding were assigned:

- $\{\text{not-vulnerable} \equiv 1, \text{slightly-vulnerable} \equiv 2, \text{vulnerable} \equiv 3, \text{very-vulnerable} \equiv 4, \text{extremely-vulnerable} \equiv 5\}$ for vulnerabilities;
- $\{\text{very-low} \equiv 1, \text{low} \equiv 2, \text{medium} \equiv 3, \text{high} \equiv 4, \text{very-high} \equiv 5\}$ for threat agents;
- $\{\text{insignificant} \equiv 1, \text{minor} \equiv 2, \text{moderate} \equiv 3, \text{major} \equiv 4, \text{severe (critical)} \equiv 5\}$ for asset values and risk (impact levels).

It is noted that the linguistic terms and coded values were assigned in an exclusive manner, such that each answer of a sample respondent was appropriately placed into a class or category of fuzzy linguistic terms.

This coding approach prepared and simplified the data for further analysis with minimal errors, especially with regards missing data. It is noted that though the PCA process identified and deleted any missing data and outliers, the entire dataset is used in the further analysis to build the neuro-fuzzy model. This is in accordance with Meyers et al [164], who posited that when samples with the missing values and outliers are "deleted" from the data set during preprocessing, the remaining data set is actually a sub-sample which in turn affects the generalization to the population.

After the coding the data is classified into categories.

6.2.2. Data Classification

In a research such as this, there were voluminous datasets that were collected from the survey. There was the need to classify the data into homogeneous categories for further and meaningful analysis. The classifications were those of the vulnerabilities, threat agents, assets values and/or business impact groupings, besides the general ones for business profiling, descriptive characteristics and statistics analysis.

[17] Multivariate data is data collected on several variables for each of sample of the respondents surveyed.

After the data coding and subsequent classification comes the computation of the cumulative impacts of vulnerabilities and threat agents, as per the study's assumptions.

Inferring from chapter 3 of this thesis, fuzzy triangular mean or fuzzy arithmetic mean [63] [64] were used to aggregate the opinions for each of the categories. That is, given n=89 sample experts (or respondents) with corresponding fuzzy triangular numbers, $x_i = (x_l^i, x_m^i, x_h^i)$ where $i = 1,2,.....,n$; and x_l is the lowest value of support value of x; x_h is the highest value of support of x; and x_m is the middle value or modal value of the triangle.

$$\begin{aligned}\overline{X} &= \frac{X_1 + X_2 + ... + X_n}{n} \\ &= \frac{(x_l^1, x_m^1, x_h^1) + (x_l^2, x_m^2, x_h^2) + ... + (x_l^n, x_m^n, x_h^n)}{n} \\ &= \left(\overline{X_l}, \overline{X_m}, \overline{X_h}\right) \\ &= \left(\frac{1}{n}\sum_{i=1}^{n} x_l^i,\ \frac{1}{n}\sum_{i=1}^{n} x_m^i,\ \frac{1}{n}\sum_{i=1}^{n} x_h^i\right)\end{aligned} \qquad [6\text{-}1]$$

To validate the model properly, a number of computations were also used on the model and their respective error margins per dataset aggregation are evaluated. For example, the min and max operators were used on the datasets. Lastly, but the least, the dataset was initially fuzzified and then similar arithmetic averages, min and max operations were performed on them for further validation. These computed datasets were appropriately tabulated as per the following section.

6.2.2. Data Tabulation

This section tabulates the datasets with appropriate referencing in the appendix, as they are too elaborate for the main body of this thesis. The caveat here is that, unless the dataset is summarized and needed for immediate supporting argument, it would be presented in the appendix instead of the main body literature.

The following are the datasets:

- Training datasets (75% of the samples) - Appendix A-2
- Testing datasets (25% of the samples) - Appendix A-3
- Security Positions - Appendix A-4
- Security Losses in US$ per Year - Appendix A-5
- Unauthorized Access per Year - Appendix A-6
- Details of data on Vulnerabilities (critical assets) - Appendix A-7

- Details of data on Threat agents - Appendix A-8
- Dataset of Experts Opinions - Appendix A-9
- Neuro-Fuzzy based Model Graphs - Appendices B-1 through B-15.

The ensuing section enumerates and highlights the key results of this study.

6.2.3. Key Results

This section enumerates highlights of key results deduced from this study:

- The cyber-security vulnerabilities assessment (CSVA) model, built with adaptive neuro-fuzzy inference system (ANFIS) based MATLAB toolbox;
- The taxonomies of vulnerabilities and threats using fuzzy similarity measures for multi-attribute decision-making (MADM) techniques; and
- The fuzzy cognitive maps (FCMs) assessment of ICT assets disposal policies and associated vulnerabilities.

The subsequent sections deal with the approaches, analysis and computations of these key results and allied descriptive findings.

6.3. The CSVA Model

The CSVA model is used to assess or characterize the uncertainties, such as the vulnerabilities (which are weaknesses or flaws that could be exploited to violate the confidentiality, integrity and availability properties of cyber-assets) or threats. The unique distinction here is that perceived or abstract notions rather physical quantities of cyber-security are assessed.

The CSVA model conveys an understanding of how to characterize vulnerabilities and to recommend the eminent risks associated with information systems. It assists in the explanation of complexities and uncertainties of vulnerabilities and threats. It presents the key cyber-security challenges confronting SMEs and highlights on the contributory roles of asset value, vulnerabilities, threats, risks and associated impact, as well as policies needed to build a secure organization.

The CSVA model is used to explain the security posture of an organization and it assists in the understanding of the effects or implications of threats on vulnerabilities, as well as utilizing the model for the prediction of risk impact on an organization.

The essence of the CSVA model is to safeguard business assets against vulnerabilities and threats to cyber-security, so as to ensure business continuity and optimum performance.

The next section deals with the building of the neuro-fuzzy based model using MATLAB ANFIS toolbox.

6.3.1. Building a Neuro-Fuzzy Model

This section deals with the processes and computations leading to the building of the Mamdani-based neuro-fuzzy model using the MATLAB fuzzy logic toolbox.

First, the system parameters are clearly identified: it has 4 inputs consisting of the vulnerabilities {i.e. weaknesses in cyber-assets, resulting in breaches of each of the confidentiality, integrity, availability properties} and threats, and an output of risk. The following membership functions were used:

- For the vulnerabilities:
  - Not-vulnerable {not-vulnerable} - [0 0 1 2]
  - Slightly-vulnerable {sli-vulnerable} - [1 2.5 4]
  - Vulnerable {vulnerable} - [3 5 7]
  - Very-vulnerable {very-vulnerable} - [6 7.5 9]
  - Extremely-vulnerable {ext-vulnerable} - [8 9 10 10]
- For the threats:
  - Very low {very-low} - [0 0 1 2]
  - Low {low} - [1 2.5 4]
  - Medium {medium} - [3 5 7]
  - High {high} - [6 7.5 9]
  - Very high {very-high} - [8 9 10 10]
- For the risks:
  - Insignificant {insignificant} - [0 0 1 2]
  - Minor {minor} - [1 2.5 4]
  - Moderate {moderate} - [3 5 7]
  - Vital {vital} - [6 7.5 9]
  - Severe {severe} - [8 9 10 10]

Upon defining the system parameters, the fuzzy rule base is also defined using the information from the experts as the basis; here about 24 rules are set (c.f. figures of the system, rules, network structure, training and testing in ANFIS, surface view of errors are Appendices B-1 through B-13).

As stated earlier, the proposed model is one of non-linearity. Also, the Sugeno fuzzy inference system (FIS) typically gives out a crisp output. In contrast to the Mamdani FIS, the Sugeno FIS

is unable to emulate the compositional rule of inference in its fuzzy reasoning [223] [56]. The CSVA model has fuzzy consequents and employs compositional rules in its inference system.

It is also noted that the MATLAB ANFIS toolbox is designed to handle ***only*** Sugeno fuzzy inference systems (FIS). So a MATLAB script, with key command "*mam2sug*", for the conversion from Mamdani to Sugeno FIS is executed for the transformation from Mamdani-based system into ANFIS feasible Sugeno-based system and for further processing.

By this time, the appropriate datasets of Training and Testing should be loaded unto the MATLAB workspace. The other network parameters of method of optimization and number of epochs are set. It is noted that the hybrid learning algorithm was used, since it performed better than the back-propagation algorithm alone.

The system was then loaded with the training dataset for the model learning to commence at predefined epochs. After training or learning, the system is loaded with testing dataset for validation and verification of system performance. The appropriate error rates are noted. The Table 6-1 below shows the results of the error rates and the type of datasets used[18].

Table 6- 1: Results of ANFIS Training, Checking & Testing Errors

		arithmetic mean	min operator	max operator	fuzzified average
Triangular MFs	training	0.1595	1.0025	0.7779	0.1882
	checking	3.7372	1.8662	1.7220	0.3776
	testing	0.1595	1.0025	0.7779	0.1887
Trapezoidal MFs	training	0.0877	1.0025	0.7779	0.1693
	checking	2.4217	1.8724	1.7118	0.5277
	testing	0.0877	1.0025	0.7779	0.1693
Gaussian MFs	training	0.0864	1.0025	0.7779	0.1357
	checking	2.2698	1.9671	1.6324	1.7543
	testing	0.0864	1.0025	0.7779	0.1383

Appendices B-13, B-14 and B-15 are example exhibits showing the errors in 4, 5 and 6 decimal places (these errors are depicted on the figures at the lower left corner).

The subsequent sections present and describe the model and associated components.

[18] The figures in the table have been rounded up to 4 decimal places each, in conformity with the least decimals generated by the ANFIS computations. The original figures, with some 5 and 6 decimals, are maintained and shown in Appendix A-10.

6.3.2. Schematic Model Description

In this section, the cyber-security vulnerabilities assessment (CSVA) model is formally presented as a key product of this study (c.f. Figure 6-1).

The proposed CSVA model consists of four layers as shown in Figure 6-1. The CSVA model can be used to describe situations of interest and to present analysis towards mitigating vulnerable systems. In the following sections, the functional description of each layer is presented.

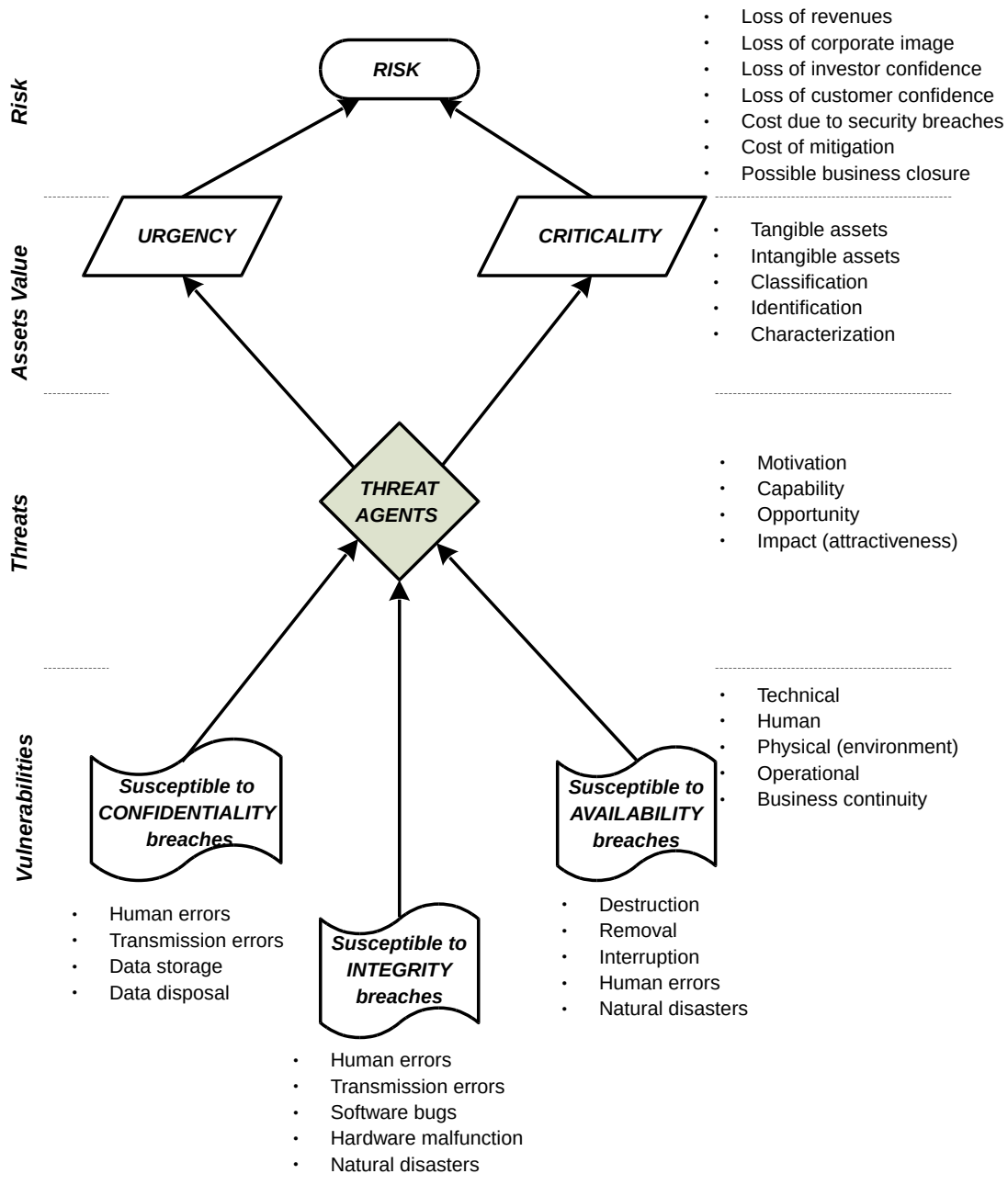


Figure 6- 1: Multi-faceted Cyber-Security Vulnerabilities Assessment (CSVA) Model

6.3.3. Functional & Logical Model

This section presents the detailed description of the functional and logical components of the CSVA model.

Layer 1: Cyber-security Vulnerabilities

Layer 1 of the CSVA model is the cyber-security vulnerabilities layer and the lowest in the model. At this layer, weaknesses in the systems, networks, infrastructures, and applications are identified and assessed. The objective is to estimate the extent to which the systems are rendered susceptible to cyber-attacks. The assessment takes into consideration the possibilities of multiple threats and estimate the combined effects of multiple and sequential incidents.

The CSVA model ought to assist SMEs to have a very good understanding of the assets that ought to be safeguarded, the threats against which those assets ought to be safeguarded, the vulnerabilities of this particular assets as well as the existing risk to the assets as a result of those threats and exposure [224].

In assessing the vulnerabilities, due recognition is taken for the fact that typical weaknesses or flaws in cyber-assets could be exploited to compromise any of the CIA security properties in a number of ways. According to X.800 [224], the following 4 types of vulnerabilities may be exploited:

i. Threat model vulnerabilities – come from the challenges of anticipating possible future threats;
ii. Design & specification vulnerabilities – originate from errors or oversight within the design of a system or protocol making it inherently susceptible;
iii. Implementation vulnerabilities – are created by errors during system or protocol implementation; and
iv. Operation & configuration vulnerabilities – come from inappropriate utilization of choices made in implementations or weak deployment policies, such as not enforcing the use of encryption in a WiFi access point.

The CSVA model is also used to classify the vulnerabilities into technical, human, physical, operational and business susceptibilities. Similarly, and in accordance with [39], the CSVA model can classify the vulnerabilities into such categories as type, source and severity. Vulnerability identification and classification are used in recommending appropriate and effective mitigation solutions to SMEs.

Layer 2: Cyber-security Threats

Layer 2 of the CSVA model is the cyber-security threats layer and the next higher layer upon the lowest. This layer deals with the evaluation of any events or situations or actions that can possibly exploit weaknesses in systems to cause harm and/or pose risk to a given cyber-asset.

Typically, vulnerabilities in the systems are exploited by threat agents to facilitate the realization of a threat, whose impact is the risk. The CSVA model is used to assess the possible threat agents, which could be either human (end-users) or technical (such as systemic or operational) or environmental in nature.

It must be noted that there are a number of threat agents or threat sources in cyber-security and this study deals with a limited list. So the CSVA model in its assessment identifies and evaluates the type, sources and possibilities of realization of threats. Threat agents capitalize on the opportunities afforded to them by the weaknesses or susceptibilities in the systems. The CSVA evaluates threat agents' motivations and capabilities, as well as the attractiveness of the resource at stake. Through the identification and assessment of threat agents, the CSVA model serves as a decision analysis technique which facilitates and prioritizes resources allocated to mitigate possible risks.

The model can also be used to evaluate historical dataset, if available, to give an indication or predict the possibilities of certain threats being realized.

Finally, the threats layer is utilized to assess threat agents and account for their transitional states as the agents actually "mutate over time" [40]. For example, a script kiddie threat agent may have acquired new skills or gathered additional capabilities to hack into a corporate system with fresh motivation, though at some point in time, his activities might have been deemed inactive or dormant.

Layer 3: Cyber-Assets

Layer 3 of the CSVA model is the cyber-security asset layer. Cyber-assets, as defined in this study, are the very embodiment of SMEs that facilitate the conduct or engagement of business activities in today's cyber-market [36]. These assets may manifest as tangible or intangible resources.

In view of that, this layer evaluates cyber-assets and endeavors to estimate the cumulative asset value involved. The process involves appropriate assets identification and classification. The classification facilitates the exact estimation or assessment of the criticality or importance label assigned to each cyber-asset, based on parameters such as business risk (upon

compromise), actual asset value (purchased price with depreciation rules applied), sensitivity, governance and compliance requirements.

This layer also estimates the urgency parameters of the given resources. In accordance with [187], the asset value is also computed by taken into account the time required for its maintenance and repairs, its sensitivity to the SMEs, as a measure of the urgency with which restoration will be required upon compromise.

The CSVA model allows for intuitive assessment of the cyber-assets based on the assessor's expertise to assign values using qualitative fuzzy criteria, such as purpose, pleasure and ideals. To make the evaluation objective, one can use the organization's asset classification policy, if available, as a guide. Also, through the use of the CSVA model, other policies which depend upon the assets classification policy can be re-formulated.

These two (2) key metrics of criticality and urgency are used to ascertain the extent or severity of impact upon cyber-attack or compromise.

Finally, it must be noted that the asset value is proportional to the impact or risk level to the SMEs; that is, the asset value is positively correlated to the risk to the SMEs. In fact, the asset value is a "disutility" and it reflects the extent of possible losses (e.g. revenue loss, loss of reputation, possible lawsuits, etc.) to be incurred upon compromise.

Layer 4: Cyber-Risks

Layer 4 of the CSVA model is the cyber-risks layer and the highest layer. It is the culmination of the essence of the CSVA model; depicting the ultimate expression of the consequences resulting from a threat agent exploiting an opportune vulnerability in a given asset.

The cyber-risk layer is used to express the fuzzy relationships existing amongst the other lower layers. It estimates qualitatively the resultant risk value upon assessing the nature and extent of vulnerabilities and the possibility of exploitation and associated severity, should a threat matures for a given cyber-asset [7]. This evaluation is carried out by taking into account all possible (including potential) threats, with the notion that a vulnerability might be exploited by multiple threat agents.

The CSVA model takes an approach in assessing and evaluating the risks by deducing the cumulative relational impact of a compromise on an asset. The CSVA

is expressed mathematically, as the impact of a breach of cyber-security properties, by the fuzzy relational function (as per equation [1-4] in Chapter 1):

$$Risk_{\text{threat}} \propto f(\text{Threat}_{\text{asset}}, \text{Vulnerability}_{threat}, \text{Asset Value}) \quad [6\text{-}2]$$

where:

- Asset Value is estimated from evaluations in layer 3, with respect to criticality and urgency of the asset to the SME business;
- Threats, to a given asset, is estimated from evaluations in layer 2, in respect of motivation, opportunity, capability and impact to SME business; and
- Vulnerability, given a particular threat agent, with respect to type, source and severity to SME systems.

The implication is that, a higher asset value (which is treated as disutility or negative utility), and a higher vulnerability value (i.e. highly susceptible asset) and/or a higher threat value (i.e. highly motivated threat agent, equipped with necessary capabilities in an opportune moment) will create a high impact or risk to the SME [24].

6.3.4. Model Significance & Applications

This section deals with the direct application and analysis using the CSVA model as the basis for assessing a system of interest. An example is provided herewith to illustrate the significance and applicability of the CSVA model.

Consider 2 SME firms with 2 different servers with vulnerabilities which are exploited by threat agents, as stipulated in Table 6-2 – CSVA Decision Matrix (illustrated)

The first case is a scenario of a consultant hired by an ISP SME for a number of assignments, but had to be terminated abruptly. This guy becomes a threat agent to the firm's network address translation (NAT) server, which is critical to the business operations of the ISP. Should he change the current settings of the server and/or bring down the server the firm risk the loss of revenue and credibility with its customers. Through the assessment, the firm can put in place proactive measures such as changing its passwords and having to backup the NAT server. It is noted that there could be multiple vulnerabilities in the SME's network or with the NAT server that could be exploited by the consultant to violate any of the confidentiality and availability properties (even integrity). Risk here is said to be severe.

During the course of his engagement, the consultant was legitimately authorized to have access to the systems and network of the ISP. Now, immediately upon his dismissal, he still could have access to the systems and thereby takes advantage to tamper with the NAT server and

associated configurations. Another way the consultant might have exploited the system, may be through elevated privilege to have had administrative access and/or he might have installed a rootkit to provide a backdoor, which is not uncommon with most consultants.

Table 6- 2: CSVA Decision Matrix (illustrated)

Vulnerabilities	Threat Agents			Assets Value			Risks (impact)	Remarks
Confidentiality & Availability	Motivation	Capability	Opportunity	Impact	Urgency	Criticality		
Availability	Consultant whose contract is terminated	Techie	Has had access to IPs and have insights into systems	Tampers with current settings & brings down system	To be restored within 1 hour	Critical business asset	SEVERE	NAT server: Vulnerabilities = {slightly vulnerable}; Threat agent = {very-high}; Asset value = {critical}
	Customer who feels cheated by firm & intends to cause harm	Tech savvy customer	Very attractive	Defaced or brought down	To be repaired within 2 hours	Vital business asset	MAJOR	Web server: Vulnerabilities = {vulnerable}; Threat agent ={high}; Asset value = {vital}

The second case concerns a marketing firm that has treated a customer unfairly. This customer is assumed to be tech-savvy and intends to deface or bring down the website. The web server is deemed by the firm as vital to the business operations. Assuming, the customer downloads a couple of exploits from the Web, e.g. exploits for SQL (structured query language)

injection or PHP shell code scripting or XSS (cross-site scripting). The vulnerabilities could have come about as a result of, say, weak passwords, third-party pop-ups or applications on the website, or an out-dated antivirus software or unpatched firewall.

By executing the exploit, the SME's website could be defaced. Mitigation measures to be taken include, choosing strong passwords as well as periodic changing of passwords, patch management and updating of relevant applications and software, such as third-party applications, antivirus software and firewall. It is also imperative that the right access controls are implemented. Through the assessment, here again, mitigation measures could be put in place to either appease the customer or as described earlier, to fortify the web server. Risk here is said to be major.

Threat agents succeed in their attacks to assets, which cause adverse impacts whenever the assets are vulnerable. The CSVA model evaluates the types, sources and severity of vulnerabilities and ensures that the identified critical assets are adequately protected. Proactive prevention and detection techniques are recommended to be in place to minimize the susceptibility of vulnerabilities.

The CSVA model provides a step-by-step comprehensive review, identification and prioritization of the potential threats to ascertain the possibility and severity of occurrence.

In practice, it may be very difficult to estimate the asset value of data, for example, and so the time value (which is utility value) required to restore a corrupted data may be used instead.

West [225] posits that a company with a web portal exposes the company's assets to all manner of threat agents. It's attractiveness is said to be directly proportional to what's at stake. For example, an e-commerce entity is a bit more attractive in view of its handling of credit cards and financial information of customers.

A number of factors influence the type and strength of the security measures put in place to protect the assets. They include asset value, the extent and severity of the consequences, the attractiveness of the assets, and the vulnerabilities at stake.

These could be elicited from asset custodians in the organization and/or through some historical data, if available.

The ensuing section deals with experts opinion elicitation and its analysis for mitigating vulnerabilities.

6.4. Experts Opinion Elicitation

The essence of the strategic interviews was to elicit expert opinions to formulate expert knowledge for the fuzzy rule-base inference of the neuro-fuzzy model and also to aggregate consensus for the evaluation of taxonomy of threats and vulnerabilities. Here, the 14 respondent experts' opinions are aggregated into a group consensus opinion. First, the index of consensus of each expert relative to other experts are defined using fuzzy similarity measures. Opinions were aggregated based on both the index of consensus and the relative importance of the experts.

The issue at stake is such that each expert has ranked the assets, vulnerabilities and the threat agents by their own subjectivity and perceived knowledge. This explains the essence of using fuzzy based multi-attribute decision making approach in estimating the consensus aggregation function. Within the multi-attribute decision-making techniques, a couple methods are utilized in the final evaluation or ranking of the taxonomies.

Experts Opinions Aggregation

Utilizing the equations from [2-3], [2-4] and [2-5] in chapter 2, and underlying principles, the sample space is the 14 experts, i.e. E_i $(i = 1,2, \ldots\ldots, 14)$ evaluating SMEs with cyber-security challenges in developing economies. Recalling those equations herewith:

The "importance" mean operator [63] is:

$$\alpha_i = \tfrac{1}{m} \sum \rho_{ij} w_j \qquad [6\text{-}3]$$

To compute the fuzzy confidence levels for experts E_1 and E_2, for instance, are given by

$$\alpha_1 = \frac{1}{m}\left(\rho_{11} w_1 \oplus \rho_{12} w_2 \oplus \ldots\ldots\ldots \oplus \rho_{1m} w_m\right) \qquad [6\text{-}4]$$

and

$$\alpha_2 = \frac{1}{m}\left(\rho_{21} w_1 \oplus \rho_{22} w_2 \oplus \ldots\ldots\ldots \oplus \rho_{2m} w_m\right) \qquad [6\text{-}5]$$

respectively.

A set of attributes used in defining the degree of importance amongst the experts include {education; experience; management; responsibility; independence}. Either one or any combination of these attributes is used in the computations of weights or relative degree of importance.

The experts opinions are analyzed using appropriate aggregation functions, which have special properties, that take real arguments from the closed interval [0 1] and produce a real value in [0 1]. This is denoted by $f:[0,1]^n \to [0,1]$, where the arguments have n components.

It is noted that aggregation functions are sometimes called aggregation operators in some literature [128], with utility in combining inputs that are interpreted as degrees of membership in fuzzy sets, degrees of preference, strength of evidence and support of a hypothesis.

Beliakov et al [128] posit that if any of the aggregation properties fail, the function cannot be considered as an aggregation function, since its output would be inconsistent with any decision support system. Paramount amongst its properties are as follows:

$\forall$ n >1 and $f:[0,1]^n \to [0,1]$

i. $f(\underbrace{0,0,.....,0}_{n \text{ times}}) = 0$ and $f(\underbrace{1,1,.....,1}_{n \text{ times}}) = 1$

ii. $X \leq Y$ implies f(X) $\leq$ f(Y); $\forall$ X, Y $\in [0,1]^n$

The second property is particularly useful in the ranking of attributes as it applied for the taxonomies. The qualitative or ordinal attributes are first converted into a numerical scale and analyzed using the requisite multi-attribute utility techniques.

6.4.1. Fuzzy Multi-Attribute Decision-Making (MADM)

An approach is employed to rank the decision alternatives in multiple attribute decision-making problem of enlisting vulnerabilities and threats as perceived by the experts. The objective is given 6 vulnerabilities and 10 threat agents deduced from the main study as alternatives, then fuzzy MADM techniques are used to rate them in the order of most-to-least.

It is noted herewith that this study chose to use fuzzy triangular numbers, for simplicity and ease of computation. For instance, it can be showed that similar treatment with fuzzy trapezoidal numbers would yield similar results.

Now, let the fuzzy linguistic variables be defined by the tuples $S = \{s_i : i = 1,2,.....,n\}$ such that $s_i < s_j$ iff i $<$ j.

In this study, $S = \{s_1 = very - \min or,\ s_2 =$ minor, $s_3 =$ important, $s_4 =$ vital, $s_5 =$ critical$\}$ and the experts are $E_i = \{E_1, E_2, ..., E_{14}\}$.

From the study (c.f. Appendix A-9), expert E_1 is deemed the most important and assigned relative importance of $r_1 = 1$. Then, relative importance of the other experts, based on education attribute, are $r_2, r_3, ..., r_{10} = 0.8$ and $r_{11}, r_{12}, r_{13}, r_{14} = 0.6$.

Degrees of importance can be computed from the equation

$$w_i = \frac{r_i}{\sum_{i=1}^{n} r_i}; \qquad [6\text{-}6]$$

As an example, for expert E_1, the degree of importance is $w_1 = 1/10.6 = 0.09$. (c.f. Appendix A-9).

For any given fuzzy sets $A = \{a_i\}$ and $B = \{b_i\}, \forall$ i = 1,2, ..., n, the grade of similarity (or agreement degree) of the fuzzy relations is given by

$$S_{(R_i, R_j)} = \frac{\sum_i (a_i \wedge b_i)}{\sum_i (a_i \vee b_i)} \qquad [6\text{-}7]$$

Equation [6-7] is known as the min-max similarity method [226], and the fuzzy sets A and B are said to be approximately equal if and only if (iff), there exists a proximity measure, ε, [227] such that $S_{(R_i, R_j)} \equiv S_{A,B} \leq \varepsilon$.

Another useful method is that of Xu [126] for similarity measure given by

$$S_{(R_i, R_j)} = 1 - \frac{|a_2 - a_1| + |b_2 - b_1| + |c_2 - c_1|}{8q} \qquad [6\text{-}8]$$

Where q = 3 for fuzzy triangular numbers and q = 4 for fuzzy trapezoidal numbers.

It is noted that $S_{(R_i, R_j)} \in [0\ 1]$ and $S_{(R_i, R_j)} \to 1$ implies that R_1 and R_2 are closer to each other. So $S_{(R_i, R_j)} = 1$ iff $R_1 = R_2$ and that also $S_{(R_i, R_j)} = S_{(R_j, R_i)}$

Assume that the fuzzy set $X = \{x_1, x_2, ..., x_n\}$ be the set of alternatives and $U = \{u_1, u_2, ..., u_m\}$ be the set of attributes. Then for a given degree of importance or weights vector $w = \{w_1, w_2, ..., w_m\}$; $\forall$ $w_i \geq 0$; i = 1,2, ..., m. the linguistic decision matrix or agreement fuzzy matrix (AM) is computed as

$$AM_{mxn} = \begin{bmatrix} S_{11} & S_{12} & & S_{1n} \\ & & & \\ S_{m1} & S_{m2} & & S_{mn} \end{bmatrix} \quad [6\text{-}9]$$

or $AM_{mxn} \equiv (a_{ij})_{mxn}$ where $a_{ij} = [a_{ij}^a \;\; a_{ij}^b \;\; a_{ij}^c] \in S$ is the attribute value, which takes the form of a fuzzy triangular linguistic variable, given by the decision maker, for the alternative $x_j \in X$ with respect to the attribute $u_i \in U$. It follows that for a vector of attribute values $a_j = (a_{1j}, a_{2j}, ..., a_{mj})$ it corresponds with the alternative $x_j : j = 1,2,....., n$.

There exists an ideal point of attribute values, where $I_i = [I_i^a, I_i^b, I_i^c]$ such that $I_i^a = \max\{a_{ij}^a\}$, $I_i^b = \max\{a_{ij}^b\}$, $I_i^c = \max\{a_{ij}^c\}$.

Details of the data collected from the strategic expert opinions elicited as follow-up on the main survey are in Appendices A-7 and A-8.

Using the data on the 14 experts, 6 key cyber-security vulnerabilities were identified and enlisted in the order of most-to-least susceptible vulnerabilities. Similarly, the lists of top 10 most common threat agents (vectors) of cyber-security compromises that affect the SMEs were deduced.

6.4.2. Key Vulnerabilities

This sub-section deals with the actual computations leading to the ranking of vulnerabilities in the taxonomy.

First the attributes are assigned fuzzy triangular numbers and weights vector based on the relative frequencies [228], $w = (0.50, 0.50)$. Note that there were only 2 attributes of {criticality, urgency}.

The vector of alternatives, however, were 6 vulnerabilities in assets; thus $X_j (j = 1,2,.....,6)$ are deduced. For example, $a_{11} = (6.57 \;\; 7.82 \;\; 9.07)$, $a_{21} = (7.86 \;\; 8.89 \;\; 9.93)$.

From here, the ideal points are also determined $\hat{I} = (\hat{I}_1, \hat{I}_2, ..., \hat{I}_{10})$ where $\hat{I}_i = \max_j \{a_{ij}\}$. This implies that $\hat{I}_1 = (7.86 \;\; 8.89 \;\; 9.93)$ and $\hat{I}_2 = (7.29 \;\; 8.46 \;\; 9.64)$ etc.

The similarity measures $\hat{Z}_j$ are computed for each of the attributes and then the overall values as well. Thus,

$$\hat{Z}_j = \sum w_i a_{ij}$$
$$where \text{ i} = 1,2 \text{ and j} = 1, 2, ..., 6 \quad [6\text{-}10]$$
$$\Rightarrow \quad \hat{Z}_1 = w_1 a_{11} \oplus w_2 a_{21}$$

Computing the overall as

$$\hat{Z}_* = w_1 \hat{I}_{11} \oplus w_2 \hat{I}_{21} \oplus ..... \oplus w_6 \hat{I}_6 \quad [6\text{-}11]$$

Where $w = (0.10 \;\; 0.14 \;\; 0.24 \;\; 0.20 \;\; 0.15 \;\; 0.17)$ is obtained from the relative importance (computed for the taxonomy of threats).

$$\Rightarrow \quad \hat{Z}_* = (7.46 \quad 8.51 \quad 9.67)$$

The similarity degrees of the alternatives are subsequently determined as in Table 6-3 below:

Table 6- 3: Results of Similarity Measures on Vulnerabilities Taxonomy

$\hat{Z}_i$	Fuzzy Triangular Number	Ideal Point $\hat{I}_i$	Fuzzy Triangular Number	$S_{(\hat{Z}_*, \hat{Z}_i)}$	Min-Max Method	Xu's Method
$\hat{Z}_1$	(7.21 8.36 9.50)	$\hat{I}_1$	(7.86 8.89 9.93)	$S_{(\hat{Z}_*, \hat{Z}_1)}$	0.961	0.957
$\hat{Z}_2$	(6.11 7.48 8.86)	$\hat{I}_2$	(7.29 8.46 9.64)	$S_{(\hat{Z}_*, \hat{Z}_2)}$	0.990	0.990
$\hat{Z}_3$	(7.36 8.46 9.57)	$\hat{I}_3$	(7.57 8.68 9.79)	$S_{(\hat{Z}_*, \hat{Z}_3)}$	0.985	0.984
$\hat{Z}_4$	(6.89 7.84 9.04)	$\hat{I}_4$	(7.57 8.29 9.50)	$S_{(\hat{Z}_*, \hat{Z}_4)}$	0.980	0.979
$\hat{Z}_5$	(7.18 8.32 9.47)	$\hat{I}_5$	(7.86 8.89 8.93)	$S_{(\hat{Z}_*, \hat{Z}_5)}$	0.961	0.957
$\hat{Z}_6$	(6.18 7.52 8.86)	$\hat{I}_6$	(6.71 8.04 9.36)	$S_{(\hat{Z}_*, \hat{Z}_6)}$	0.940	0.936

Therefore ranking the alternatives of vulnerabilities:

$$X_2 > X_3 > X_4 > X_1 \approx X_5 > X_6$$

The taxonomy of vulnerabilities, inherent in cyber assets, as perceived by SMEs in developing economies are from the most likely susceptible to the least, as follows:

i. DNS Servers
ii. Databases

iii. Email Servers
iv. Core Switches
v. Routers
vi. Web Servers

Based on the study, the above listed assets are said to have diverse forms of weaknesses and are susceptible to attacks that would violate or compromise the CIA security properties.

The ensuing section presents similar treatment for the taxonomy of threats.

6.4.3. Key Threats

This sub-section deals with the actual computations leading to the ranking of threat agents in the study.

First, the attributes are assigned fuzzy triangular numbers and weights vector based on the relative frequencies, $w = (0.10,\ 0.14, 0.24, 0.20, 0.15, 0.17)$; from the expert opinion elicitation.

The vector of alternatives for each threat agent is $X_j (j = 1,2,.....,10)$ are deduced. For example, $a_{11} = (4.5 \quad 6.39 \quad 7.78)$, $a_{21} = (5.43 \quad 6.82 \quad 8.21)$, $a_{31} = (6.93 \quad 8.03 \quad 9.14)$, etc.

From here, the ideal points are also determined $\hat{I} = (\hat{I}_1, \hat{I}_2, ..., \hat{I}_{10})$ where $\hat{I}_i = \max_j \{a_{ij}\}$. This implies that $\hat{I}_1 = (6.93 \quad 8.03 \quad 9.14)$ and $\hat{I}_2 = (5.43 \quad 6.72 \quad 8.0)$ etc.

The similarity measures $\hat{Z}_j$ are computed for each of the attributes and then the overall values as well. Thus,

$$\hat{Z}_j = \sum w_i a_{ij}$$
$$where\ \text{i} = 1,2, ..., 6 \text{ and } \text{j} = 1, 2, ..., 10 \qquad [6\text{-}12]$$
$$\Rightarrow \ \hat{Z}_1 = w_1 a_{11} \oplus w_2 a_{21} \oplus ..... \oplus w_6 a_{61}$$

Computing the overall as

$$\hat{Z}_* = w_1 \hat{I}_{11} \oplus w_2 \hat{I}_{21} \oplus ..... \oplus w_{10} \hat{I}_{10} \qquad [6\text{-}13]$$

Where w_i is obtained from the relative importance.

$$\Rightarrow \ \hat{Z}_* = (6.12 \quad 7.40 \quad 8.68)$$

The similarity degrees of the alternatives are subsequently determined as in Table 6-4 below.

Table 6- 4: Results of Similarity Measures on Threats Taxonomy

$\hat{Z}_i$	Fuzzy Triangular Number	Ideal Point $\hat{I}_i$	Fuzzy Triangular Number	$S_{(\hat{Z}_*,\hat{Z}_i)}$	Min-Max Method	Xu's Method
$\hat{Z}_1$	(5.85 7.11 8.37)	$\hat{I}_1$	(6.93 8.03 9.14)	$S_{(\hat{Z}_*,\hat{Z}_1)}$	0.96	0.96
$\hat{Z}_2$	(4.74 6.10 7.46)	$\hat{I}_2$	(5.43 6.72 8.00)	$S_{(\hat{Z}_*,\hat{Z}_2)}$	0.82	0.84
$\hat{Z}_3$	(3.53 5.06 6.59)	$\hat{I}_3$	(4.93 6.40 7.86)	$S_{(\hat{Z}_*,\hat{Z}_3)}$	0.68	0.71
$\hat{Z}_4$	(5.77 7.03 8.30)	$\hat{I}_4$	(6.64 7.85 9.06)	$S_{(\hat{Z}_*,\hat{Z}_4)}$	0.95	0.95
$\hat{Z}_5$	(4.87 6.22 7.58)	$\hat{I}_5$	(5.78 7.10 8.42)	$S_{(\hat{Z}_*,\hat{Z}_5)}$	0.84	0.85
$\hat{Z}_6$	(5.51 6.80 8.10)	$\hat{I}_6$	(6.80 7.90 9.00)	$S_{(\hat{Z}_*,\hat{Z}_6)}$	0.92	0.93
$\hat{Z}_7$	(5.69 7.07 8.45)	$\hat{I}_7$	(6.40 7.65 8.90)	$S_{(\hat{Z}_*,\hat{Z}_7)}$	0.96	0.96
$\hat{Z}_8$	(4.25 5.76 7.27)	$\hat{I}_8$	(5.40 6.95 8.50)	$S_{(\hat{Z}_*,\hat{Z}_8)}$	0.78	0.80
$\hat{Z}_9$	(3.34 4.93 6.52)	$\hat{I}_9$	(4.90 6.40 7.90)	$S_{(\hat{Z}_*,\hat{Z}_9)}$	0.67	0.69
$\hat{Z}_{10}$	(6.91 8.07 9.23)	$\hat{I}_{10}$	(8.00 9.00 10.00)	$S_{(\hat{Z}_*,\hat{Z}_{10})}$	0.92	0.92

Therefore ranking the alternatives of threat agents:

$$X_1 \approx X_7 > X_4 > X_6 \approx X_{10} > X_5 > X_2 > X_8 > X_3 > X_9$$

The list of threats as perceived by SMEs in developing economies are from the most likely threats to the least, as follows:

i. Natural disasters
ii. Poor authentication
iii. Viruses and malware
iv. Hacking
v. No backup
vi. Spyware and adware
vii. Power failure
viii. Un-scanned attachments
ix. Spam
x. Social engineering.

The next section discusses the evaluation of vulnerabilities with ICT assets disposal policies using fuzzy cognitive maps (FCMs).

6.5. Fuzzy Cognitive Map (FCM) Analysis

In addressing some of the key research questions, 6 constructs were subjected into further scrutiny and that is the import of this section. The issues are, how do SMEs ensure that the end-of-useful-life assets they disposed of would not create security challenges for them? Are there elaborate policies to deal with cyber threats? Do SMEs have an idea of vulnerabilities or threats due to asset disposal? How do SMEs dispose of corporate information? And finally, do they use outside disposal contractors?

The study evaluated the possible vulnerabilities of ICT asset disposal policies and the associated impact on SMEs. There are limited historical data on the assessment of vulnerabilities caused by indiscriminate disposal of ICT assets. As a result of the deficiency, a form of uncertainty is created and methods employing fuzzy set theory become handy. Fuzzy Cognitive Maps (FCMs) was used to evaluate the relationships between the policies and vulnerabilities that confront SMEs in developing economies. The FCM approach analyzed the policies (as concepts) using expert's opinion and basic fuzzy matrices to capture the latent knowledge inherent in detecting cyber-security vulnerabilities. By using fuzzy matrices and directed graphs tools the perceived correlations between the asset disposal policies and vulnerabilities were established.

The following section discusses the detail evaluation of vulnerabilities associated with the asset disposal policy using FCM.

6.5.1. FCM Evaluation of Vulnerabilities

The Table 6-5 (as cited in [215]) depicts the data collected from the survey of SMEs in two developing economies. It consists of 89 sampled respondents on policies on information asset disposal, Internet use and remote access.

Table 6- 5: Vulnerabilities Associated With Asset Disposal Policies

	Physical Disposal Policy	E-Waste Disposal Policy	Regulation & Compliance Policy	Acceptable Use Policy	Duly Signed Policy	Remote Access Policy
Low risk	37	25	24	34	17	37
	0.42	0.28	0.27	0.38	0.19	0.42
Moderate risk	34	27	27	37	41	35
	0.38	0.30	0.29	0.42	0.46	0.39
High risk	18	37	38	18	31	17
	0.20	0.42	0.44	0.20	0.35	0.19

"The top lines for each category contain the actual counts or frequency of the 89 respondents in the survey. The data depict the levels of vulnerability, by the fuzzy tuples {low-risk, moderate-risk, high-risk}, in respect of perceived impact of each construct or policy. For example, a high risk vulnerability is seen as that which could potentially allow a threat agent to compromise a mission-critical asset. The bottom lines depict the fuzzified values for each construct. Thus, three vectors (or matrices) are derived from the data table" [215].

The normalization of the data is as follows. The normalized values are given by the equation,

$$x_n = a + \frac{(x_i - A)(b-a)}{(B-A)} \qquad [6\text{-}14]$$

Where, x_i is the data to be normalized; a is the minimum normalized scale value (here $a = 0$ is chosen); b is the maximum normalized scale value (here $b = 1$ is chosen); A is the minimum possible value in the data set (here $A = 0$); B is the maximum possible value in the data set (here $B = 89$). Note that, the values of a and b are in accordance with fuzzy set theory, such that the membership values map onto the (unit interval) set [0 1].

A fuzzy relationship between two or more sets is an expression of association, interrelationship, interconnection, or interaction amongst the sets [18] (as cited in [215]). Accordingly, there is a degree of presence (or belief about the existence) or absence (or non-existence) of such relations [211] (as cited in [215]). That degree of presence in the relationship $\mathbf{R}$ between two constructs $\mathbf{A}$ and $\mathbf{B}$, is given by $\mathbf{R(A,B)}$ or $\mu_R \in [0,1]$ such that μ_R (a, b) ∈ [0, 1]. In applying the principles for analysis, the empirical data is fuzzified or normalized in view of perceived "belief" in the existence of some relations amongst the constructs [215].

Also, in order to ensure that any relationship existing between any constructs were not due to pure chance, the Chi-square statistic tests is applied on the data [215].

The results for a significance of 0.05, at degrees of freedom (DF) of 10, were as follows [215]:

- Pearson's Chi-square, $\lambda^2 = 35.071$; p-value = 0.000121
- Yates' Chi-square = 30.999; Yates' p-value = 0.000587

The critical value at the significance of 0.05 is 18.307. Since $\lambda^2 \geq 18.307$, it is inferred that any relationships between the variables are not due to chance.

In order for the product of the two matrices to be defined, the number of columns in the 1st matrix must be equal to the number of rows in the 2nd matrix. Now, let

$\mathbf{Y}_{low} = \{0.42 \quad 0.28 \quad 0.27 \quad 0.38 \quad 0.19 \quad 0.42\}$ be a fuzzy set of low-risk vulnerable parameters; $\mathbf{Y}_{\text{mod}} = \{0.38 \quad 0.30 \quad 0.29 \quad 0.42 \quad 0.46 \quad 0.39\}$ be a fuzzy set of moderate-risk vulnerable parameters; and $\mathbf{Y}_{high} = \{0.20 \quad 0.42 \quad 0.44 \quad 0.20 \quad 0.35 \quad 0.19\}$ be a fuzzy set of high-risk vulnerable parameters [215].

Note that, the augmentation matrices are permuted to facilitate meaningful aggregation of the vulnerability rankings – for which the FCM as a tool, has aggregation functionality [201] [202] (as cited in [215]). Kandasamy et al. [202] (as cited in [215]) posits that all matrices associated with an FCM are always square matrices of dimension which is equal to the total number of distinct concepts or events used by the experts, and with diagonal elements as zero.

The fuzzy matrix relation R ($\mathbf{Y}_{low}, \mathbf{Y}_{\text{mod}}$) is given as [215]:

$$\begin{bmatrix} 0.42 \\ 0.28 \\ 0.27 \\ 0.38 \\ 0.19 \\ 0.42 \end{bmatrix} \begin{bmatrix} 0.38 & 0.30 & 0.29 & 0.42 & 0.46 & 0.39 \end{bmatrix} = \begin{bmatrix} 0.16 & 0.13 & 0.12 & 0.18 & 0.19 & 0.16 \\ 0.11 & 0.08 & 0.08 & 0.12 & 0.13 & 0.11 \\ 0.10 & 0.08 & 0.08 & 0.11 & 0.12 & 0.11 \\ 0.14 & 0.11 & 0.11 & 0.16 & 0.17 & 0.15 \\ 0.07 & 0.06 & 0.06 & 0.08 & 0.09 & 0.07 \\ 0.16 & 0.13 & 0.12 & 0.18 & 0.19 & 0.16 \end{bmatrix} \quad [6\text{-}15]$$

Similarly, the fuzzy matrix relation R ($\mathbf{Y}_{low}, \mathbf{Y}_{high}$) is given as (note that of R ($\mathbf{Y}_{\text{mod}}, \mathbf{Y}_{high}$) is also computed, but not shown here):

$$\begin{bmatrix} 0.42 \\ 0.28 \\ 0.27 \\ 0.38 \\ 0.19 \\ 0.42 \end{bmatrix} \begin{bmatrix} 0.20 & 0.42 & 0.44 & 0.20 & 0.35 & 0.19 \end{bmatrix} = \begin{bmatrix} 0.08 & 0.18 & 0.18 & 0.08 & 0.15 & 0.08 \\ 0.06 & 0.12 & 0.12 & 0.06 & 0.10 & 0.05 \\ 0.05 & 0.11 & 0.12 & 0.05 & 0.09 & 0.05 \\ 0.08 & 0.16 & 0.17 & 0.08 & 0.13 & 0.07 \\ 0.04 & 0.08 & 0.08 & 0.04 & 0.07 & 0.04 \\ 0.08 & 0.18 & 0.18 & 0.08 & 0.15 & 0.08 \end{bmatrix} \quad [6\text{-}16]$$

The matrix $\mathbf{E}_{ixj} = \{e_{ij}\}$, where e_{ij} are the weights of the directed edge $\mathbf{C}_i\mathbf{C}_j$. $\mathbf{E}_{ixj}$ is called adjacent matrix of the FCM or connection matrix of the FCM.

For a finite number k of FCMs, there exist a combined FCM which produces the joint effect of all the FCMs put together. Let $\mathbf{E}_i (i = 1,2,.....,k)$ be the connection matrices of the FCMs with nodes $P_1, P_2, ...P_n$, then the combined FCM is given by adding all the connection matrices:

$$\mathbf{E} = \mathbf{E}_1 + \mathbf{E}_2 + ... + \mathbf{E}_k \quad [6\text{-}17]$$

So the combined connection matrix is given by

$$\begin{bmatrix} 0.32 & 0.46 & 0.47 & 0.34 & 0.47 & 0.32 \\ 0.22 & 0.33 & 0.34 & 0.23 & 0.33 & 0.22 \\ 0.21 & 0.32 & 0.32 & 0.23 & 0.32 & 0.21 \\ 0.30 & 0.45 & 0.46 & 0.32 & 0.45 & 0.30 \\ 0.20 & 0.33 & 0.34 & 0.21 & 0.31 & 0.20 \\ 0.32 & 0.47 & 0.48 & 0.34 & 0.48 & 0.32 \end{bmatrix} \text{ transformed into } \begin{bmatrix} 0.0 & 0.46 & 0.47 & 0.34 & 0.47 & 0.32 \\ 0.22 & 0.0 & 0.34 & 0.23 & 0.33 & 0.22 \\ 0.21 & 0.32 & 0.0 & 0.23 & 0.32 & 0.21 \\ 0.30 & 0.45 & 0.46 & 0.0 & 0.45 & 0.30 \\ 0.20 & 0.33 & 0.34 & 0.21 & 0.0 & 0.20 \\ 0.32 & 0.47 & 0.48 & 0.34 & 0.48 & 0.0 \end{bmatrix}$$

For practical purposes and in accordance with Kandasamy et al [202] (as cited in [215]), the diagonal elements or the self-feedbacks at the edges are all zeroed.

Theoretically, in using the expert's opinion, if an increase in one concept (or policy) leads to an increase in another concept, then the value 1 is assigned. Otherwise, if the effect is negative or decreasing, -1 is assigned. For concepts which have no relation or causative effect on each other, the value 0 is assigned [215].

Kandasamy et al [202] (as cited in [215]) referred to the Fuzzy Cognitive Map (FCM) nodes as fuzzy nodes and assigned the set {-1, 0, 1} to the edge weights or causalities. The concept nodes are used to represent processes, events, values, norms or policies.

To build the asset disposal policy model the following 6 fuzzy nodes of FCM are used [215]:

- P_1 - physical asset disposal policy (e.g. hardware, use of shredder, hard disk drive, etc.)
- P_2 - electronic waste (e-waste) disposal policy (e.g. software, data sheets, hardware, storage media, applications, or intellectual property (IP), etc.)
- P_3 - regulation & compliance policy (e.g. regulation, compliance, asset custodians, data disruption processes, etc.)
- P_4 - acceptable Internet use policy (e.g. do's & don't's of computer usage, websites to visit and not to visit, system updates, etc.)
- P_5 - duly signed employee policy (e.g. all employees are required to sign off on the ICT policies upon engagement in the organization)
- P_6 - remote access policy (e.g. guidance on Intranet or Extranet interconnections, Wi-Fi connections, café usage, etc.)

Using directed graphs (digraphs) to represent the aggregated fuzzy relations of $\mathbf{Y}_{low}$, $\mathbf{Y}_{\text{mod}}$ and $\mathbf{Y}_{high}$. The resulting FCM map or directed graph is shown in Figure 6-2 (as cited in [215]) below:

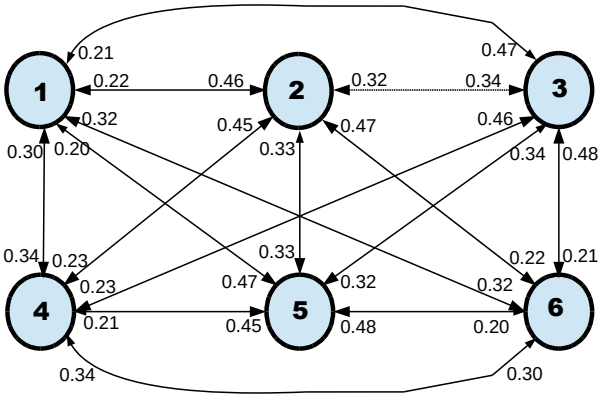


Figure 6- 2: Original FCM Map

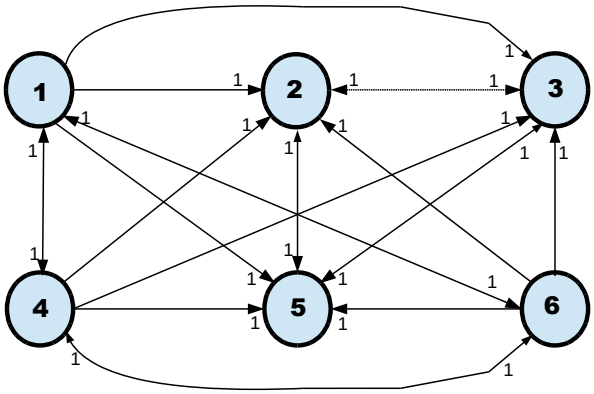


Figure 6- 3: FCM with alpha at 0.25

By choosing the lower percentile α –cut, α = 0.25, the resulting FCM map or directed graph is given in Figure 6-3 above.

Deducing from Figure 6-3 above an expert's opinion is created, a 6x6 causal connection matrix, $\mathbf{E}_{6x6}$, representing the asset disposal policy model using FCM [215].

That is, $\mathbf{E}_{6x6} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$

Since matrix multiplication involves both addition and multiplication, the max-min principle (or operation) for fuzzy matrices were used. In many cases, the algebraic addition "+" is replaced with "max" operation; i.e. instead of (0.5 + 0.7) = 1.2, max (0.5, 0.7) = 0.7 is obtained. Similarly, the algebraic multiplication "x" is replaced with "min" operation; i.e. (0.8 x 0.9) = 0.72, min (0.8, 0.9) = 0.8 is obtained [215].

A vector $\mathbf{A} = \{a_1, a_2, ...a_n\}$ $\forall$ $a_i \in [0,1]$ is known as the instantaneous state vector, denoting the ON-OFF states of the nodes at any given instant; e.g. $a_i = 0 \Rightarrow a_i$ is OFF and $a_i = 1 \Rightarrow a_i$ is ON. Suppose $\mathbf{C} = \{c_1, c_2, ...c_n\}$ is an initial state vector passed through the dynamic system $\mathbf{E}$, then $\mathbf{CE} = (c_1^{'}, c_2^{'}, ...c_n^{'})$. Upon thresholding and updating the vector, suppose the resultant vector is $\mathbf{D} = (d_1, d_2, ...d_n)$ such that $\mathbf{CE} = (c_1^{'}, c_2^{'}, ...c_n^{'}) \mapsto (d_1, d_2, ...d_n)$, where the symbol "↦" implies the resultant vector has been thresholded or non-linearly transformed and updated after each pass [215].

Irrespective of the FCM matrix dimension, the system settles down to a temporal associative memory (TAM) limit cycle or fixed equilibrium point which is an indication of the hidden

pattern of the system. This fixed point inference is a summary of the joint causal effects of all the interacting fuzzy concepts [202] (as cited in [215]).

Now, let the starting input vector is $\mathbf{C}_1 = [1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0]$, representing the physical asset disposal policy. The state vector $\mathbf{C}_1$ is repeatedly passed through the FCM connection matrix $\mathbf{E}_{6x6}$ thresholding and simultaneously updating the result after each pass [215]. Thus,

$$\mathbf{C}_1\mathbf{E}_{6x6} = [0 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1] \mapsto [1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1] = \mathbf{C}_2 \qquad [6\text{-}18]$$

$$\mathbf{C}_2\mathbf{E}_{6x6} = [1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1] \mapsto [1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1] = \mathbf{C}_3 = \mathbf{C}_2 \qquad [6\text{-}19]$$

This indicates that the prevalence of vulnerabilities associated with physical asset disposal results in risks due to regulation and compliance, e-waste and remote use policies. Also, the resultant vector indicates (from the latent patterns) that similar vulnerabilities could manifest from the acceptable use and unsigned policies effects [215].

Similarly, using the acceptable use policy input vector $\mathbf{D}_1 = [0 \quad 0 \quad 0 \quad 1 \quad 0 \quad 0]$, then

$$\mathbf{D}_1\mathbf{E}_{6x6} = [1 \quad 1 \quad 1 \quad 0 \quad 1 \quad 1] \mapsto [1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1] = \mathbf{D}_2 \qquad [6\text{-}20]$$

$$\mathbf{D}_1\mathbf{E}_{6x6} = [1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1] \mapsto [1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1] = \mathbf{D}_3 = \mathbf{D}_2 \qquad [6\text{-}21]$$

Here, the resultant vector indicates that there exist interacting effects of e-waste disposal, regulation & compliance, unsigned and remote use policies, as well as physical asset disposal [215].

The subsequent section discusses some other findings presented in descriptive statistics.

6.6. Other Descriptive Statistics

This section presents the rest of the findings of the study in descriptive statistics.

6.6.1. Other Findings

Enumerated below are some findings from the study:

- Cyber-Security Positions in SMEs - 89.9% have none or no more than 2 persons dedicated to security. (53.9% no positions; only 36% had 1 or 2 positions).
- Security losses within one particular year – 76.4% SMEs had lost at least 1000 US$, whilst over 92% had lost around US$ 10000 per year due to security incidents;
- Unauthorized access or intrusions – 84.3% SMEs had indicated that there had been about 10 unauthorized access per year, whilst about 95% had around 100 intrusions per year.
- The profile of the ICT functionaries and C-level officers who responded to the survey are as follows:
  - 28.6% has first degree; 64.3% has second degree and 7.1% has third degree;
  - 28.6% has worked in the ICT sector for at least 4 years;

- 28.6% has worked between 5 and 9 years in the ICT sector;
- 35.7% has worked between 10 and 15 years in the ICT sector;
- 7.1% has worked for over 15 years;
- 7.1% were associates, whilst another 7.1% were senior associates;
- 50% were managers, whilst 35.7% were either senior managers or chief officers.

The last sub-section concludes the chapter.

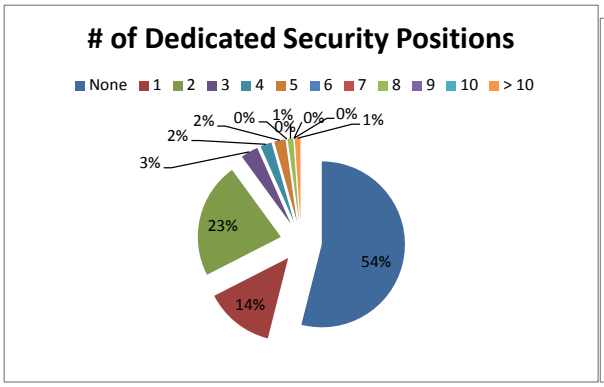


Figure 6- 4: # of Dedicated Security Positions

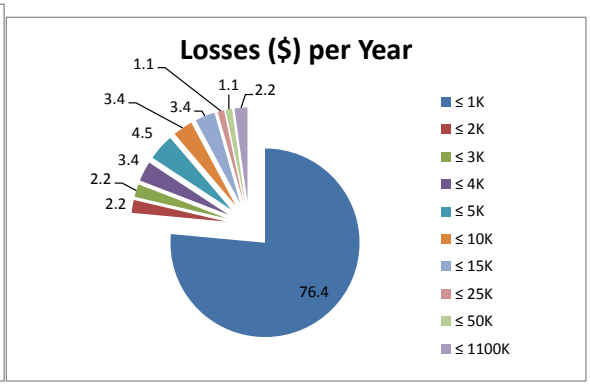


Figure 6- 5: Losses ($) per Year

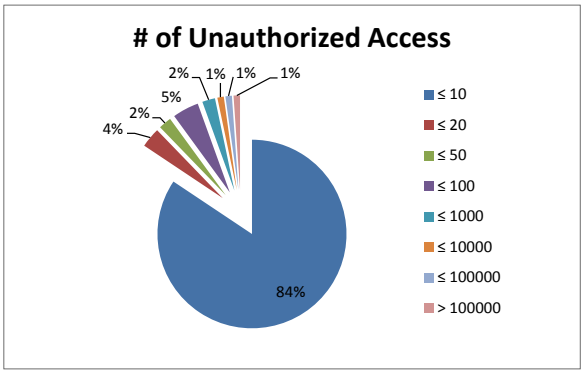


Figure 6- 6: # of Unauthorized Access

There has been attempt to present the results and findings of this study as well as making the efforts to address the research questions of this study. Appendices are used as supporting documentation in reviewing the details of the sample data and some graphs. The actual discussions and conclusions are drawn in Chapters 7 & 8.

Chapter 7 Discussion

"Dear Small Business Owner:

New security issues such as viruses, hackers, and worms come to light in news articles every day and underline the importance of taking preventative measures. These are serious threats with serious consequences. Yet, many small businesses have not taken the steps to safeguard their businesses. In some cases, it's a matter of limited resources. But, in most cases, small business owners are simply unclear as to what steps they should take or even where to start"[19].

Cindy Bates, General Manager,

US Small Business, Microsoft Corporation.

This chapter discusses the study by interpreting and evaluating the empirical findings. It summarizes the discussions and emphasizes on the contributions of the study.

It dilates on the major patterns or trends observed from the study, as well as relationships and generalizations among results obtained.

The key drivers instigating these trends are reviewed. The discussion is taken further by also examining some related works vis-à-vis any agreements or disagreements with contributions in literature. Then, the research findings are interpreted with respect to the research questions, implications of the findings are spelt out, especially, in relation to any unanswered questions.

It also discusses other possible explanations that these findings may be ascribed.

Before drawing conclusions, this chapter clearly presents the study's contributions, as the case may be, offering associated evidence in support of any reasoning and the significance of these findings.

Preamble

In the preceding chapter, a number of assumptions were formulated to underscore the essence of this study. It is recalled that paramount themes that run throughout this study are the fact that cyber-security constructs are assumed to be intangibles and very subjective. This gives credence to the use and treatment of the metrics as fuzzy constructs. The strategic measurement has been the perceptions of the sample SME experts who were surveyed and interviewed using natural language.

[19] *"Security Guide for Small Business", Microsoft Corporation, 2005*

Typically, fuzzy data is expressed in natural languages, e.g. as in the linguistic value "vulnerable" for the fuzzy statement "the router is vulnerable". This fuzzy concept "vulnerable" describes the router's susceptibility or extent of vulnerability from one's perceptive. It assumes that the statement "contains" the true "level of vulnerability" of the router. Since the supposed boundary that "contains" the router's security posture is not sharply defined, it expresses the vagueness or fuzziness in the metric [228]. This approach is intended to capture as much information as possible from these intrinsic cyber-security constructs.

The main research questions raised for the study were:

i. *How do SMEs mitigate the impact of cyber-security compromises of Confidentiality, Integrity & Availability against their assets in developing economies?*
ii. *What risks do compromises of CIA have on business performance and continuity?*

The supplementary questions were:

- Are there elaborate policies to deal with cyber-security vulnerabilities or threats?
- Do SMEs have an idea of vulnerabilities or threats due to asset disposal?
- How do SMEs dispose of corporate information? Do they use outside disposal contractors (outsourced)?
- How do SMEs ensure that the intended recipients have their correspondences intact, safe and at the right time?
- To what extent would these affect the business, if unauthorized persons or entities got their data sheets or pricing strategy?

Having recapped these questions, the following sections will discuss, interpret and evaluate them in relations with the findings.

Summary of Most Important Results

This section summarizes the most important results from this study:

- The cyber-security vulnerabilities assessment (CSVA) model has been designed and built with adaptive neuro-fuzzy inference system (ANFIS) based on MATLAB toolbox. The model has been presented as a schematic description of a system of cyber-security vulnerabilities assessment tool. It accounts for intrinsic or inferred vulnerabilities which upon exploitation would violate the security properties of confidentiality, integrity and availability (CIA); and models threats, asset value, vulnerabilities to risks or impact to SMEs. The model can be used to study further susceptibility characteristics

of cyber-security posture of an organization or information assurance of systems. Finally, the model is presented in a functional and logical manner for ease of application.

- The taxonomies of vulnerabilities and threats using fuzzy similarity measures for multi-attribute decision-making (MADM) techniques have been presented. In the order of the most critical or significant to the least, a list of vulnerable assets is ranked with the most susceptible being the domain name-server (DNS) and the least being the web servers, according to sample data obtained from SMEs in developing economies. Similarly, a list threats is ranked with the most plausible threat being natural disasters and/or poor authentication, and the least being social engineering threats, as afar as the SMEs were concerned.
- The fuzzy cognitive maps (FCMs) evaluation of ICT assets disposal policies and associated vulnerabilities. ICT assets disposed at the end-of-useful life span are susceptible to vulnerabilities associated with data confidentiality. The perceived correlation amongst ICT assets disposal policies have been established using fuzzy cognitive maps (FCMs).

The subsequent sections discuss the findings of this study, their interpretations, their attempts at addressing the research questions formulated for the study, their relationships with other related works as well as their implications.

7.1. Major Contributions in the Study

The section details major trends in the findings and evaluates the observed patterns with respect to related works.

7.1.1. The CSVA Model

The multivariate datasets needed to be pre-processed in a manner that would facilitate easy analysis and subsequent interpretation of the findings. In view of that, the correlated variables of vulnerabilities and threats were aggregated. The methods of aggregation used for the vulnerabilities and threat constructs were fuzzy triangular means [63] [64], min and max operators, as well as fuzzified averages and fuzzified min-max operations. Each method created a unique set of data that were used to train and test the CSVA model. Figures 7-1. & 7-2. depict visually the training and checking errors and associated trends as per the 3 system generated membership function techniques (c.f. Table 6-1 in Chapter 6).

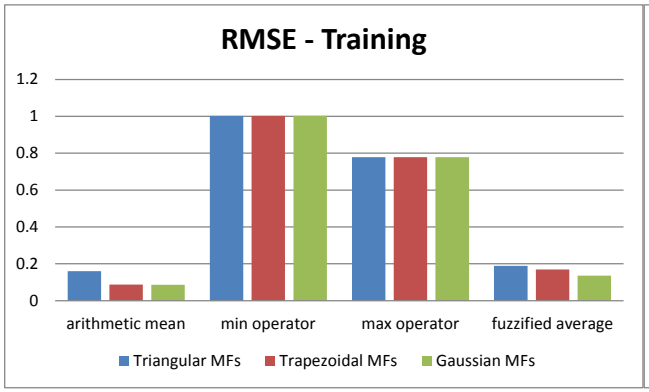


Figure 7- 1: RMS Errors for Training

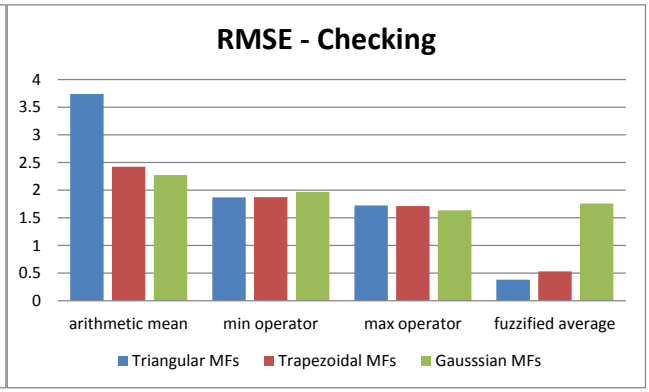


Figure 7- 2: RMS Errors for Checking

By definition, the training error is the difference between the desired output and the computed output from the training, given in root mean square error at each epoch. Similarly, the checking error is the root mean square differences of training samples and that of the checking samples, when they are fed concurrently into the system during training epoch.

The checking dataset is used to validate the model, as a means of evaluating how well the model can predict dataset without necessarily over-fitting it. The checking dataset is selected such that it is both representative of the dataset to be modeled, and yet distinct enough to make the validation reliable. In the event of over-fitting, the checking error will suddenly increase whilst the training error decreases. After the validation, the model is verified using the testing dataset to ascertain the generalizability of the model.

It was observed that in all cases (irrespective of datasets), the training errors due to fuzzy arithmetic means were lowest, whereas that of the min operator were the highest (see Fig. 7-1.). Also, it was observed by closely examining the checking error sequence during the training session, that the fuzzified average dataset exhibited tendencies of over-fitting as its checking error increased whilst the training error decreased [229].

The dataset generated by FIS rule-base was done with fuzzy grid partition algorithm in ANFIS toolbox. Here, the input variable spaces are dynamically divided into fuzzy partitioned subspaces [220] [104]. It generates rules such that all possible combinations of input membership functions are utilized, thus leading to the “curse of dimensionality”. The curse of dimensionality is a problem associated with fuzzy rule-base systems such that the number of possible rules is exponentially proportional to the number of fuzzy input sets and related linguistic terms [229]. However, the alternate algorithm – subtractive clustering, which produces scattering partitions was found to be unsuitable with the model. When used, the training session almost immediately ended, giving an indication of possible over-fitting or unsuitability.

If linear relations exist amongst the antecedent rule components, then the Sugeno method is ideal for the model. In which case, the Sugeno FIS would be efficient interpolating the presence of vulnerabilities with the threats. In spite of the above, the Sugeno FIS can still model non-linear systems by using adaptive techniques to customize the membership functions for the construction of the model [220]. Its advantages are compactness and computational efficiency than the Mamdani system [104].

Finally, the CSVA model was best modeled using the Gaussian membership functions as seen from the errors and due to fine-tuning of the antecedent parameters, thus optimizing the prediction accuracy [230].

7.1.2. Vulnerability Assessment

In fuzzy multi-attribute decision-making situations, as is the case with the 14 cyber-security experts, whose opinions or perceptions were elicited in the strategic interviews, each expert has an individual (a unique) perception on any criterion. Each expert comes to the bench of group judgment with varied backgrounds and expertise in cyber-security. That necessitated the computations of relative degrees of importance of each attribute or criterion as well as the degree of optimism or confidence level of each expert, in order to factor in the preferences of experts [126] [209].

Having assumed that these experts were representative of the sample population, the consensus or group or "social choice" [104] decision is made in respect of the most-to-least attribute as perceived by the experts.

The following assets are ranked based on perceived vulnerabilities and threats, as observed from the study:

i. {DNS servers > Databases > Email servers > Core switches > Routers > Web servers}
ii. {Natural disasters > Poor authentication > Viruses (Malwares) > Hacking > No Backup > Spywares (Adwares) > Power failure > Un-scanned attachments > Spam >Social engineering}

The list of vulnerabilities is discussed first, then that of threats. The approach here is to give a very concise background of the assets and discuss the interesting rankings of these challenges.

The following section discusses the trends in the list of vulnerabilities as observed from the survey in relation to the literature.

Taxonomy of Vulnerabilities Discussed

i. Domain Name Service (DNS) is a server that translates or resolves host names to IP addresses. It has a special and important role in the proper functioning and integrity of the Internet communications framework. The Internet is organized in a hierarchical structure with 13 Root DNS servers (*caveat: DNS servers herewith are NOT Root DNS servers*). These are lower-level DNS servers, usually owned by ISPs or businesses. DNS server was ranked as the most susceptible, which implies that DNS servers are most vulnerable for the sampled data.
It is very likely that most of these experts were ISPs or businesses like banks (in the category of SMEs) that can own DNS servers. DNS vulnerabilities include DNS spoofing or cache poisoning, remote code execution [231], DNSChanger Trojan (www.DNSChanger.com) and others (www.HostExploit.com, 2010).

ii. Databases – are collections of data. They are invaluable assets that store and manage SME data, as well as analyze data from archival or historical sources [127].
Young & Aitel [232] posit that databases are amongst the most vulnerable softwares "on the planet, despite any marketing claims of "unbreakability"". Most databases are prone to similar vulnerabilities such as buffer overflows, end-user input validation issues, default configuration weaknesses, authentication issues, SQL injection, etc. [232] [233] [3] [27].

iii. E-Mail server – email service is at the forefront of Internet applications; every firm who uses the Internet has some form of mail server for communications. Some mail servers' vulnerabilities could grant administrative access rights to intruders who could use email accounts for any nefarious activities. Because of its central role in business communications, it is also very attractive to a number of attacks. Some mail server vulnerabilities include buffer overflows, login failures, configuration issues, remote code execution [234].

iv. Core Switches – provide high-speed switching and traffic aggregation points, usually serving as gateways to the networks. They also offer reliable connections to resources on the network. It must be noted that the term "core" refers to the centrality as the device in the network responsible for LAN connections for the SME. Depending on one's setup, other modules such as wireless access modules could be added to the core switch for the purposes of network performance, and not security. For example, some networks may have Cisco 6509 or Cisco 3750 as their core switch. They may be referred to as edge or backbone or gateway switches. Apart from configuration issues, vulnerabilities with core switches center on VLAN hopping, code execution, MAC address spoofing [235].

v. Router is a special purpose device that routes both in-coming and out-going traffic to appropriate destinations based on decisions from routing tables or policies. Some vulnerabilities include misconfiguration or default configuration, session hijacking, CSRF (cross site request forgeries) with default passwords.
Kavalla [236] posits that some of the router vulnerabilities are embedded services or applications most of which are susceptibly or inadvertently enabled by default. The router therefore can only be made "secured" by disabling these services.

vi. Web server – in today's cyber-economies, virtually all competitive SMEs have a web presence. Whether they host the service or are hosted by a third party is another issue. The concern here is that there is a web portal, which is managed, most likely by the end-user. Most of the vulnerabilities with web servers are, of course configuration and managed hosting related. Cisco's [237] assessment of network protocols revealed that most servers were either outdated or had inherent vulnerable web applications at installations.
Cisco Security Consulting [237] ranked Internet services vulnerabilities based on its 'most dangerous' formula with mail server (61.1%) followed by web server (42.4%), followed by DNS (35%) in the order of most susceptible to the least, where most dangerous = most common + most vulnerable.
Strassman [238] posits that the infrastructure of the Internet is intrinsically vulnerable, due in part to its engineering of the core switches, routers and general network connections which are usually owned and/or managed by ISPs and Telcos. He argues that vulnerabilities may result from malfunctions of the Internet infrastructures, which in turn could affect core switches and routers. This lends credence to the attractiveness of core switches and routers to threat agents.

7.1.3. Threats Assessment

This section discusses the trends in threats observed from the study in relation to literature. The threats discussed are:

i. Natural Disasters – this encompasses any event considered as force majeure in legal parlance or business settings, including flood, earthquake, fire outbreak and excavations. Karley [239] asserts that heavy rains in Accra, Ghana, for example, hamper economic activities and "telecommunications [infrastructure] are submerged in waters." The threats of floods in Ghana and Nigeria are perennial events (c.f. www.ghanadistricts.gov.gh alludes to the fact, citing "similar incidents were recorded in 1995, 1997 and 2001") [240].

CORDIS [241] in its project on "Advancing ICT for Disaster Recovery Management (DRM) in Africa" attests to the impact of natural disasters on ICT infrastructure, writing:

> "*Many developing countries in Africa are exposed to serious natural disaster risks and their need for an adequate ICT infrastructure supporting DRM is high. Unfortunately, access to ICT knowledge and affordable ICT systems is often lacking.*"

ii. Poor authentication – the authentication implemented in most networks or systems are the single-factor type, where username and password is required before granting access to the end-user. This behooves enormous responsibility on the end-user to be cautious in choosing and administering his/her password. For systems or resources that are sensitive, it is incumbent upon the systems administrator to procure multi-factor authentication techniques, such as hardware (e.g. smartcard) and/or software (e.g. digital certificates & tokens) second-factor or third-factor (e.g. biometrics), which can ensure higher levels of security assurance for the systems. Stronger passwords can be used with extended strings coupled with alphanumeric and special characters [27].
An exploratory analysis of the type of authentication techniques used by the SMEs revealed that most of them (80%) used single-factor authentication or lesser mode, as depicted in the Figure 7-3.

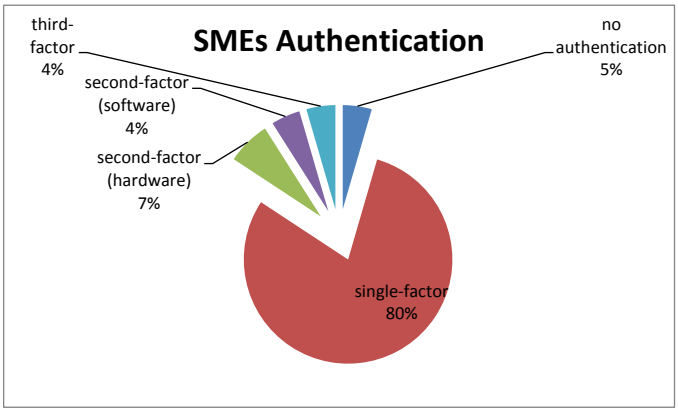


Figure 7- 3: SMEs Authentication Techniques

iii. Malware – is a term for malicious code or software, with the commonest forms as viruses and worms, which attacks computer systems or networks [242]. Depending on the type and purpose of the malware, they may self-propagate and self-replicate (e.g. worms), self-discover (or has the ability to scan and discover other vulnerable assets, e.g. bots). The infection with malware may start by opening an attachment of an email. Some come through installation of software that have been compromised or are themselves malwares.
The OECD [243] best describes what a malware is:

> *"Malware can gain remote access to an information system, record and send data from that system to a third party without the user's permission or knowledge, conceal that the information system has been compromised, disable security measures, damage the information system, or otherwise affect the data and system integrity."*

At the advent of computer malware, it was more of a nuisance to the end-user than a realized risk. With advancement in computer technologies, malware have become very dangerous and disruptive due to their stealthy operations and sophistication.

Bots are typically scripts or programs with the capability to perform predefined functions repeatedly and automatically after being triggered intentionally or through a system infection [244]. Originally, bots were intended as a useful program for repetitive automated and time consuming tasks, such as search engines, coordinating file transfers and online games, but now they are used for malicious code distribution.

For example, botnets have evolved as mere malware using Internet relay chat (IRC) protocols [245] to simulate distributed denial-of-service (DDoS) attacks, with great difficulty to trace and apprehend the botherder [246] [247].

The malware can exploit systems in a number of ways including through executable codes, through unpatched software, backdoors, brute force attacks, emails, unauthorized instant message, infected website, etc. Most malwares are transmitted like normal web traffic using regular ports, so as to evade firewalls and intrusion detection systems (IDS) [248].

iv. Hacking – is a process of breaking into one's system or decrypting a password, or by accessing one's network without authorization. Technically, any system can be hacked from anywhere via the Internet by exploiting identified vulnerabilities. Some of these vulnerabilities include a susceptible modem behind a firewall, weaknesses in TCP/IP and NetBIOS, exploiting an insecure wireless network, port scanning, packet sniffing, clickjacking, etc.
The erroneous notions that hackers look for secrets, or "there's nothing attractive about one's network", have to be discarded. On the contrary, hackers take advantage of unprotected systems and may hack into systems for different reasons, including gaining access to financial information, intellectual property, or corporate sensitive information, etc. [232].

v. No Backup – backup is a process of archiving data or making copies of programs or data unto separate storage media or additional resources for the purposes of being used for restoration or recovery, and usually keeping them out-of-site for business continuity reasons. In the event of exploitation or attack, backups can be very useful to restore failed systems and/or restore corrupted data. Backups can greatly mitigate risks if the backups are robust and reliable [27]. Incidentally, most firms or end-users do not backup regularly (outdated copies) nor store off-site.

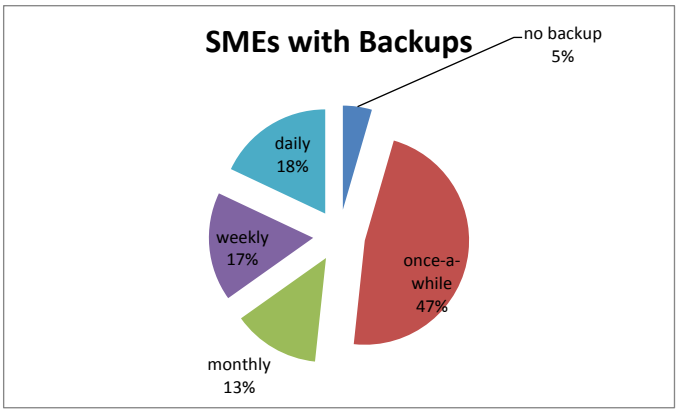


Figure 7- 4: SMEs Backup Trends

An exploratory analysis into the study revealed that 52% seldom backup, 13% backup monthly, 17% weekly whilst 18% backup daily (see Figure 7-4), which compares with the mere 30% of Kenyan SMEs who backup regularly [249].

vi. Spyware – spyware is a form of malware that spies on the user by stealthily collecting predefined user data for further actions [232]. They are usually installed unknowingly through web browsing or unprotected installations or downloads, especially as bundled freewares or peer-to-peer (P2P) applications. Typical examples of spyware are keystroke loggers, instant messaging (IM) aggregators, etc. Adwares are not quite distinct from spyware except that they are usually used by some marketing firms (called sponsors) to collect information on users. The sponsors earn revenue through these adverts. They usually come in the form of pop-ups, "sponsored" freewares, toolbars, etc.

vii. Power failure – is the event of power supply outage to the ICT resources. It can be augmented with standby diesel engine generators (DEGs) or uninterruptible power supply (UPS) or solar cell power supplies to hold forth and supply power to essential resources in the event of outages. The augmented power supply is usually installed in functionally hot-standby mode, i.e. upon sensing commercial power failure, the standby units take-over automatically. In fact, due to the sensitive nature of the essential communications resources, the power supply is usually "sensitive" to power fluctuations and that any fluctuations outside the tolerance range are cut-off for smooth take-over by the conditioned UPS or other standby supply. For typical data centers or

server farms, there are at least 2 different sources of UPS to ensure seamless switchovers [27].

viii. Un-scanned Attachment – when users open attachments to email messages without scanning them with up-to-date anti-virus software, malware could be downloaded, or executed on the user's system. This may lead to exploitation of information stored on the system. In the corporate environments, most firms have policies dealing with email attachments. However, some end-users ignore or violate the policies and open unsuspecting attachments, e.g. "I Love You" (2005) or "Melissa" (1999) viruses.
This threat usually operates in concert with the last two threats, i.e. spam and social engineering.

ix. Spam is unsolicited email messages, usually received from unknown senders who may blind copy" numerous addressees. Spams could be spoofed as coming from legitimate or known sources and may have enticing content luring users to take certain detrimental actions [250]. Spam tends to be a lot more than a nuisance. Whenever it lures a user into opening an infected attachment or clicking on a questionable link, one can end up with severe damage to the computer or risk towards personal information loss. Certainly, spammers who can capitalize on spam to steal ones information might gain access to bank accounts or credit cards information.

x. Social engineering is the practice of manipulating or luring end-users to divulge confidential information by appealing to their sense of social norms, with the aim to gain access to one's system [232]. This threat exploits the vulnerability of end-users, e.g. receptionists, to solicit access credentials. The social engineer exploits and leverages on pre-existing trusted relationship amongst a victim and the assumed entity, to lure the victim to take some detrimental actions [251]. Some examples of social engineering are information gathered via telephone calls purporting to be a system administrator, or a consultant or a visitor asking to use a corporate computer, etc.

7.1.4. Trends – Other Challenges

The motivation for this study has been to highlight on the cyber-security challenges that confront SMEs in developing economies. In this section, other vulnerabilities, as evaluated with fuzzy cognitive maps (FCMs) are discussed.

FCMs use directed graphs and fuzzy matrices to model interrelationships amongst concepts, such as policies and events. One advantage of the FCM is the simple and visual manner in representing causal relationships, thus aiding simple decision-making.

In this study, vulnerabilities with SMEs, and in particular their asset disposal policies, were modeled with FCM, using fuzzy linguistic terms. Nodes or vertices were used to represent the

policies, whilst directed links with arrows indicating the direction of impact represent the relational effects [201]. Typically, positive or negative signs are appended to indicate whether the causal effects are enablers (drivers) or inhibitors, respectively [202].

The trend in vulnerabilities associated with asset disposal policies is shown in figure 7-5 below.

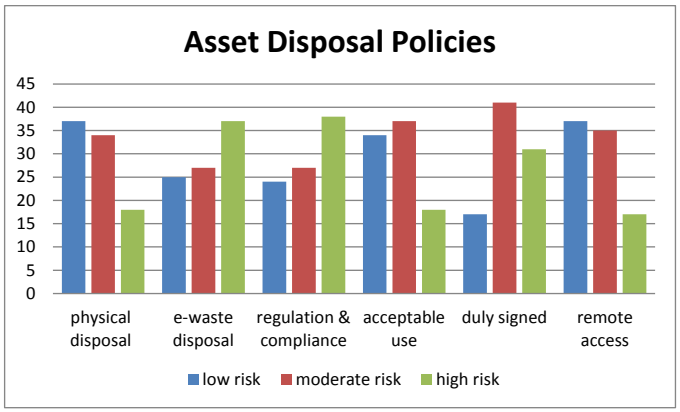


Figure 7- 5: Vulnerabilities with Assets Disposal Policies

It is observed that policies bothering on third party supervision or management, such as regulation & compliance and e-waste disposal exhibited similar characteristics, and indicated more SMEs being vulnerable. On the other hand, policies with SMEs having absolute control showed varied characteristics, probably expected of SMEs in developing economies.

Olander et al [252] studied SMEs intangible asset protection and focused on intellectual properties. They showed that SMEs are more vulnerable to assets exposure to others, with the exception of those within the bio-technology industry.

Ogalo [249] assessed the impact of cyber-security policies on Kenyan SMEs. He found out that over 90% of the SMEs either had gaps in their policies or the policies did not exist. Similarly, Curtis & Cobham [253] posited that most SMEs are vulnerable due in part to employees not adhering to acceptable use policy and un-enforceable policies.

MacLean et al [254] perceived cyber-security policy framework in developing economies as bedeviled with vulnerabilities.

The succeeding sections discuss the findings as they address the research questions of the study.

7.2. Interpretation with respect to the Research Questions

This section addresses the research questions using the findings made from this study. First, the key questions are tackled in succeeding sub-sections, and followed by the ancillary questions.

7.2.1. Mitigating the Impact of Cyber-security

The system of mitigating risks when vulnerabilities and threats are present against a given asset is non-linear. This makes it challenging in modeling, unlike linear problems which could be modeled with simple linear algorithms.

This non-linearity is modeled using the input-output dataset from the survey. The relationships between the constructs were first modeled by IF-THEN rules in the Mamdani system. However, due to the curse of dimensionality associated with fuzzy systems, there was the need to utilize the computational capabilities of neural networks.

The MATLAB toolbox of adaptive network-based fuzzy inference system (ANFIS) was used to construct the model from the dataset. Since the original model is a non-linear Mamdani system, a MATLAB script with the key function "mam2sug" was executed to transform the system unto a Sugeno type.

The transformed system was then loaded unto the ANFIS editor with training data, as well as checking data. The fuzzy rule-base designed with the Mamdani system was deemed unsuitable and so the ANFIS generated its own rule-base using grid partition algorithm. The model is subsequently trained and the surface views are shown in Figures 7-6 & 7-7.

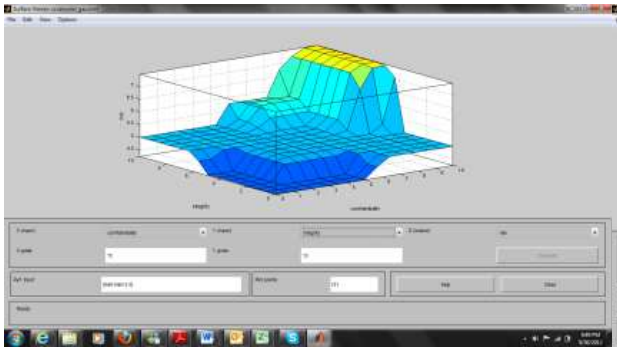


Figure 7- 6: Gaussian MFs Surface View (before Training)

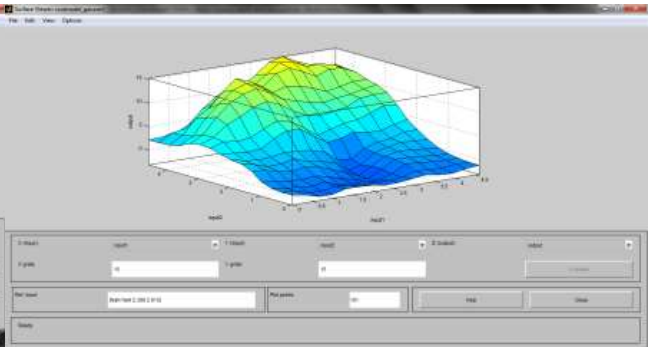


Figure 7- 7: Gaussian MFs Surface View (after Training)

Figures 7-6 & 7-7 depict the surface views, where the input space has, say vulnerabilities, which upon exploitation would violate the confidentiality property and threats, and the output space, risks. The figures show the non-linearity and illustrate how the model responds to varying values of the inputs, i.e. vulnerabilities and threats. The surface view shows the relationship between the vulnerabilities and threats on the antecedent side, and risks on the

consequent side, resulting from the rule-base generated from the datasets [220] [64]. The bumps represent fuzziness in the description of the variables linguistically [104]. The bumps are also due in part to the fuzziness (vagueness) in the membership functions of the variables.

In spite of that, it can be seen that the surface views mimic the system behavior of the CSVA model. First, figure 7-6 describes the exact system behavior expected of the CSVA model. That is, lower values of both vulnerabilities and threats yield low risk as expected. Similarly, as threat level increases (i.e. a move towards the left edge), and with a corresponding high vulnerabilities (i.e. a move towards the right edge), results in high risk (i.e. elevation view – edge of top view). However, after the training (figure 7-7) the system behavior is understandably degraded; especially when both threats and vulnerabilities are high. This may be due to factors, including "noise" in measurement, error in aggregation of the datasets, and again difficulties associated with optimizing a non-linear system behavior with a linear model.

Throughout this study, attempts are made at depicting this non-linear fuzzy relationship existing amongst vulnerabilities, threats, assets value and risks. That has been the basis of the fuzzy relational function (aforementioned as equation [1-4] in Chapter 1 of this Thesis).

$$Risk_{\text{threat}} \; f(\text{Threat}_{\text{asset}}, \text{Vulnerability}_{threat}, \text{Asset Value}) \qquad [7\text{-}22]$$

where:

- Asset Value is the summation of contributing values from the CIA utilities as evaluated in respect of the urgency for restoring a compromised asset and/or its criticality to the business;
- Vulnerability is a weakness within the system that can be exploited by threat agents; and
- Threat is the possibility of exploiting the weakness, given the conditions of motivation or intent, capability, opportunity and attractiveness of the asset.

The CSVA model resulting from the fuzzy relational equation [7-1] above, has the inputs modeled by a set of conjunctive rules, which eventually decompose into a single aggregated fuzzy output, risks. Practically, the system ought to have been modeled with the input space infused with some disjunctive rules. For instance, some of the vulnerabilities could relate in disjunctive settings, since there are instances when a particular vulnerability or the other may be present. The MATLAB ANFIS and/or fuzzy logic toolboxes are handicapped with such combinations; one has to use either conjunctive or disjunctive set of rules per scenario [64] [104] [205].

Now looking at the surface views in figures 7-6 & 7-7, it is observed that the surfaces cover the entire decision spaces. The surface of a particular fuzzy set relates to variables and associated

membership functions in the set [47]. The surface view is generated as a result of the mapping from the input space unto the output space in one-to-many "truth function grade" which is typical with convex fuzzy sets, such as triangular, trapezoidal, Gaussian [47]. Babuska [230] regards the surface view as a mapping from the antecedent space to a convex region in the parameters space of a quasi-linear system. In all scenarios of fuzzy inference system dataset generation, the linear consequent was chosen irrespective of the membership functions adopted.

The non-linearity of the CSVA model creates the non-uniformity on the surface as some of regions are well approximated, whilst others may require further tuning [230]. If the system had linear relationships, the least-squares algorithm would have been optimally ideal. So in order to optimize the non-linear parameters of the CSVA model, hybrid methods of gradient and least-squares algorithms in the ANFIS toolbox were applied. The least-squares algorithm is used to estimate consequent parameters during the forward pass in the learning process, whilst the back-propagation based gradient-descent algorithm is utilized during the backward pass to update the antecedent parameters [220] [64] [255].

7.2.2. Compromises of Confidentiality, Integrity & Availability (CIA)

This study has been discussing the compromises of confidentiality, integrity and availability (CIA) vulnerabilities confronting most SMEs in developing economies and the need to mitigate them with appropriate measures to curb the challenges. The taxonomies of vulnerabilities and threat agents dealt with issues of risks that could impact on SMEs business performance and continuity.

Revisiting threats, for example – natural disasters were deemed to be the most serious threats to the SMEs. This may be subjective in respect of SMEs in developing economies, since SMEs in developed economies are not likely to face this type of threat. Some of the reasons are not farfetched. For instance, the fire and emergency services work and they respond promptly to situations in the developed world. The situation is certainly different with developing economies.

Similarly, the threat of power failure is another interesting and probably peculiar challenge. Because of the unreliable commercial power supply in developing economies, power failure could greatly hamper on SMEs. The usual trend is that the power supply is so erratic and fluctuates very often (e.g. in Nigeria for example, the electric utility distributor is the National Electric Power Authority (NEPA), which has earned the nickname "never expect power always"). The situation is not different in Ghana, where Electricity Company of Ghana (ECG) is the distributor (also nicknamed "Except Candles & Generators" one would not have power).

Overall, the threats associated with malwares including spams, spyware and so on, are high risks to SMEs. In a report released in 2010, the Business Software Alliance (BSA) [256] indicated that over 80% of software in West, East and Central Africa were pirated. Here pirated software is defined as any software program installed or duplicated without proper license.

According to BSA [256], there is significant evidence to link software piracy with the frequency of malware attacks. They posited that further evidence suggests that "markets with high software piracy rates also have the tendency to experience high rates of malware infections". Again the reason is that users of pirated or unlicensed software typically are unable to access patches or critical updates released by the vendors in order to ensure and remain secured.

In today's ubiquitous computing environments, a myriad of cyber-security challenges face SME stakeholders. Some of the notable challenges are:

- Powerful computers – used as storage or repository of valuable data or information, without adequate understanding of the workings or operations of computers, e.g. Windows registry, ports, passwords, file storage, etc. For instance, new operating systems come with innovative registry, which may be different from the previous version. The registry is a hierarchical database which has the configuration settings for the operating system and applications. The registry also has the user's authentication credentials. As an enormous source of information about the system, what has been installed, when the system was last running, who the users are, what network cards are present, etc., the registry is definitely a useful and attractive source of information.
- Status-quo end-users – in spite of sophistication of the Internet services and technologies, end-users remain unsophisticated; thus, the average end-user is still the weakest link in the cyber-security chain and many indiscriminately install pirated software and visit questionable websites – even though, it violates corporate acceptable Internet use policy. Mallery [257] advocates for addressing the threats associated with untrained and unwary end-users.
- Security as an after-thought to computer development - advancement in computer technologies focused on interconnection, information processing and dissemination, rather than protection.
- Current trend is to share, not to protect - social networking, web-based applications make it easier to share information (and even for data analysis), thus bypassing security checks, resulting in a number of data compromises and breaches.

- Data accessible from anywhere - data compromises resulting in remote access from devices – intellectual property compromises, e.g. Google's free data storage via FTP Gmail accounts. Mallery [257] posited that security posture is a measure of how good its configurations and maintenance programs are.
- Sophisticated hacker profile – even though the end-users are unsophisticated, the hacker profile is constantly evolving; they are more of organized cyber-crime entities.
- Management perceives security investment as a drain on the organization – unless and until the business is impacted.

The following section discusses the supplementary questions raised.

7.2.3. Supplementary Questions

In addressing the subsidiary questions, the study took an in-depth look at the vulnerabilities associated with ICT assets disposal policies, as case examples. Indeed, it has been established that there exist data confidentiality exposures occurring as a result of ICT security policies. The implications are that vulnerabilities in one policy do have adverse impact on others [215].

The survey revealed that overall 81% of SMEs were unaware of policies (if existed) and as well, stakeholders had not signed off the policies. Also, it was found that, 58% of SMEs do not have shredders, nor any physical asset disposal policies; 72% of SMEs do not have any e-waste policy, neither is due care taken in discarding end-of-useful-life assets.

Interestingly, 73% SMEs used third party asset disposal contractors without any due diligence or special recourse to the third party's procedures [215].

Yeboah-Boateng [215] showed that correlations existed amongst the various cyber-security policies using the FCM approach. He ascertained that in the event of a different expert opinion, used as the causal connection matrix, the results still show some correlations amongst most of the policy constructs.

The policies put in place are only effective if all stakeholders are duly informed of the tenets of those policies, which will in turn enhance enforcement, hence assuring the confidentiality security property. Through this study, it has been amply established that SMEs ought to put in place appropriate asset disposal policies.

The succeeding section will discuss the contributions made by the study.

7.3. Contributions

This section is a very important segment of this study that spells out the contributions made herein. Typical Ph.D. contribution(s) could take the form of either discovery of knowledge, or formulation of a theory, or an innovative re-interpretation of known data and established ideas. This study contributes to the cyber-security or information assurance and techno-economics bodies of knowledge through empirically based characterization of the risk assessment and information assurance literature. The study re-contextualized the risk formula as a cyber-security vulnerability assessment model. It also provides a set of taxonomies of vulnerabilities and threat agents confronting SMEs in developing economies.

7.3.1. The CSVA Model Revisited

In this section, the importance of the CSVA model is re-emphasized. The thematic problem being addressed in this study has been "how could SMEs, in developing economies, mitigate the impact of cyber-security vulnerabilities against their assets?"

The use of ICT resources and the Internet, in general, for business communications and operations, has undoubtedly come to stay. Consequent to these innovations, are the myriad of cyber-security challenges that threaten the SMEs and their survivability. If nothing is done, these weaknesses shall be exploited by threat agents (c.f. sections 7.1.2. & 7.1.3. on vulnerabilities and threats). This may adversely impact SMEs by way of loss of revenues, loss of customer and investor confidence, loss of resources, loss of credibility, cost related to dealing with the security breaches, cost of mitigation as well as possible business closure, etc.

This study, cognizance of the SMEs in developing economies and their budget needs, proposed the cyber-security vulnerabilities assessment (CSVA) model which takes into account all intrinsic elements and perceived uncertainties associated with risk metrics. The CSVA model is simple to use, intuitive and requires not a huge budget to apply, as amply illustrated by the example in section 6.3.4. – Model Significance & Applications.

Associated with and paramount to the development of the CSVA model is the fuzzy risk relational function which has the vulnerabilities, threats and assets value as fuzzy arguments. The traditional risk equation in probability has been completely re-contextualized in fuzzy set theoretic, as well as adding the impact due to assets value to the equation. The notion is that information is invaluable.

Finally, the simple fuzzy cognitive maps (FCMs) approach to evaluate cyber-security vulnerabilities with SMEs is also a tool that requires neither special skillset nor programing.

Just basic algebraic matrices and understanding of the inherent attributes of security posture would assist SMEs to identify and mitigate some challenges.

The succeeding section restates the provision of taxonomies in contribution to this study.

7.3.2. Provision of Taxonomies

The taxonomies defined a set of vulnerabilities and threat agents organized in the order of most susceptible to least ICT assets, for the vulnerabilities, and from the most likely or critical to the less likely or minor for the threat agents. The taxonomies provide a benchmark of cyber-security challenges by which SMEs can mitigate risks in their systems and networks.

This benchmark offers a common platform about SMEs assets importance or criticality labels that ought to be appropriately safeguarded. It must be noted that accurately identifying critical assets can lead to proactive prevention and detection measures that eventually mitigate the risks.

Similarly, the threat agents taxonomy provides panoramic view of the extent and severity of threat agents militating against SMEs assets and resources. It can also assist in the appropriate determination and formulation of mitigation strategies and policies for the SMEs.

The findings of this study are adduced from a sample population of SMEs in developing economies. This may place some limitations on the generalizability of the study.

7.3.3. The Scope of Generalization

At the onset of this study, the scope was defined for a population of SMEs in developing economies which characteristically use the Internet for communications and business operations. The study further defined the sample set based on the number of employees engaged by the SMEs.

The study ensured that the pre-defined sample population was adhered to and that credible measurement techniques were put in place to ensure validity and reliability. Intrinsic cyber-security metrics measured the security postures of SMEs and inferences were drawn.

Though, the inferences or deductions are empirically based, they are limited due in part to the SMEs definition, the web portal facilities used for data collection, the sampling techniques employed, and the analytical tools employed, such as the MATLAB based ANFIS toolbox.

The above notwithstanding, the analysis, findings and deductions were statistically confident with respect to the sample SME population.

Chapter 8 Conclusions

This is the concluding chapter of the study on cyber-security challenges with SMEs in developing economies: issues of confidentiality, integrity and availability (CIA). This chapter entails some concluding remarks that are given in the ensuing sections.

Finally, recommendations and some suggested areas for future studies are made.

8.1. Concluding Remarks

Globally, SMEs have been defined in a number of different ways. Some definitions involve revenues, capital and staff strength. Interestingly, SMEs in developing countries are characterized by uncertain revenues. Coupled with that, most developing economies have fluctuating currencies. These challenges create uncertainties with any definitions involving monetary value; that is, the set of target SMEs population would vary with exchange rates.

Cognizant of the above, the only common denominator is the number of employees. So this study defined SMEs based solely on staff strength, which is also consistent with the norms applied in the case study countries. At least, this approach enhances the generalization of findings to some reasonable extent.

Having so defined the SMEs in developing economies, the study focused on those who have embraced the information and communications technology (ICT) and the surge in doing business in the cyber-space. They use the Internet to communicate with business stakeholders, they order and receive requests for supplies via web portals, they store critical corporate information on computers and storage media, etc. In essence, SMEs in developing economies also stay competitive via the web presence and utilize the Internet resources in their business operations.

New and innovative security challenges confront the SMEs on a daily basis, thus exploiting most “zero-day” vulnerabilities. SMEs are faced with lots of uncertainties. This results in various losses to the SMEs, even with the possibility of business closure. SMEs ought to ensure that their networks and systems are both available and protected.

SMEs ought to safeguard their mission critical assets through the effective use of policies, education, training and awareness of their end-users, as well as deployment of appropriate technology solutions. Periodic re-classification of assets is imperative; since the asset value changes over time, especially as business needs or focus change. The asset value may increase or more commonly, decrease.

In business, confidentiality exists to protect the privacy of a business entity, including its critical or sensitive business information, and to safeguard intentional or unintentional

disclosure. For effective operations, SMEs must facilitate the right access to the right users or entities at the right time. Furthermore, unauthorized entities must be prevented from gaining access to any facility and/or resource.

A key objective of this study has been to identify some of these challenges and to offer proactive mitigation measures to deal with them. The basic premise has been the fact that cyber-security is an intangible concept and has key attributes in confidentiality, integrity and availability (CIA).

Admittedly, there are other dimensions or attributes of cyber-security besides the CIA triad, but literature support the CIA as the bedrock in any holistic security initiative.

From that standpoint, cyber-risk has been seen and treated as the possibility of loss of confidentiality, integrity and availability due to a specific threat on a given asset. This study focused on the perceived uncertainties in cyber-security vulnerabilities and threats, and used fuzzy linguistic variables that represent the real life business environment decision-making to model assessment techniques.

In view of the above, the study pursued a more holistic risk assessment model in departure from the traditional notion which has been based on simplistic probabilistic computations and usually treated with overly binary outlook. This study has been greatly inspired and influenced by the works of Professors Zadeh, Katsikas and Shaurette.

For instance, Zadeh's possibility theory holds the view that first, much of the information needed for human decision-making or reasoning are in essence possibilistic rather than probabilistic, and that the intrinsic fuzziness in natural languages is a logical expression of information from possibilistic perceptive.

Also, in modeling risk management, one needs to take into consideration the complexities and uncertainty measures in order to have a holistic and viable solution. Any attempt at using just simplistic probabilistic assessment renders the technique a mere guesstimate rather than a formal prediction with statistical basis.

Though the probabilistic risk evaluation is grounded on sound mathematical theory of probability, its ratings are fraught with subjective guesstimates. This implies that qualitative risk values may be best estimated based on rules, such as fuzzy inference rules, that capture the consolidated advice of cyber-security experts.

In this study, both quantitative and qualitative analyses have been utilized. This was necessitated by the fact that cyber-security metrics and associated data analysis is essentially, techno-economic; i.e. it is intrinsically a social process as much as a technical one.

The study dealt with multivariate data which represented the perceived opinions of experts that were sampled. The key constructs were mainly manipulated using triangular fuzzy

numbers (TFNs) to represent natural language and information processing in multi-attribute decision-making (MADM) problems, since they are intuitive, easy to use and computationally simple.

In addressing the issue of how SMEs in developing economies mitigate the impact of cyber-security challenges, this study first identified a number of risks due to compromises or violations of CIA properties. Key compromises inherent in mission-critical assets such as DNS server, mail server, web server, database server, routers and core switches are said to be paramount as far as SMEs are concerned.

Based upon these cyber-assets, the study designed and proposed an empirically based cyber-security vulnerabilities assessment (CSVA) model on the basis of a fuzzy relational function of cyber-risk. The CSVA model is a means by which SMEs can be assisted in finding mitigation measures proactively for any identified cyber-security susceptibilities.

Also identified in this study are the ten (10) top-most threats that commonly exploit SMEs in developing economies. These threats are natural disasters that are perennial in developing economies, poor authentication methods, power outages and failure, viruses, hacking, no backups, un-scanned attachments, spamming, spywares, and social engineering due to apparent gullibility of most cultures in developing economies.

Again, fuzzy similarity measures were applied with multi-attribute decision-making techniques to benchmark taxonomies of vulnerabilities and threat agents. These simple approaches employed in identifying and creating the taxonomies are geared towards assisting SMEs to have some base metrics for referencing in risk management and information assurance.

Accurate identification of critical assets can assist SMEs in their strategy and cyber-security plan, such that appropriate protection is deployed around critical assets.

Finally, a simple but intuitive fuzzy cognitive map approach was used to evaluate the existence and possible implications of cyber-security vulnerabilities amongst SMEs. The study established the following:

- that vulnerabilities, due to cyber-security policies or the lack thereof, can have serious adverse implications on other policies;
- that SMEs are generally unaware of cyber-security policies (81% SMEs according to the empirical study), as well as the policies are not duly signed for adherence or enforcement;
- that almost three-quarters (73%) of SMEs used third-party or external contractors for asset disposal, without any due diligence or special recourse to underlying (or even knowing) the contractor's procedures for data disposal and/or destruction.

In conclusion, the novel approach of evaluating cyber-risk based on intuitive, subjective and holistic assessment of each of the key constructs of cyber-security can be applied by SMEs due to its simplicity and low cost. The taxonomies could also fill the gap created by the lack of standardized lists of vulnerabilities and threats in developing economies for SMEs. At least, SMEs can have some empirical basis of cyber-security challenges to benchmark their business and security performance metrics, rather than relying upon the usual "TV news effect" of most-publicized compromises with disproportionate mitigation measures.

In essence, all these techniques have been modeled with the SMEs in developing economies in mind. For example, the CSVA model does not require any specialized software or tools; just basic analytical reasoning with technical knowledge in cyber-security and network operations could suffice. Similarly, the application of fuzzy cognitive map approach to assess vulnerable policies requires only algebraic matrices and the requisite technical knowledge in cyber-security.

The following section recommends some measures needed to be taken into consideration by SMEs and propose areas of future research needs.

8.2. Recommendations & Future Works

The introductory quote of this thesis "more small businesses today use networks and the Internet as vital business tools than ever before …." and the concluding quote "yet, many small businesses have not taken the steps to safeguard their businesses …." sum up the significance of this study on cyber-security challenges with SMEs in developing economies.

Needless to say, SMEs need to take necessary steps to safeguard their critical information assets and to build secure organizations. SMEs ought to first assess their vulnerabilities, and to evaluate the risks and threats posed to them as a step towards building a secure organization.

Generally, mission-critical assets are identified, and appropriate security resources are apportioned based on the asset value to the business. For a very effective and secure business, the threats and vulnerabilities pair assessment, must encompass threats based on the business itself, and that based on its industry, as well as global threats. This is in view of the boundless or borderless nature of the Internet.

Other factors that SMEs ought to consider include the following:

- Common myths of security, such as security by obscurity, the business not having anything worthy of interest to the hackers, or immunity from attacks, etc.

- Security awareness, training and education – ICT security functionaries ought to be abreast with the trend of vulnerabilities, re-training of end-users and to build or inculcate a culture of security amongst employees, etc.
- Identification and utilization of built-in security features in the operating systems and applications. This includes ensuring that corporate security policies are strictly adhered to. For instance, policy guides such as USB flash disk must be brought from outside the organization, or use of strong passwords and periodic changing of passwords, or reconfiguring systems to ensure that unutilized default ports are closed or disabled, etc.
- Last but not the least, constant monitoring of system behavior, periodic reviewing of system logs, patching and updates in a timely fashion, and use of administrator's accounts for administrative tasks only.

Whilst literature on cyber-security tools, techniques and technologies are available, there's still gap in information assurance or information security management to SMEs, especially for those in developing and emerging economies. This study has emphasized on decision-making process in a proactive manner. An attempt has been made to identify some plausibly challenges and also some guidance in addressing them. The global economy has forced SMEs to compete in cyber-space, with increased reliance on their IT infrastructure and the expertise needed to handle them. This situation makes it imperative for SMEs to make decision with an appropriate balance amongst uncertainties of risks and opportunities. Strategies aimed at deploying solutions will be well placed taking into account the awareness of ever-evolving lists of vulnerabilities and threats. Also, the mitigation measures undertaken to minimize risk must involve all stakeholders, especially the custodians of corporate assets.

It would be interesting to review the cyber-risk function to ascertain the true mathematical nature of it. For instance, the CSVA model could be reviewed using fuzzy polynomials. Further research areas include exploration with fuzzy logic and other soft computing techniques, such as genetic algorithm and/or evolutionary computing.

In any case, the CSVA could be further enhanced with graphical user interface (GUI) based environment where SMEs could just evaluate their assets with a few inputs.

References

[1] PriceWaterhouseCoopers, "Information security Breaches Survey, 2006," PWC & DTI, 2007.

[2] Wiles, Jack & Russ Rogers, Techno Security's Guide to Managing Risks - For IT Managers, Auditors & Investigators, Elsevier, Inc., 2007.

[3] D. Gibson, Managing Risk in Information Systems, Jones & Bartlett Learning, 2011.

[4] Dept. of Homeland Security, *Security Guidelines for the Petroleum Industry,* American Petroleum Institute (API) Publications., 2006.

[5] L. Zadeh, "Fuzzy Sets as a Basis for a Theory of Possibility," *Fuzzy Sets & Systems,* vol. 1, pp. 3-28, 1978.

[6] L. Zadeh, "Fuzzy Sets," *Information & Control,* vol. 8, pp. 338-353, 1965.

[7] S. K. Katsikas, "Risk Management," in *Computer & Information Security Handbook*, Morgan-Kaufmann, Inc., 2009, pp. 605-625.

[8] K. M. Shaurette, "The Building Blocks of Information Security," in *Information Security Management Handbook*, 2002.

[9] M. Dondo, *A Fuzzy Risk Calculations Approach for a Network Vulnerability Ranking System,* 2007.

[10] ITU-T, "International Telecommunications Union (ITU) - Telecoms Standards Recommendation X.805," ITU, Geneva, 2005.

[11] P. Zimmerman, The Official PGP User's Guide, MIT Press, 1995.

[12] Dhillon, G. & J. Backhouse, "Information System Security Management in the New Millenium," *Communications of the ACM,* vol. 43, no. 7, 2000.

[13] D. Parker, "Toward a New Framework for Information Security," in *The Computer Security Handbook*, 4th ed., New York, John Wiley & sons, 2002.

[14] D. Denning, "Cyber-Security as an Emergent Infrastructure," in *Bombs & Bandwidth: The Emerging Relationship between IT & Security*, The New Press, 2003.

[15] I. Perfilieva, "Fuzzy Function: Theoretical and Practical Point of View," in *EUSFLAT*, Aix-les-Bains, France, 2011.

[16] L. Zadeh, "The Concept of a Liinguistic Variable and Its Application to Approximate Reasoning," *Information Sciences,* vol. 8, pp. 199-257, 1975.

[17] Moller, Bernd & Uwe Reuter, Uncertainty Forecasting in Engineering, Berlin: Springer, 2007.

[18] B. M. Ayyub, Elicitation of Expert Opinions for Uncertainty & Risks, CRC Press LLC, 2001.

[19] S. Bavisi, "Penetration Testing," in *Computer & Information Security Handbook*, Morgan-Kaufmann, Inc., 2009, pp. 369-382.

[20] J. Walker, "Internet Security," in *Computer & Information Security Handbook*, Morgan-Kaufmann, Inc., 2009, pp. 93-117.

[21] Whitman & Mattord, Principles of Information Security, vol. 2nd Edition, Thomson Course Technology, 2005.

[22] M. Ciampa, Security Awareness: Applying Practical Security in Your World, Thomson Learning Inc., 2004.

[23] J. L. Darby, "Estimating Terrorist Risk with Possibility Theory," Los Alamos National Laboratory, USA, 2004.

[24] N. Ye, Secure Computer & Network Systems: Modeling, Analysis & Design, John Wiley & Sons, 2008.

[25] Cashell, Brian, William D. Jackson, Mark Jickling & Baird Webel, "The Economic Impact of Cyber-Attacks," US Congressional Reserach Service, 2004.

[26] PITAC, "Cyber-Security: A Crisis of Prioritization," National Coordination Office for Information Technology Research & Development, 2005.

[27] B. Mansoor, "Intranet Security," in *Computer & Information Security Handbook*, Morgan-Kaufmann, Inc., 2009, pp. 133-148.

[28] D. Storey, Understanding the Small Business Sector, London: Routledge, 1994.

[29] Kapurubandara, Mahesha & Robyn Lawson, "Barriers to adopting ICT & e-Commerce with SMEs in Developing Countries: An Exploratory Study on Sri Lanka," in *CollECTeR '06*, Adelaide, Australia, 2006.

[30] L. Daniels, "Changes in the Small-scale Enterprise sector from 1991 to 1993," GEMINI Technical Report, N.71 Bethesda, MD, 1994.

[31] Gallagher, C. & G. Robson, "The Job Creation Effects of Small & Large Firms Interaction," *International Small Business Journal,* vol. 12, pp. 23-37, 1995.

[32] E. Aryeetey, "Priority Research Issues Relating to Regulation & Competition in Ghana," *Center on Regulation & Competition Working Paper Series,* 2001.

[33] Kayanula, D. & P. Quartey, "The Policy Environment for Promoting Small & Medium-sized Enterprises in Ghana & Malawi," *Finance & Development Research Program, Working Paper Series,* vol. 15, 2000.

[34] Abor, J. & P. Quartey, "Development in Ghana & South Africa," *International Research Journal of Finance & Economics,* vol. 39, 2010.

[35] D. Ariyo, "Small Firms are the Backbone of the Nigerian Economy," Africa Economic Analysis, 2005.

[36] W. Ozier, "Risk Assessment," in *Information Security Management Handbook*, CRC Press, 2002.

[37] ISO-27005, "Risk Management Standard," [Online]. Available: www.27005.org/iso-27005.htm.

[38] "Information Security Risks," 1995. [Online]. Available: www.docstoc.com. [Accessed 19 March 2010].

[39] D. S. Hermann, A Practical Guide to Security Engineering & Information Assurance, Auerbach Publications, CRC Press, 2003.

[40] Vidalis, S. & A. Jones, "Analyzing Threat Agents & Their Attributes," School of Computing, University of Glamorgan, Pontypridd, Wales, 2005.

[41] C. Pfleeger, Security in Computing, New Jersey: Prentice Hall, 1997.

[42] Pedrycz, Witold & Fernando Gomide, Fuzzy Systems Engineering: Towards Human Centric Computng, John Wiley & Sons, 2007.

[43] C. McEachem, "Technology Risks: Don't Panic - Financial Services Firms Seem to Have Cyber-Risk Under Control," *Wall Street Technology,* vol. 38, 2001.

[44] Ngai, E.W.T. & F.K.T. Wat, "Fuzzy Decision Support System for Risk Analysis in e-Commerce Development," *Decision Support Systems,* vol. 40, pp. 235-255, 2005.

[45] Z. Yazar, *A Qualitative Risk Analysis & Management Tool - CRAMM,* SANS Institute, 2002.

[46] Yang, M.S. & M.C. Liu, "On Possibility Analysis of Fuzzy Data," *Fuzzy Sets & Systems,* vol. 94, pp. 174-183, 1998.

[47] E. Cox, The Fuzzy Systems Handbook: A Practioner's Guide to Building, Using & Maintaining Fuzzy Systems, Academic Press, Inc., 1994.

[48] H. Zimmerman, Fuzzy Sets, Decision Making & Expert Systems, Boston, MA: Kluwer Academic, 1987.

[49] Kirschfink, H & K. Lieven, *Basic Tools for Fuzzy Modeling, Tutorial on "Intelligent Traffic Management Models",* Aachen University, 1999.

[50] Kramosil, Ivan & Jiri Michalek, "Fuzzy Metrics & Statistical Metric Spaces," *Kybernetika,* vol. 11, no. 5, pp. 336-344, 1975.

[51] Sarker, R.A. & C.S. Newton, Optimal Modeling: A Practical Approach, Taylor & Francis Group, 2007.

[52] Wilcox, R. & B.M. Ayyub, "Uncertainty Modeling of Data & Uncertainty Propagation for Risk Studies," in *4th International Symposium on Uncertainty Modeling & Analysis*, 2003.

[53] B.-Y. Cao, Optimal Models& Methods with Fuzzy Quantities, Springer-Verlag, 2010, pp. 95-115.

[54] D. Bell, "Concerning "Modeling" of Computer Security," *Trusted Information Systems,* 1988.

[55] Nguyen, H. et al, A First Course in Fuzzy & Neural Control, Chapman & Hill, 2003.

[56] Moon, J.H. & C.S. Kang, "Use of Fuzzy Set Theory in the Aggregation of Expert Judgments," *Annals of*

Nuclear Energy, vol. 26, pp. 461-469, 1999.

[57] Costa Branco, P.J., N. Lori & J.A. Dente, "New Approaches on AStructure identification of Fuzzy Models: Case Study in an Electro-Mechanical System," in *Fuzzy Logic, Neural Networks & Evolutionary Computation*, Berlin, Springer-Verlag, 1996, pp. 104-143.

[58] V. Kecman, Learning & Soft Computing: Support Vector Machines, Neural Networks & Fuzzy Logic Models, Cambridge: The MIT Press, 2001.

[59] Mamdani, E.H. & Assilian, S., "An Experiment in Linguistic Syntheisi with a Fuzzy Logic Controller," *International Journal of Man-Machine Studies,* vol. 7, no. 1, pp. 1-13, 1975.

[60] J. Mendel, Uncertain Rule-based Fuzzy Inference Systems: Introduction & New Directions, Prentice Hall, 2001.

[61] Takagi, T. & Sugeno, M., "Fuzzy Identification of Systems & its Applications to Modeling & Control," *IEEE Trans. on Systems, Man & Cybernetics,* vol. 15, pp. 116-132, 1985.

[62] Meyers, Carol, Alan Lamont & Alan Sickerman, "Use of Multi-attribute Utility Functions in Evaluating Security Systems," Lawrence Livermore National Security Laboratory, USA, 2008.

[63] H. L. Larsen, "Importance Weighting and ANDness Control in De Morgan Dual Power Means and OWA Operators," *Fuzzy Sets and Systems,* vol. 196, pp. 17-32, 2012.

[64] J. Jantzen, Foundations of Fuzzy Control, John Wiley & Sons, 2007.

[65] Onwubiko, C. & A. Lenaghan, "Spatio-Temporal Relationships in the Analysis of Threats for Security Monitoring Systems," in *Proceedings of the 2nd International Conference on Computer Science & Informations Systems*, Athens, 2006.

[66] Seacord, Robert & Allen. D. Householder, "A Structured Approach to Classifying Security Vulnerabilities," Carneige Mellon University, Pittsburgh, PA, 2005.

[67] J. Bolton, "Report of the Committee of Inquiry on Small Firms," HMSO, London, 1971.

[68] P. Julien, The State of the Art in Small Business & Enterprenuership, Ashgate, Aldershot, 1998.

[69] Canadian Business for Social Responsibility, "Engaging Small Business in Corporate Social Responsibility," 2003.

[70] Naffziger, D.W., N.U. Ahmed & R. Montagno, "Perceptions of Environmental Conciousness in US Small Business: An Empirical Study," *SAM Advanced Management Journal,* 2003.

[71] Besser, T. & N. Miller, "Small Business Community Values & Their Relationship to Management Strategies," *The Journal of Socio-Economics,* vol. 30, no. 6, pp. 221-241, 2001.

[72] Better Business Bureau Wise Giving Alliance, "Small Business Giving Survey," 2001. [Online]. Available: www.give.org/news/SBSurvey.pdf. [Accessed January 2012].

[73] BIS, UK, "Business Population Estimates for the UK and Regions," 2011. [Online]. Available: www.bis.gov.uk/assets/biscore/statistics/docs/. [Accessed January 2012].

[74] Baldwin, J. et al, "The Trend to Smaller producers in Manufacturing in Canada & US," Statistics Canada Working Paper, 2001.

[75] International Finance Corporation (IFC), "The World Bank Group SME Investments - Fiscal 2004," The World Bank, 2005.

[76] A. Deaton, "Savings in Developing Countries: Theory & Review," in *Proceedings of the World Bank Annual Conference on Developing Countries, 1989.*, 1990.

[77] Hooks & Duncombe, Handbook for Enterprenuers in Developing Countries, University of Manchester, UK , 2001.

[78] Parker & Castleman, "New Directions for Research on SMEs," vol. 1, no. 1-2, pp. 21-40, 2007.

[79] Walsham, Geoff & Sundeep Sahay, "Research on Information Systems in Developing Countries: Current Landscape & Future Prospects," *Information Technology for Development,* 2005.

[80] Ellefsen, I.D. & S.H. von Solms, *Framework for Cyber Security Structure in Developing Countries,* University of Johannesburg, 2012.

[81] International Telecommunications Union (ITU), "International Multilateral Partnership Against Cyber Threats (IMPACT)," ITU, 2011.

[82] International Telecommunications Union (ITU), "Guide to Cyber-security for Developing Countries," ITU, 2007.

[83] L. Pierre, "The Wall Street Networks," 2008.

[84] Sharma, Kunal, Amarjeet Singh & Ved Prakash, "SMEs & Cyber-security Threats in e-Commerce," vol. 39, no. 5-6, pp. 1-49, 2009.

[85] Abouzakhar, N. et al, "An Intelligent approach to Prevent Distributed Systems Attack," vol. 10, no. 5, pp. 203-209, 2002.

[86] B. Planque, "La PME Innovatrice: Quel est le role du milieu local?," *Revue Internationale PME,* vol. 1, no. 2, pp. 177-191, 1988.

[87] Ashrafi, R. & M. Murtaza, "Use and Impact of ICT on SMEs in Oman," *The Electronic Journal Information Systems Evaluation,* vol. 11, no. 3, pp. 125-138, 2008.

[88] Harindranath, G., R. Dyerson & D. Barnes, "ICT Adoption & Use in UK SMEs: A Failure of Initiatives?," *The Electronic Journal Information Systems Evaluation,* vol. 11, no. 2, pp. 91-96, 2008.

[89] M. Dondo, "A Fuzzy Risk Calculations Approach for a Network Vulnerability," 2007.

[90] A. Jaquith, Security Mterics: Replacing Fear, Uncertainty & Doubt, Addison-Wesley, 2007.

[91] J. J. A. Bubenko, "From Information Algebra to Enterprise Modeling & Ontologies - A Historical Perspective on Modeling for Information Systems," in *Conceptual Modeling in Information Systems Engineering*, Springer, 2007, pp. 1-18.

[92] J. Miller, "Risk Management for Your Website," *International Risk Management Institute Expert Commentary,* 2000.

[93] D. Tan, Quantitative Risk Analysis: Step-by-Step, SANS Institute, 2003.

[94] D. Bernoulli, "Exposition of a New Theory on the Measurement of Risk," *Econometrica,* vol. 22, no. 1, pp. 23-36, 1954.

[95] C. Culp, The Risk Management Process, John Wiley & Sons, 2001.

[96] Lange, T. et al, "SMEs & Barriers to Skills Development: A Scottish Perspective," vol. 24, no. 1, pp. 5-11, 2000.

[97] Bass, T. & R. Robichaux, "Defense-in-Depth Revisited: Qualitative Risk Analysis Methodology for Computer Network-centric Operations," in *IEEE Military Communications Conference*, 2001.

[98] Srinivasan, G. & M. Abi-raad, "Risk Factors with e-Business on SMEs," in *1st Australian Information Security Management Conference*, Perth, Australia, 2003.

[99] D. Wawrzyniak, "Information Security Risk Assessment Model for Risk Management," *TrustBus,* pp. 21-30, 2006.

[100] Stajano, F. & Ross Anderson, "The Resurrecting Duckling: Security Issues for Ubiquitous Computing," vol. 35, no. 4, pp. 22-26, 2002.

[101] F. Knight, Risk, Uncertainty & Profit, New York: Houghton Mifflin, 1921.

[102] S. Bradley, "Scientific Uncertainty: A User's Guide," *Working Paper,* p. London School of Economics, 2011.

[103] G. A. Holton, Value-at-Risk: Theory & Practice, Academic Press, 2004.

[104] Sivanandam, S.N., S. Sumathi, S.N. Deepa, Introduction to Fuzzy Logic Using MATLAB, Springer-Verlag Berlin, 2007.

[105] Friedlob, G.T. & L.F. Schleffer, "Fuzzy Logic: Application for Audit Risk & Uncertainty," *Managerial Audit Journal,* vol. 14, no. 3, pp. 127-135, 1999.

[106] Ayyub, B.M. & G.J. Klir, Uncertainty Modeling & Analysis in Engineering & the Sciences, Taylor & Francis Group, 2006.

[107] Tversky, A. & D. Kahneman, "Advances in Prospect Theory: Cumulative Representation of Uncertainty," *Journal of Risk & Uncertainty,* vol. 5, no. 4, pp. 297-323, 1992.

[108] F. J. Milliken, "Three Types of Perceived Uncertainty about the Environment: State, Effect & Response

Uncertainty," *The Academy of Management Review,* vol. 12, no. 1, pp. 133-143, 1987.

[109] R. Duncan, "Characteristics of Organizational Environments & Perceived Environmental Uncertainty," *Administrative Science Quarterly,* vol. 17, pp. 313-327, 1972.

[110] Lawrence, P.R. & J.W. Lorsch, Organization & Environment, Boston: Harvard University, Graduate School of Business Administration, 1967.

[111] R. N. Taylor, Behavioral Decision Making, Glenview, IL: Scott, Foresman, 1984.

[112] Kaplan, Stanley & John Garrick, "On the Quantitative Definition of Risk," *Risk Analysis,* vol. 1, no. 1, pp. 11-37, 1981.

[113] Walker, W.E. et al, "Defining Uncertainty: a conecptual basis for uncertainty management in model-based decision support," *Integrated Assessment,* vol. 4, no. 1, pp. 5-17, 2003.

[114] McFadzean, E., Jea-Noel Ezingeard & David Birchall, "Perception of Risk & the Strategic Impact of existing IT on Information Security Strategy at the Board level," vol. 31, no. 5, pp. 622-660, 2007.

[115] Barnett, T. et al, "The moderating effect of individual's perceptions of ethical work climate on ethical judgments & behavoral intentions," vol. 27, no. 4, pp. 317-362, 2000.

[116] B. Frey, "The Impact of Moral Intensity on Decision Making in a business context," vol. 26, no. 3, pp. 181-195, 2000.

[117] Ayyub, B.M. & R. McCuen, Numerical Methods for Engineers, Upper Saddle River, NJ: Prentice Hall, 1996.

[118] G. Klir, Architecture of Systems Problem Solving, New York: Plenum Press, 1985.

[119] Klir, G.J. & T.A. Folger, Fuzzy Sets, Uncertainty & Information, Prentice Hall, New Jersey, 1988.

[120] H. J. Zimmerman, Fuzzy Set Theory & its Applications, Boston: Kluwer-Nijhoff Publishing, 1985.

[121] Douligeris, C. & P. Katzanikoloau, "Network Security," *Telecommunications Systems & Techmologies,* vol. II, 2007.

[122] The UK Cabinet Office, "The Cost of Cyber Crime," The Office of Cyber Security & Information Assurance in the Cabinet Office, UK, 2012.

[123] K.-L. Lai, "Generalized Uncertainty in Structural Reliability Assessment," University of Maryland, College Park, MD, 1992.

[124] Ayyub, B.M. & K-L. Lai, "Structural Reliability Assessement with Ambiguity & Vagueme=ness in Failure," *Nav. Engineering Journal,* vol. 104, no. 3, pp. 21-35, 1992.

[125] Lai & B.M. Ayyub, "Generalized Uncertainty in Structural Reliability Assessment," *Civil Engineering System,* vol. 11, pp. 81-110, 1994.

[126] Z. Xu, "An Approach Based on Similarity Measure to Multiple Attribute Decision Making with Trapezoid Fuzzy Linguistic Variables," in *Fuzzy Systems & Knowledge Discovery - Lecture Notes in Artificial Intelligence*, vol. 3613, Springer, 2005, pp. 110-117.

[127] L. Hayden, IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data, McGraw-Hill, Inc., 2010.

[128] Beliakov, Gleb, Ana Pradera & Tomasa Calvo, Aggregation Functions - A Guide to Practitioners, Springer, 2007.

[129] Wheeler, T.A., S.C. Hora, W.R. Cramond & S.D. Unwin, "Analysis of Core Damage Frequency from Internal Events: Experts Jidgment Elicitation," US Nuclear Regulatory Commission, 1989.

[130] Bonano, E.J. & G.E. Apostolakis, "Theoretical Foundations & Practical Issues for Using Expert Judgment in Uncertainty Analysis of High Level Radiocative waste Disposal," *Radioactive Waste Management & the Nuclear Fuel Cycle,* vol. 16, pp. 137-159, 1991.

[131] E. Zio, "On The Use of the Analytic Hierarcy Process in the Aggregation of Expert Judgment," *Reliability Engineering & Systems Safety,* vol. 53, pp. 127-138, 1996.

[132] R. Cooke, Experts in Uncertainty, New York: Oxford University Press, 1991.

[133] G. Rowe, "Perspectives on Expertise in Aggregation of Judgments," in *Expertise & Decision Support*, New York, Plenum, 1992, pp. 155-180.

[134] R. T. Clemen, "Combining Forecasts: A Review & Annotated Bibliography," *International Journal of Forecasting,* vol. 5, pp. 559-583, 1989.

[135] W. Ferrell, "Combining Individuals Judgments," in *Behavioral Decision Making*, Plenum, NY, 1985.

[136] Klir, G.J. & M.J. Wierman, "Uncertainty-based Information: Elements of Generalized Information Theory," *Studies in Fuzziness & Soft Computing,* 1999.

[137] Mosleh, A., V.M. Bier & G. Apostolakis, "Methods for the Elicitation & Use of Expert Opinion in Risk Assessment," US Nuclear Regulatory Commission, 1987.

[138] Liou, T.S. & M.J.J. Wang, "Ranking Fuzzy Numbers with Integral Value," *Fuzzy Sets & Systems,* vol. 50, pp. 247-255, 1992.

[139] Carnegie Mellon University, 2004.

[140] IBM Wireless Security Auditor, IBM , [Online]. Available: www.ibm.com/wsa/.

[141] Peng, Y. et al, "Reaserch about Security Audit Platform in E-Governance System," vol. 3, 2008.

[142] European Union, "Secure SME under the auspices of the 7th Framework Program," EU Secure Project.

[143] Garg, Ashish, Jeffrey Curtis & Hilary Halper, "The Financial Impact of IT Security Breaches: What do Investors Think?," *Security Management Practices,* pp. 22-33, 2003.

[144] Cavusoglu, H. et al, "A Model for Evaluating IT Security Investments," *Communications of the ACM,* vol. 47, no. 7, 2004.

[145] D. Dubois, *Possibility Theory & Statistical Reasoning,* Institut de Recherche en Informatique de Toulouse, 2006.

[146] Dubois, D. & H. Prade, Possibility Theory: An Approach to Computerized Processing of Uncertainty, New York: Plenum Press, 1988.

[147] P. Shenoy, "Using Possibility Theory in Expert Systems," *Fuzzy Sets & Systems,* vol. 52, no. 2, pp. 129-142, 1992.

[148] K. H. Lee, First Course on Fuzzy Theory & Applications, Verlag-Berlin Heidelberg: Springer, 2006.

[149] Ladenheim, Marc L., Brad H. Pollock, Allan Rozanski, Daniel S. Berman, Howard M. Staniloff, James S. Forrester & George A. Diamond, "Extent & Severity of Myocardial Hypoperfusion as Predictors of Prognosis in Patients with Suspected Coronary Artery Disease," *Journal of the American College of Cardiology,* 1986.

[150] Olivry, T., R. Marsella, T. Iwasaki & R. Mueller, "Validation of CADESI-03: A Severity Scale for Clinical Trials Enrolling dogs with Atopic Dematitis," *Vet Dermatol,* vol. 18, no. 2, pp. 78-86, 2007.

[151] B. Ayyub, Risk Analysis in Engineering & Economics, Chapman Hill/CRC, 2003.

[152] DEF STAN 00-55, Requirements for Safety Related Software in Defence Equipment, Part 1, U.K. Ministry of Defence, 1997a.

[153] DEF STAN 00-55, "Requirements for Safety Related Software in Defence Equipoment, Part 2," U.K., Ministry of Defdence, 1997b.

[154] IEC 601-1-4, "Medical Electrical Equipment -part 1: General Requirements for Safety -4," ISO/IEC, 1996-06.

[155] EN 50128, "Railway Applications: Software for Railway Control & Protection Systems," European Committee for Electrotechnical Standardization (CENELEC), 1997.

[156] ANSI X9.30.2, "Public Key Cryptography Using Irreversible Algorithms for the Financial Services Industry," ANSI, 1995.

[157] Wright, David, Serge Gutwirth & Michael Friedewald, "Shining light on the dark side of ambient Intelligence," *Foresight Journal,* vol. 9, no. 2, pp. 46-59, 2007.

[158] R. G. Johnston, "Philosophy on Vulnerability Assessments," Argone Vulnerability Assessment Team, 2010.

[159] A. G. Bluman, Elementary Statistics: A Step By Step Approach, 8th ed., McGraw Hill, 2012.

[160] UNIDO, "Corporate Social Responsibility: Implications of Small & Medium Enterprises (SMEs) in Developing Countries," United Nations Industrial Development Organization (UNIDO), Vienna, 2002.

[161] B. A. Onugu, *Small & Medium Enterprises (SMEs) in Nigeria: Problems & Prospects,* St. Clement University, 2005.

[162] B. Addo, *E-Business Adoption Among SMEs in Ghana: A Case Study of Businesses in The Accra Mall,* Kumasi: Kwame Nkrumah University of Science & Technology (KNUST), 2012.

[163] I. Dey, Qualitative Data Analysis: A User-friendly Guide for Social Scientists, 1st published in 1993 ed., Routledge: Taylor & Francis e-Library, 2005.

[164] Meyers, Lawrence S., Glenn Gamot & A.J. Guarino, Applied Multivariate Research - Design & Interpretation, Thousand Oaks, CA: Sage Publications, 2008.

[165] Raykov, T. & G. Marcoulides, A First Course in Structural Equation Modeling, Mahwah, NJ: Lwarence-Erlbaum, 2000.

[166] Ritchie, Jane, Jane Lewis & Gillian Elam, "Designing & Selecting Samples," in *Qualitative Research Practice: A Guide for Social Science Students & Researchers*, Thousand Oaks, CA, Sage Publications, 2003, pp. 77-108.

[167] Snape, Dawn & Liz Spencer, "The Foundations of Qualitative Research," in *Qualitative Research Practice: A Guide for Social Science Students & Researchers*, Thousand Oaks, Sage Publications, 2003, pp. 1-23.

[168] Strauss, Anselm & Juliet Corbin, Basics of Qualitative Research: Techniques & Procedures for Developing Grounded Theory, Sage Publications, 1998.

[169] Cooper, Donald & Pamela Schindler, Business Research Methods, 11th ed., McGraw-Hill, Inc., 2001.

[170] Polit, Denise & Bernadette Hungler, Essentials of Nursing Research: Methods, Appraisal & Utilization, Philadephia, PA: Lippincott, 1993.

[171] Easterby-Smith, Mark, Richard Lowe & Andy Lowe, Management Research: An Introduction, Sage Publications, 2002.

[172] World Health Organization (WHO), "Revised Injection Safety Assessment Tool - Tool C Revised," WHO Press, 2008.

[173] Visser, P.S., J.A. Krosnick, J. Marquette & M. Curtis, "Mail Surveys for Election Forecasting? An Evaluation of the Columbs Dispatch Polls," *Public Opinion Quarterly,* vol. 60, pp. 181-227, 1996.

[174] P. DePaulo, "Sample Size for Qualitative Research," *Quirk's Marketing Research Media,* December 2000.

[175] D. Bertraux, "From the Life History Approach to the Transformation of Sociological Practice," in *Biography & Society: The Life History Approach in Social Sciences*, London, Sage Publications, 1981, pp. 29-45.

[176] J. Creswell, Qualitative Inquiry & Research Design: Choosing Among Five Traditions, Thousand Oaks, CA: Sage Publications, 1998.

[177] M. Mason, "Sample Size & Saturation in PhD Studies Using Qualitative Interviews," *Forum: Qualitative Social Research,* vol. 11, no. 8, September 2010.

[178] S. Greener, Business Research Methods, Ventus Publishing, 2008.

[179] F. Fowler, Survey Research Methods, 3rd ed., Thousand Oaks, CA: Sage Publications, 2000.

[180] F. Capra, The Tao of Physics: An Exploration of the Parallels Between Modern Physics & Eastern Mysticism, London: Fontana Paperbacks, 1983.

[181] K. H. Esbensen, Multivariate Data Analysis - in Practice, 5th ed., Camo Software, 2010.

[182] Patriciu, Victor, Iustin Priescu & Sebastian Nicolaescu, "Security Metrics for Enterprise Information Systems," *Journal of Applied Quantitative,* no. 2, 2006.

[183] J. Appleyard, "Information Classification: A Corporate Implementation Guide," in *Information Security Management Handbook*, vol. 4, CRC Press, 2002.

[184] P. R. Garvey, Analytical Methods for Risk Management: A Systems Engineering Perspective, Taylor & Francis Group, LLC, 2009.

[185] Sajko, M. et al., "How to Calculate Information Value," *Journal of Information & Organizational Sciences,* vol. 30, no. 2, 2006.

[186] P. K. M'Pherson, "Business Value Modeling," in *48th Federation Internationale d'Information et de Documentation (FID)*, Graz, Austria, 1998.

[187] Fisch, E.A. & G.B. White, Secure Computer & Networks: Analysis, Design & Implementation, Boca Raton: CRC Press, 2000.

[188] Dong, Wen & Jin Peng, "Two Types of Fuzzy Risk Measures with Transform Functions," in *7th International Conference on Fuzzy Systems & Knowledge Discovery (FSKD 2010)*, 2010.

[189] Keeney, Ralph L. & Detlof von Winterfeldt, "A Value Model for Evaluating Homeland Security Decisions," *Risk Analysis,* vol. 31, no. 9, 2011.

[190] D. Viehland, "Managing Business Risk in Electronic Commerce," in *5th Americas Conference on Information Systems*, 2000.

[191] Chongfu, Huang & Shi Peijun, "Fuzzy Risk & Calculation," China Natural Science Foundation, 2001.

[192] Thorani, Y.L.P., Phani B. Rao & Ravi Shankar, "Ordering Generalized Trapezoidal Fuzzy Numbers," *International Journal of Contemporary Mathematics & Sciences,* vol. 7, no. 12, pp. 555-573, 2012.

[193] P. Schmucker, Natural Language Computations & Risk Analysis, Rockville, MD: Computer Science Press, 1984.

[194] Tee, A.B. & M.D. Bowman, "Bridge Condition Assessment Using Fuzzy Weighted Averages," *Civil Engineering Systems,* vol. 8, no. 1, pp. 49-57, 1991.

[195] Wat, F.K.T. & E.W.T. Ngai, "Analysis in Electronic Commerce Development Using Fuzzy Set," in *Joint 9th IFSA World Congress & 20th NAFIPS*, Piscataway, NJ, 2001.

[196] Bojadziev, G. & M. Bojadziev, Fuzzy Logic for Business, Finance and Management, Singapore: World Scientific, 2007.

[197] Talasova, Jana & Pavel Holecek, *Multi-Criteria Fuzzy Evaluation: The FuzzME Software Package,* Palacky University Olomouc, 2009.

[198] Bass, S.M. & H. Kwakernaak, "Rating and Ranking of tysMultiple-Aspect Alternatives Using Fuzzy Sets," *Automata,* vol. 1, no. 1, pp. 47-58, 1977.

[199] Tah, J.H. & V. Carr, "A Proposal for Construction Project Risk Assessment Using Fuzzy Logic," *Construction Management & Economics,* vol. 18, pp. 491-500, 2000.

[200] Wirba, E.N., J.H.M. Tah & R. Howes, "Risk Interdependencies and Natural Language Computations," *Engineering Construction & Architectural Management,* vol. 3, no. 4, pp. 251-269, 1996.

[201] B. Kosko, Neural networks & Fuzzy Systems: A Dynamical Systems Approach to Machine Intelligence, Englewood Cliffs, NJ: Prentice Hall, 1992.

[202] Kandasamy, W., Florentin Smarandache & K. Ilanthenral, Elementary Fuzzy Matrix Theory & Fuzzy Models for Social Scientists, Automaton, 2008.

[203] R. Fuller, "Neural Fuzzy Systems," Abo Akademi University, Abo, 1995.

[204] Hellendoorn, H. & C. Thomas, "Defuzzification of Fuzzy Controllers," *Intelligent Fuzzy Sets,* vol. 1, pp. 109-123, 1993.

[205] T. J. Ross, Fuzzy Logic with Engineering Applications, John Wiley & Sons, 2004.

[206] C. Kahraman, Fuzzy Multi-Criteria Decision Making, Springer Science & Business Media, 2008.

[207] Saaty, Thomas L. & Luis G. Vargas, Decision Making with the Analytic Network Process: Economic, Political, Social and Technological Applications with Benefits, Opportunities, Costs and Risks, Springer Science & Business Media, 2006.

[208] N. K. Kasabov, Foundations of Neural Networks, Fuzzy Systems and Knowledge Engineering, Cambridge, MA: The MIT Press, 1998.

[209] Wang, Shin-Yun & Chih-Chiang Hwang, "An Application of Fuzzy Set Theory to the Weighted Average Cost of Capital and Capital Structure Decision," *Technology & Investment,* vol. 1, no. 4, pp. 248-256, November 2010.

[210] Bilgic, Taner & I. Burhan Turksen, "Measurement Theoretic Frameworks for Fuzzy Set Theory," in *Fuzzy Logic in Artificial Intelligence: Towards Intelligent Systems. Lecture Notes in Artificial Intelligence I188*, Springer, 1997, pp. 252-265.

[211] P. Dadone, *Introduction to Fuzzy Sets,* 1995 ed., vol. 83, J. Mendel, Ed., Proceedings of IEEE, 2000.

[212] A. Abraham, "Artificial Neural Networks," in *Handbook of Measuring System Design*, John Wiley & Sons, 2005, pp. 901-908.

[213] Liu, P. & H. Li, Fuzzy Neural Network Theory & Applications, Singapore: World Scientific, 2004.

[214] Beale, R. & T. Jackson, Neural Computing - An Introduction, London: Taylor & Francis , 1990.

[215] E. O. Yeboah-Boateng, "Using Fuzzy Cognitive Maps (FCMs) To Evaluate The Vulnerabilities With ICT Assets Disposal Policies," *International Journal of Electrical & Computer Sciences IJECS-IJENS,* vol. 12, no. 5, pp. 20-31, October 2012.

[216] Bougaardt, G. & M. Kyobe, "Investigating the Factors Inhibiting SMEs from Recognizing and Measuring Losses from Cyber-crime in South Africa," *The Electronic Journal Information Systems Evaluation,* vol. 14, no. 2, pp. 167-178, 2011.

[217] Siraj, Anbareen, Susan Bridges & Rayford Vaughn, "Fuzzy Cognitive Maps for Decision Support in an Intelligent Intrusion Detection System," *IEEEXplore,* 2001.

[218] Smith, E. & J. Eloff, "Cognitive Fuzzy Modeling for Enhanced Risk Assessment in Health Care Institution," *IEEE Intelligent systems & their Applications ,* pp. 69-75, 2000.

[219] Heydebreck, Peter, Magnus Klofsten & Lars Kruger, "F2C - An Innovative Approach to Use FCM for the Valuation of High-Technology Ventures," *Communications of the IBIMA,* pp. 1-14, 2011.

[220] J.-S. R. Jang, "Adaptive-Network-based Fuzzy Inference System (ANFIS)," *IEEE Transactions on Systems, Man and Cybernetics,* vol. 23, no. 3, pp. 665-685, May 1993.

[221] Lin, Jerry W., Mark I. Hwang & June F. Li, "A Neural Fuzzy System Approach to Assessing The Risk of Earnings Restatements," *Issues in Information Systems,* vol. V, no. 1, pp. 201-207, 2004.

[222] M.Gh. Negoita et al, Induction Machine Diagnostic Using Adaptive Neuro Fuzzy Inferencing System, Springer-Verlag, 2004.

[223] L. Fausett, Fundamentals of Neural Networks: Architectures, Algorithms & Applications, Prentice Hall, 1993.

[224] ITU-T, Security in Telecommunications and Information Technology: An Overview of Issues and the Deployment of Existing ITU-T Recommendations for Secure Telecommunications, Geneva: International Telecommunications Union (ITU), 2006.

[225] M. West, "Preventing System Intrusion," in *Computer & Information Security Handbook*, Morgan-Kaufmann, Inc., 2009, pp. 39-52.

[226] Hsu, Hsi-Mei & Chen-Tung Chen, "Aggregation of Fuzzy Opinions Under Group Decision Making," *Fuzzy Sets & Systems,* vol. 79, pp. 279-285, 1996.

[227] Pappis, Costas & Nikos Karacapilidis, "A Comparative Assessment of Measures of Similarity of Fuzzy Values," *Fuzzy Sets & Systems,* vol. 56, pp. 171-174, 1993.

[228] Nguyen, Hung & Berlin Wu, Fundamentals of Statistics withFuzzy Data, Springer Helderberg, 2006.

[229] A. Gegov, Complexity Management In Fuzzy Systems - A Rule Base Comprehenssion, Berlin Heidelberg: Springer-Verlag, 2007.

[230] R. Babuska, "System Identification Using Fuzzy Models," *Control Systems, Robotics & Automation,* vol. VI, 1997.

[231] MS11-058 - Critical, "Vulnerabilities in DNS server Could Allow Remote Code Execution," MicroSoft Security Bulletin, 2011.

[232] Young, Susan & Dave Aitel, The Hacker's Handbook - Strategies for Breaking Into and Defending Networks, CRC Press, 2007.

[233] Chen, Tom & Patrick Walsh, "Guarding Against Network Intrusion," in *Computer & Information Security Handbook*, Morgan-Kaufmann, Inc., 2009, pp. 53-66.

[234] MS10-030 - Critical, "Vulnerability in Outlook Express & Windows Mail Could Allow remote Code Execution," MicroSoft Inc., 2010.

[235] D. Piscitello, "VLAN Security Guidelines," WatchGuard Technologies, 2004.

[236] C. Kavalla, "How Vulnerable Are Your Cisco IOS Router?," Global Knowledge Training LLC, 2009.

[237] Cisco, "Vulnerabilities Statistics Report," Cisco Security Consulting, 2001.

[238] P. Strassman, "The Internet's Vulnerabilities Are Built Into Its Infrastructure," *Signal Online Magazine,* 2009.

[239] N. K. Karley, "Flooding & Physical Planning in Urban Areas in West Africa: Situational Analysis of Accra, Ghana," *Theoretical & Empirical Researches in Urban Management,* pp. 25-41, 2009.

[240] I. Adelekan, "Vulnerability of Poor Urban Coastal Communities to Flooding in Lagos, Nigeria," *Envrionment & Urbanization,* vol. 22, no. 2, pp. 433-450, 2010.

[241] CORDIS, "Advancing ICT for Disaster Recovery Maanagement in Africa," Community Research & Development Information Service, Brussels, 2010.

[242] A. Caballero, "Information Security Essentials for IT Managers: Protecting Mission-Critical Systems," in *Computer & Information Security Handbook*, Morgan-Kaufmann, Inc., 2009, pp. 225-253.

[243] OECD, "Malicious Software (Malware): A Security Threat to the Internet Economy," Organization for Economic Cooperation & Development, 2009.

[244] Bandy, M.T. et al, "Study of Botnets & their Threats to Internet Security," *Working Papers on Information Security,* 2009.

[245] IETF, "RFC 2812 & ISON," 2001. [Online]. Available: www.irc.org/mla/ircd/2001/.

[246] C. Day, "Intrusion Prevention & Detection Systems," in *Computer & Information Security Handbook*, Morgan-Kaufmann, 2009, pp. 293-306.

[247] Schiller, C., Seth Fogie, Colby DeRodeff & Michael Gregg, InfoSecurity 2008: Threat Analysis, Syngress, 2007.

[248] Georgia Tech, "Emerging Cyber Threats Report for 2009," Information Security Center, 2008.

[249] J. O. Ogalo, "The Impact of Information Systems Security Policies & Controls on Firm Operation Enhancement for Kenyan SMEs," *Prime Journal of Business Administration & Management,* vol. 2, no. 6, pp. 573-781, June 2012.

[250] Wang, Xinyuan & Daniel Ramsbrock, "The Botnet Problem," in *Computer & Information Security Handbook*, Morgan-Kaufmann, 2009, pp. 119-132.

[251] Jacobsson, Markus & Alex Tsow, "Identity Theft," in *Computer & Information Security Handbook*, Morgan-Kaufmann, 2009, pp. 519-549.

[252] Olander, Heidi, Pia Hurmelinna-Laukkanen & Jukka Mahonen, "What's Small Size Got To Do With It? - Protection of Intellectual Assets In SMEs," *International Journal of Innovation Management,* vol. 13, no. 3, pp. 349-370, 2009.

[253] Curtis, G. & D. Cobham, Business Information Systems: Analysis, Design & Practice, Pearson Education Ltd, 2005.

[254] MacLean, D., J. Deane, D. Souter & S. Lilley, "Louder Voices, Strengthening Developing Country Participation in International ICT Decision Making," CTO & Panos, DFID, London, 2002.

[255] Hinton, Geoffrey & Terrence Sejnowski, Unsupervised Learning: Foundations of Neural Computing, MIT Press, 1999.

[256] Business Software Alliance (BSA), "BSA/IDC Global Software Piracy Study," BSA/IDC, 2010.

[257] J. Mallery, "Building a Secure Organization," in *Computer & Information Security Handbook*, Morgan-Kaufmann, Inc., 2009, pp. 3-22.

[258] H. Kwakemaak, "Fuzzy Random Variables: Definitions and Theorems," *Information Science,* vol. 15, pp. 1-29, 1978.

[259] Kruse, R. & K.D. Meyer, Statistics with Vague Data, Reidel: Dordrecht, 1987.

[260] Taylor, B., Marjorie Darrah & Christiana Moats, "Verification & Validation of Neural Neworks: a Sampling Research in Progress," in *Intelligent Computing Theory & Applications*, 2003.

[261] The World Bank, "How to Classify Countries," 20 August 2012. [Online]. Available: www.data.worldbank.org/about/country-classifications.

[262] UN Statistics Division, "United Nations Statistics Division," 20 August 2012. [Online]. Available: www.unstats.un.org/unsd/.

[263] J.-S. R. Jang, "Adaptive-Neural-based Fuzzy Inference System (ANFIS)," *IEEE Transactions on Systems, Man and Cybernetics,* vol. 23, no. 3, pp. 665-685, May 1993.

[264] Z. Yazar, "Threats & Vulnerabilities," 2002.

[265] M. Spivak, Calculus, Texas: Publish or Perish, Inc., 2008.

Appendices

Appendix A- 1: Fuzzy Sets Nomenclature

Symbols	*Meanings*
¯	set NOT (also complement or inversion)
∩	set AND (also intersection operator)
∪	set OR (also union operator)
(x_i, x_j, x_n)	indicates a fuzzy membership value
∈	member of a set (general membership)
poss(x)	the possibility of event x
prob(x)	the probability of event x
{x}	crisp or Boolean membership function
•	dyadic operator or product operator
ξ(x)	The expected value of a fuzzy region
μ	fuzzy membership function (MF)
α	proportionality
μ(x)	membership or truth function in fuzzy set
$\tilde{F}$	Fuzzy function, F
⊗	Cartesian product or space
∅	empty or null set
⇒	implication
∧	logical AND
∨	logical OR
∑	summation
x⊤y	t-norm
x⊥y	t-conorm
|	Such that
(x, μA[x])	Discrete elements of a fuzzy set A with membership function
⊕	Bounded sum operator
⊙	Bounded product operator
≙	Estimates

Appendix A- 2: Training Dataset

Fuzzy Arithmetic Mean					Min Operator					Max Operator					Fuzzified Averages				
confide	integri	availat	threats	risk	confide	integri	availat	threats	risk	confide	integri	availat	threats	risk	confide	integri	availat	threats	risk
0.00	0.00	0.00	3.17	3	0	0	0	2	3	0	0	0	4	3	0.00	0.00	0.00	0.33	0.8
2.12	2.07	2.61	3.00	4	1	1	1	1	4	3	3	4	4	4	0.73	0.72	0.71	0.27	0.4
4.12	4.20	4.17	4.50	3	2	2	3	4	3	5	5	5	5	3	0.33	0.29	0.33	0.07	0.8
4.59	4.60	4.78	1.50	2	3	3	3	1	2	5	5	5	2	2	0.16	0.16	0.09	0.10	0.8
0.00	0.00	0.00	3.82	4	0	0	0	2	4	0	0	0	5	4	0.00	0.00	0.00	0.37	0.4
0.00	0.00	0.00	2.00	2	0	0	0	2	2	0	0	0	2	2	0.00	0.00	0.00	0.07	0.8
1.65	1.67	1.89	3.42	3	1	1	1	2	3	3	3	3	5	3	0.59	0.59	0.64	0.60	0.8
2.71	3.00	3.22	4.27	1	1	1	1	2	1	5	5	5	5	1	0.61	0.64	0.40	0.23	0.4
1.59	1.47	1.67	3.75	1	1	1	1	1	1	3	3	3	5	1	0.59	0.56	0.58	0.37	0.4
0.00	0.00	0.00	2.92	4	0	0	0	2	4	0	0	0	4	4	0.00	0.00	0.00	0.67	0.4
2.71	3.00	3.22	3.25	3	1	1	1	2	3	5	5	5	5	3	0.61	0.64	0.40	0.57	0.8
0.00	0.00	0.00	3.42	1	0	0	0	2	1	0	0	0	5	1	0.00	0.00	0.00	0.47	0.4
4.06	4.07	4.00	3.08	3	3	3	3	1	3	5	5	5	5	3	0.38	0.37	0.40	0.50	0.8
2.06	1.93	2.28	3.67	4	1	1	1	2	4	3	3	4	5	4	0.78	0.75	0.76	0.47	0.4
3.35	3.00	2.83	1.67	3	1	1	1	1	3	5	5	5	4	3	0.40	0.51	0.47	0.57	0.8
2.35	2.33	2.33	3.33	4	1	2	1	1	4	3	3	3	5	4	0.78	0.80	0.78	0.47	0.4
1.65	1.67	1.89	2.17	4	1	1	1	1	4	3	3	3	4	4	0.59	0.59	0.64	0.57	0.4
2.71	3.00	3.22	2.33	5	1	1	1	1	5	5	5	5	4	5	0.61	0.64	0.40	0.70	0
1.59	1.47	1.67	3.42	4	1	1	1	1	4	3	3	3	5	4	0.59	0.56	0.58	0.47	0.4
2.12	2.07	2.06	3.83	3	1	1	1	2	3	4	3	4	5	3	0.68	0.72	0.64	0.40	0.8
1.82	1.60	1.83	3.50	4	1	1	1	1	4	3	2	3	5	4	0.71	0.64	0.69	0.43	0.4
2.29	2.27	1.94	2.58	2	1	1	1	1	2	5	5	5	5	2	0.45	0.48	0.53	0.63	0.8
0.00	0.00	0.00	3.67	3	0	0	0	3	3	0	0	0	4	3	0.00	0.00	0.00	0.13	0.8
2.24	2.20	1.83	3.08	1	1	1	1	1	1	5	4	4	4	1	0.56	0.56	0.51	0.50	0.4
2.00	1.80	1.89	3.67	3	1	1	1	2	3	3	3	3	5	3	0.73	0.69	0.69	0.50	0.8
2.76	2.60	2.44	2.50	1	1	1	1	1	1	3	3	4	5	1	0.75	0.72	0.67	0.47	0.4
2.82	2.87	2.94	4.25	5	1	1	2	3	5	3	3	3	5	5	0.78	0.77	0.80	0.30	0
2.76	2.67	2.33	3.17	2	1	1	1	2	2	4	4	4	5	2	0.56	0.61	0.62	0.57	0.8
1.82	1.73	2.00	2.64	3	1	1	1	2	3	3	3	4	4	3	0.64	0.61	0.62	0.67	0.8
2.29	2.27	2.17	3.17	4	2	1	1	2	4	3	3	3	5	4	0.80	0.77	0.73	0.63	0.4
4.12	4.07	3.72	2.00	5	1	1	1	1	5	5	5	5	4	5	0.28	0.21	0.36	0.67	0
1.59	1.27	1.50	3.58	2	1	1	1	1	2	4	2	5	5	2	0.56	0.51	0.49	0.40	0.8
2.35	2.40	2.11	3.17	4	1	1	1	2	4	4	3	3	4	4	0.71	0.77	0.76	0.63	0.4
1.94	1.67	2.39	3.92	2	1	1	1	2	2	4	3	4	5	2	0.64	0.61	0.64	0.37	0.8
0.00	0.00	0.00	1.13	4	0	0	0	1	4	0	0	0	2	4	0.00	0.00	0.00	0.30	0.4
0.00	0.00	0.00	4.00	3	0	0	0	3	3	0	0	0	5	3	0.00	0.00	0.00	0.37	0.8
2.06	1.80	2.00	3.83	4	1	1	1	2	4	4	4	4	5	4	0.66	0.64	0.62	0.43	0.4
1.71	1.73	1.78	3.91	3	1	1	1	2	3	2	2	2	5	3	0.68	0.69	0.71	0.37	0.8
3.00	3.27	3.33	2.58	4	1	1	1	1	4	5	5	5	4	4	0.42	0.37	0.33	0.60	0.4
2.12	2.07	2.06	2.92	4	2	2	2	1	4	3	3	3	4	4	0.80	0.80	0.80	0.60	0.4
2.12	2.07	2.61	2.50	5	1	1	1	1	5	3	3	4	4	5	0.73	0.72	0.71	0.70	0
4.12	4.20	4.17	4.09	4	2	2	3	3	4	5	5	5	5	4	0.33	0.29	0.33	0.33	0.4
4.59	4.60	4.78	3.64	3	3	3	3	1	3	5	5	5	5	3	0.16	0.16	0.09	0.37	0.8
3.12	3.20	2.94	2.00	4	2	2	2	1	4	4	4	4	3	4	0.64	0.61	0.69	0.77	0.4
3.00	3.00	2.89	3.25	4	1	1	1	1	4	5	5	5	4	4	0.59	0.59	0.64	0.57	0.4
3.06	2.93	2.94	2.25	2	3	1	1	2	2	4	4	4	4	2	0.78	0.75	0.73	0.77	0.8
4.41	4.53	4.39	2.08	3	3	4	2	1	3	5	5	5	5	3	0.24	0.19	0.22	0.57	0.8
3.12	3.13	3.28	2.83	2	2	2	2	1	2	5	5	5	5	2	0.66	0.67	0.62	0.63	0.8
1.29	1.33	1.33	4.33	4	1	1	1	3	4	3	3	3	5	4	0.49	0.51	0.49	0.27	0.4
2.00	2.00	2.00	3.67	2	2	2	1	2	2	2	2	3	4	2	0.80	0.80	0.78	0.50	0.8
2.24	2.07	1.89	3.64	2	1	1	1	1	2	4	3	3	5	2	0.71	0.69	0.67	0.37	0.8
0.00	0.00	0.00	2.00	3	0	0	0	1	3	0	0	0	4	3	0.00	0.00	0.00	0.63	0.8
3.24	3.07	3.61	3.50	4	1	1	2	2	4	5	4	5	5	4	0.54	0.59	0.49	0.50	0.4
1.94	1.93	2.00	2.83	5	1	1	1	1	5	4	4	4	5	5	0.64	0.64	0.64	0.57	0
2.35	2.40	2.00	2.82	4	1	1	1	1	4	3	3	3	5	4	0.78	0.77	0.69	0.60	0.4
3.06	2.80	2.94	2.75	5	2	1	1	1	5	5	4	4	5	5	0.66	0.67	0.67	0.53	0
2.53	2.47	2.39	3.00	2	2	2	1	1	2	4	4	5	5	2	0.73	0.72	0.64	0.53	0.8
1.76	1.67	1.72	1.83	1	1	1	1	1	1	3	2	3	4	1	0.68	0.67	0.67	0.63	0.4
2.18	2.00	2.06	3.33	4	2	2	1	2	4	3	2	3	5	4	0.80	0.80	0.76	0.53	0.4
3.59	3.60	3.11	1.42	4	2	2	1	1	4	4	4	4	2	4	0.54	0.53	0.62	0.57	0.4
3.35	3.33	3.06	2.00	5	2	2	2	1	5	4	4	4	3	5	0.64	0.64	0.71	0.73	0
3.76	3.60	3.39	2.58	4	2	1	1	1	4	5	4	5	4	4	0.45	0.45	0.49	0.70	0.4
3.94	3.80	3.50	1.92	4	3	1	1	1	4	4	4	4	3	4	0.42	0.40	0.51	0.70	0.4
4.06	3.87	3.50	2.25	4	4	1	1	2	4	5	5	5	3	4	0.38	0.37	0.42	0.80	0.4
3.06	2.80	3.17	2.33	4	2	2	2	1	4	5	5	5	5	4	0.64	0.69	0.58	0.63	0.4
3.29	3.13	3.28	3.33	4	2	2	2	2	4	4	4	4	5	4	0.61	0.67	0.64	0.53	0.4
3.65	3.53	3.17	2.58	4	2	1	1	2	4	4	4	4	3	4	0.52	0.48	0.56	0.80	0.4

Appendix A- 3: Testing Datasets

Fuzzy Arithmetic Mean					Min Operator					Max Operator					Fuzzified Averages				
confide	integri	availat	threats	risk	confide	integri	availat	threats	risk	confide	integri	availat	threats	risk	confide	integri	availat	threats	risk
1.71	1.73	1.78	3.91	3	1	1	1	2	3	2	2	2	5	3	0.68	0.69	0.71	0.37	0.8
3.00	3.27	3.33	2.58	4	1	1	1	1	4	5	5	5	4	4	0.42	0.37	0.33	0.60	0.4
0.00	0.00	0.00	2.25		0	0	0	2		0	0	0	3		0.00	0.00	0.00	0.27	0
3.35	3.00	2.83	2.00	3	1	1	1	2	3	5	5	5	2	3	0.40	0.51	0.47	0.13	0.8
2.35	2.33	2.33	3.00		1	2	1	1		3	3	3	4		0.78	0.80	0.78	0.17	0
1.65	1.67	1.89	2.00	3	1	1	1	1	3	3	3	3	4	3	0.59	0.59	0.64	0.17	0.8
2.71	3.00	3.22	2.00		1	1	1	1		5	5	5	4		0.61	0.64	0.40	0.17	0
1.59	1.47	1.67	2.00	3	1	1	1	2	3	3	3	3	2	3	0.59	0.56	0.58	0.13	0.8
2.29	2.07	2.28	3.50	4	1	1	1	2	4	5	5	5	5	4	0.64	0.64	0.64	0.33	0.4
3.00	3.27	3.33	2.08	2	1	1	1	1	2	5	5	5	5	2	0.42	0.37	0.33	0.57	0.8
0.00	0.00	0.00	2.00		0	0	0	1		0	0	0	3		0.00	0.00	0.00	0.27	0
2.82	2.80	2.94	2.50	4	1	1	1	2	4	5	5	5	3	4	0.38	0.37	0.38	0.13	0.4
2.47	2.87	2.67	2.80		1	1	1	2		4	4	4	4		0.66	0.61	0.64	0.30	0
0.00	0.00	0.00	3.50	4	0	0	0	2	4	0	0	0	4	4	0.00	0.00	0.00	0.17	0.4
0.00	0.00	0.00	2.00		0	0	0	1		0	0	0	3		0.00	0.00	0.00	0.10	0
4.59	4.60	4.78	2.00	2	3	3	3	1	2	5	5	5	3	2	0.16	0.16	0.09	0.20	0.8
3.12	3.20	2.94	2.25	4	2	2	2	1	4	4	4	4	3	4	0.64	0.61	0.69	0.23	0.4
0.00	0.00	0.00	2.75	3	0	0	0	2	3	0	0	0	4	3	0.00	0.00	0.00	0.23	0.8
4.12	4.20	4.17	2.00	4	2	2	3	2	4	5	5	5	2	4	0.33	0.29	0.33	0.13	0.4
0.00	0.00	0.00	2.67	3	0	0	0	2	3	0	0	0	3	3	0.00	0.00	0.00	0.20	0.8
4.59	4.60	4.78	3.17	3	3	3	3	1	3	5	5	5	5	3	0.16	0.16	0.09	0.13	0.8
3.12	3.20	2.94	4.00	4	2	2	2	2	4	4	4	4	5	4	0.64	0.61	0.69	0.17	0.4

Appendix A- 4: Security Positions

Zero (0)	One (1)	Two (2)	Three (3)	Four (4)	Five (5)	Six (6)	Seven (7)	Eight (8)	Nine (9)	Ten (10)	➢ Ten (10)
48	12	20	3	2	2	0	0	1	0	0	1
53.9%	13.5%	22.5%	3.4%	2.2%	2.2%	0	0	1.1%	0	0	1.1%

Appendix A- 5: Security Losses in US$ Per Year

≤ 1K	≤ 2K	≤ 3K	≤ 4K	≤ 5K	≤ 10K	≤ 15K	≤ 25K	≤ 50K	≤ 100K
68	2	2	3	4	3	3	1	1	2
76.4%	2.2%	2.2%	3.4%	4.5%	3.4%	3.4%	1.1%	1.1%	2.2%

Appendix A- 6: Unauthorized Access Per Year

≤ 10	≤ 20	≤ 50	≤ 100	≤ 1000	≤ 10000	≤ 100000	> 100000
72	3	2	4	2	1	1	1
84.3%	3.4%	2.2%	4.5%	2.2%	1.1%	1.1%	1.1%

Appendix A- 7: Taxonomy of Vulnerabilities Dataset

	CoreSwitches			DNS Server			Databases		
criticality	6.57	7.82	9.07	4.93	6.50	8.07	7.14	8.25	9.35
urgency	7.86	8.89	9.93	7.29	8.46	9.64	7.57	8.68	9.79
	Email Server			Router			Web Server		
criticality	6.22	7.39	8.57	6.50	7.75	9.00	5.64	7.00	8.36
urgency	7.57	8.29	9.50	7.86	8.89	9.93	6.71	8.04	9.36

Triangular fuzzy numbers of various cyber-assets.

Appendix A- 8: Taxonomy of Threat Dataset

	natural disaster			powerfailure			Spam			Viruses			Spyware			
coreswitch	5.00	6.39	7.78	3.79	5.21	6.64	2.50	4.03	5.57	3.78	5.17	6.56	3.92	5.39	6.85	
dnsserver	5.43	6.82	8.21	4.50	5.79	7.07	2.28	3.96	5.64	5.57	6.89	8.21	3.86	5.39	6.92	
databases	6.93	8.03	9.14	5.00	6.36	7.72	4.00	5.46	6.93	5.93	7.18	8.42	5.71	6.96	8.21	
emailserver	5.64	6.89	8.14	5.43	6.72	8.00	4.93	6.40	7.86	6.64	7.85	9.06	5.78	7.10	8.42	
router	6.07	7.35	8.64	4.58	6.01	7.44	2.64	4.25	5.86	5.36	6.61	7.86	3.85	5.28	6.71	
webserver	5.22	6.50	7.79	4.42	5.85	7.28	3.57	5.11	6.64	6.14	7.39	8.64	4.86	6.15	7.44	
	Hacking			Poor Authentication			Unscanned Attachment			Social Engineering			No Backup			
coreswitch	4.50	5.95	7.40	4.30	5.90	7.50	3.30	4.85	6.40	3.20	4.85	6.50	6.10	7.40	8.70	
dnsserver	4.50	5.95	7.40	5.50	6.95	8.40	3.00	4.70	6.40	2.20	3.85	5.50	6.70	7.80	8.90	
databases	6.80	7.90	9.00	6.40	7.65	8.90	5.40	6.95	8.50	4.90	6.40	7.90	8.00	9.00	10.00	
emailserver	5.40	6.70	8.00	6.00	7.35	8.70	5.40	6.70	8.00	3.20	4.75	6.30	7.10	8.30	9.50	
router	5.20	6.60	8.00	5.20	6.60	8.00	2.70	4.20	5.70	2.50	4.10	5.70	5.80	7.00	8.20	
webserver	5.50	6.75	8.00	5.70	7.10	8.50	4.20	5.75	7.30	3.10	4.75	6.40	6.80	8.05	9.30	

Triangular fuzzy numbers of threats.

Appendix A- 9 : Datasets of Experts Opinions

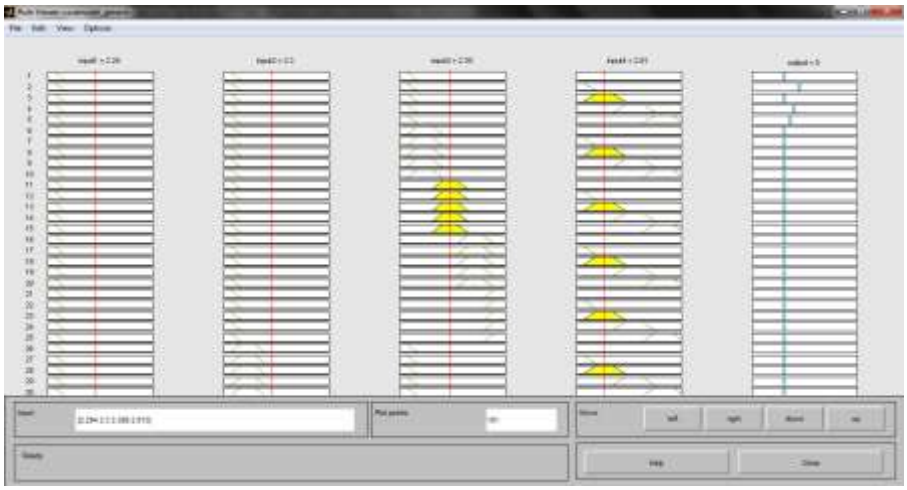
experts	Fuzzy Triangular Numbers(l)	Fuzzy Triangular Numbers (c')	Fuzzy Triangular Numbers(r')	relative importance	degree of importance	average agreement degree	relative agreement degree	consensus degree coefficients
E1	8	9	10	1	0.09	0.75	0.06	0.07
E2	6	7.5	9	0.8	0.08	0.88	0.08	0.08
E3	6	7.5	9	0.8	0.08	0.88	0.08	0.08
E4	6	7.5	9	0.8	0.08	0.88	0.08	0.08
E5	6	7.5	9	0.8	0.08	0.88	0.08	0.08
E6	6	7.5	9	0.8	0.08	0.88	0.08	0.08
E7	6	7.5	9	0.8	0.08	0.88	0.08	0.08
E8	6	7.5	9	0.8	0.08	0.88	0.08	0.08
E9	6	7.5	9	0.8	0.08	0.88	0.08	0.08
E10	6	7.5	9	0.8	0.08	0.88	0.08	0.08
E11	3	5	7	0.6	0.06	0.74	0.06	0.06
E12	3	5	7	0.6	0.06	0.74	0.06	0.06
E13	3	5	7	0.6	0.06	0.74	0.06	0.06
E14	3	5	7	0.6	0.06	0.74	0.06	0.06

Dataset collated from the experts opinions elicitation study

Appendix A- 10: Results of ANFIS Training, Checking & Testing Errors (Original figures)

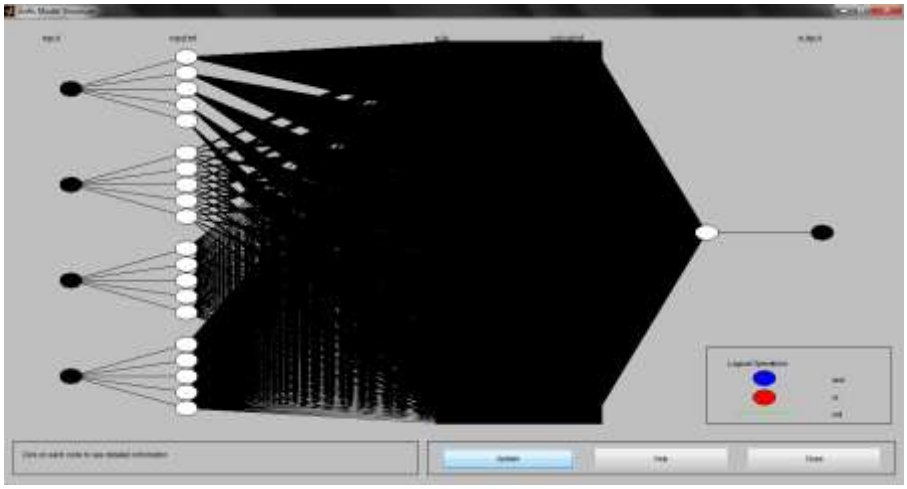
		arithmetic mean	min operator	max operator	fuzzified average
Triangular MFs	training	0.159488	1.00254	0.777855	0.188186
	checking	3.73724	1.86624	1.72203	0.377566
	testing	0.15949	1.0025	0.77785	0.1887
Trapezoidal MFs	training	0.087682	1.00254	0.777855	0.16925
	checking	2.42168	1.87243	1.71179	0.527704
	testing	0.087682	1.0025	0.77785	0.16925
Gaussian MFs	training	0.086388	1.00254	0.777855	0.135743
	checking	2.26983	1.96705	1.63243	1.754271
	testing	0.086388	1.0025	0.777855	0.13825

Appendix B- 1: Rules Viewer

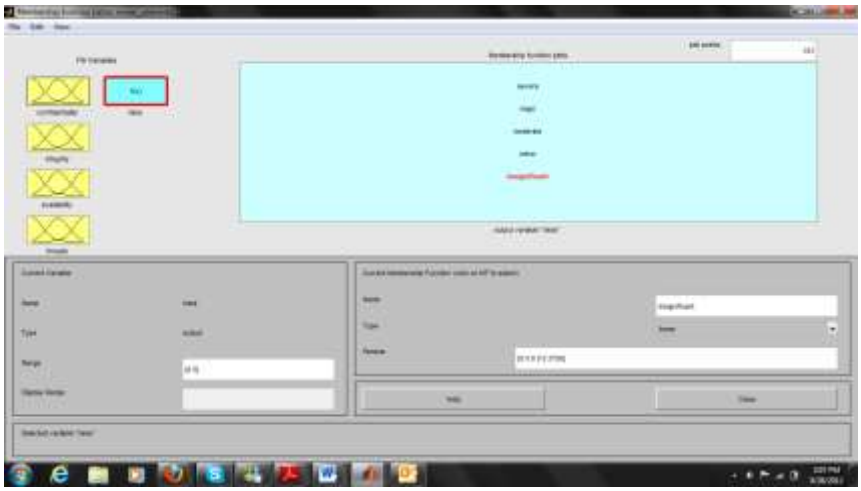


Fuzzy Rules viewer showing firing states and the corresponding risk evaluation.

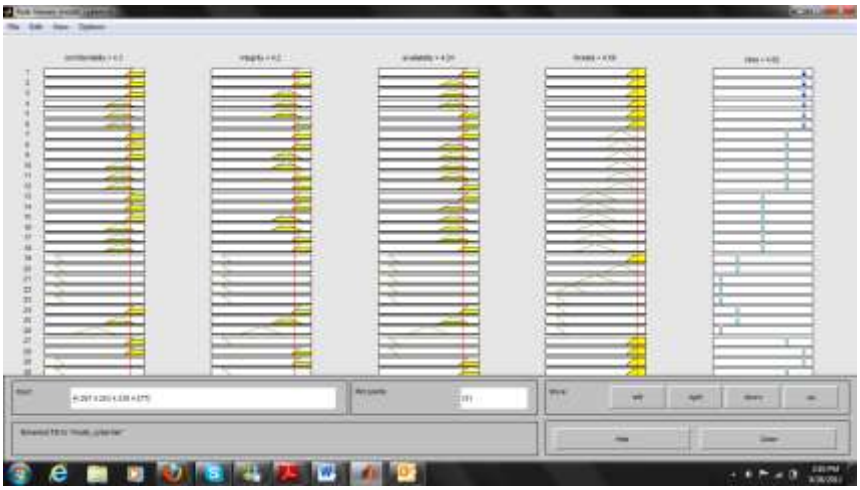
Appendix B- 2: Structure of CSVA Model_generic (Grid Partition Dataset Generated)



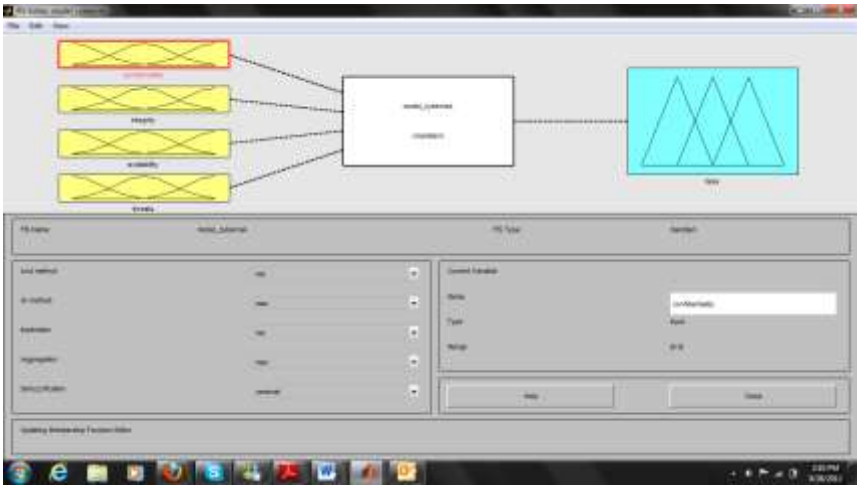
Appendix B- 3: ANFIS Sugeno Model



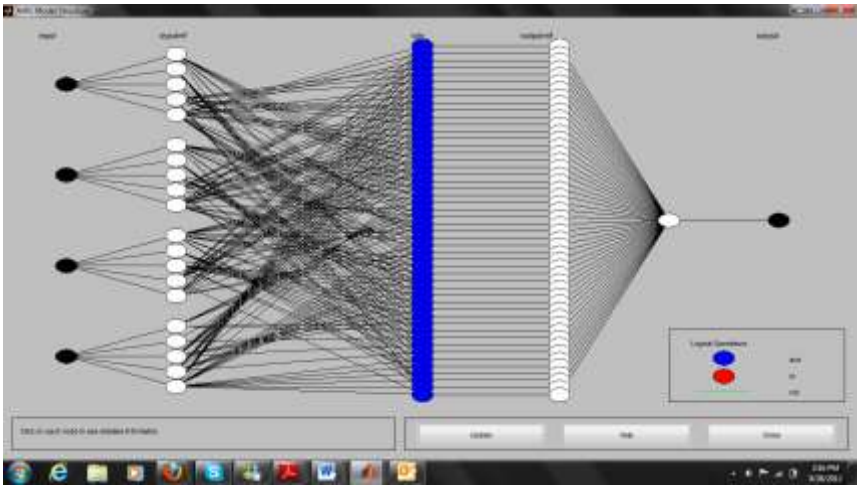
Appendix B- 4: Rules Viewer



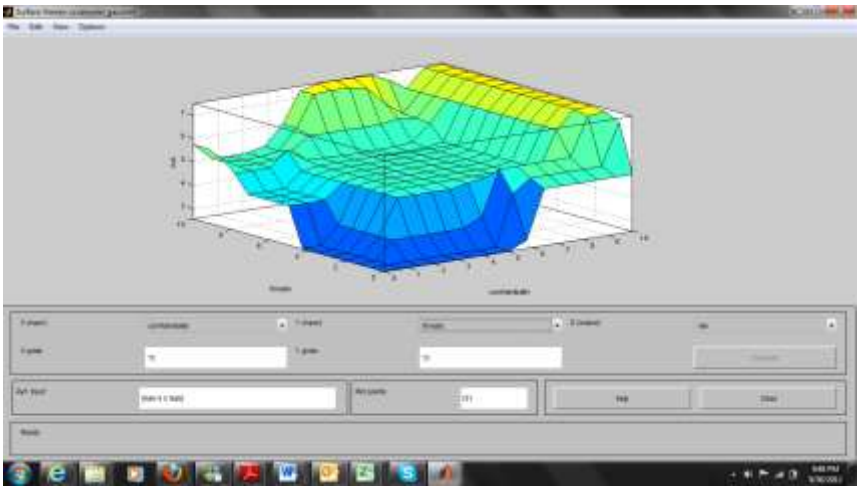
Appendix B- 5: ANFIS Mamdani Model



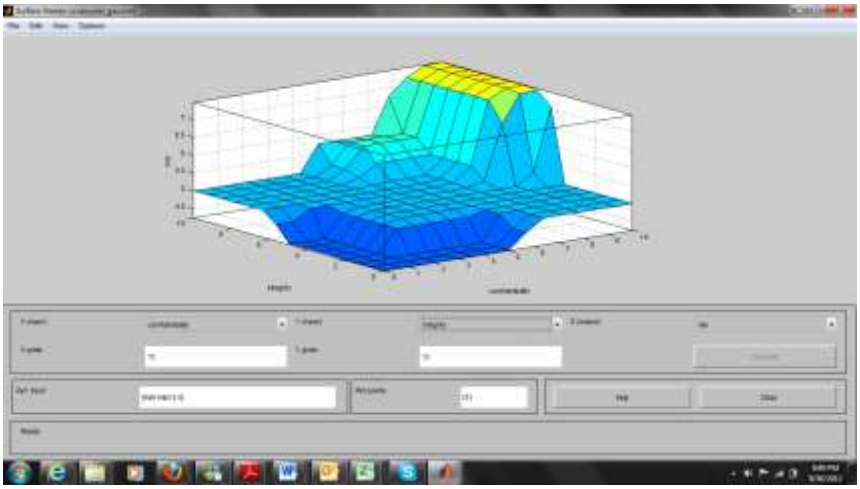
Appendix B- 6: Structure with Experts Rules



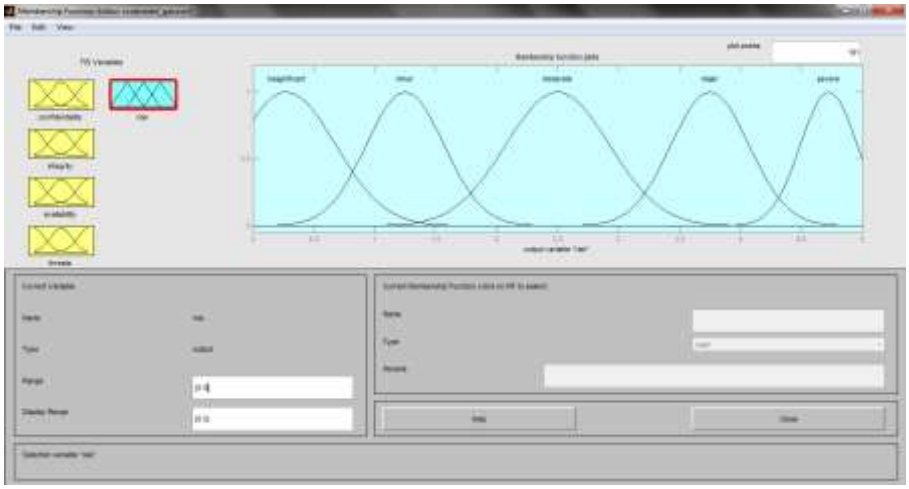
Appendix B- 7: Triangular MFs – Surface View (Before Training)



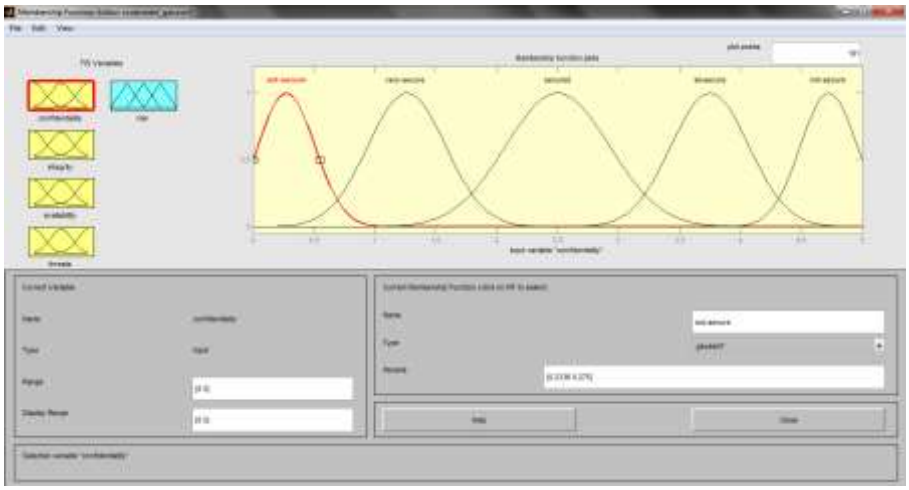
Appendix B- 8: Gaussian MFs – Surface View (Before Training)



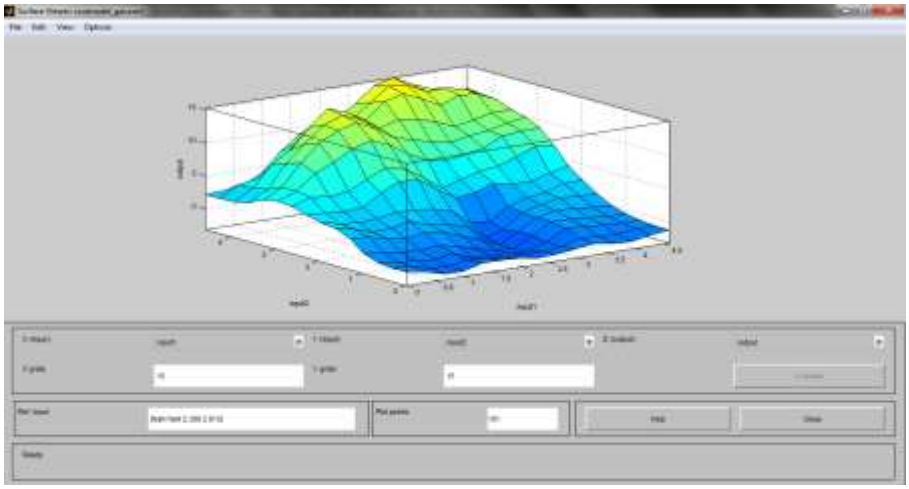
Appendix B- 9: Gaussian MFs – Risk Linguistic Terms



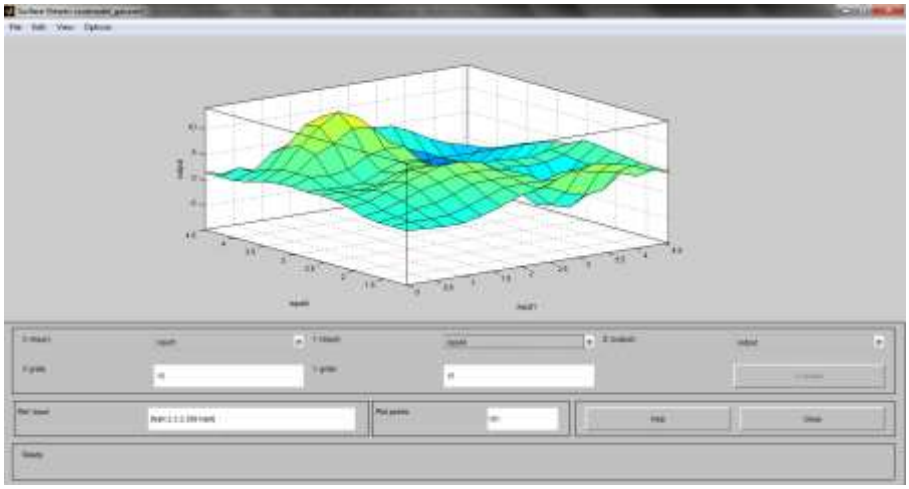
Appendix B- 10: Gaussian MFs – Confidentiality Linguistic Terms



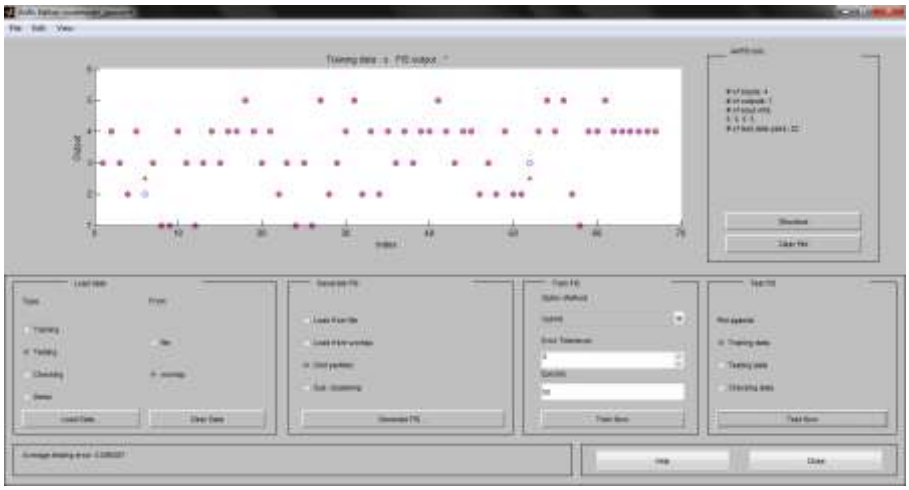
Appendix B- 11: Gaussian MFs – Surface View (After Training)



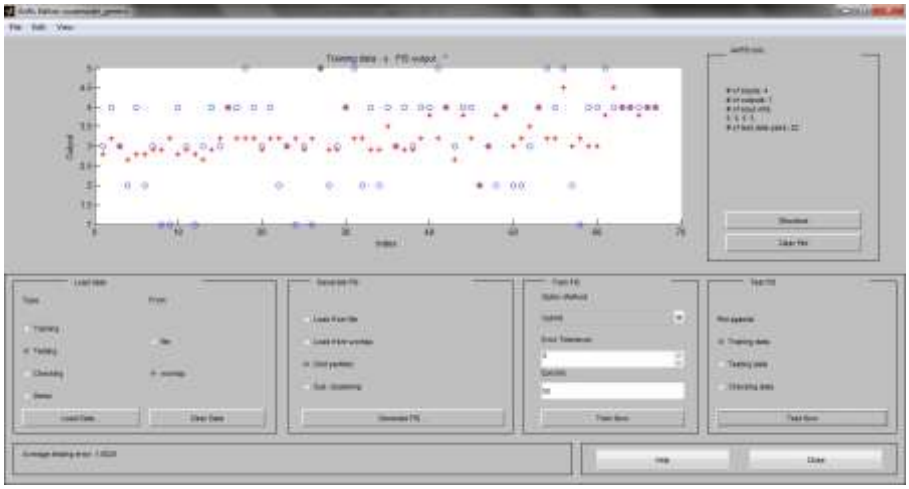
Appendix B- 12: Triangular MFs – Surface View (After Training)



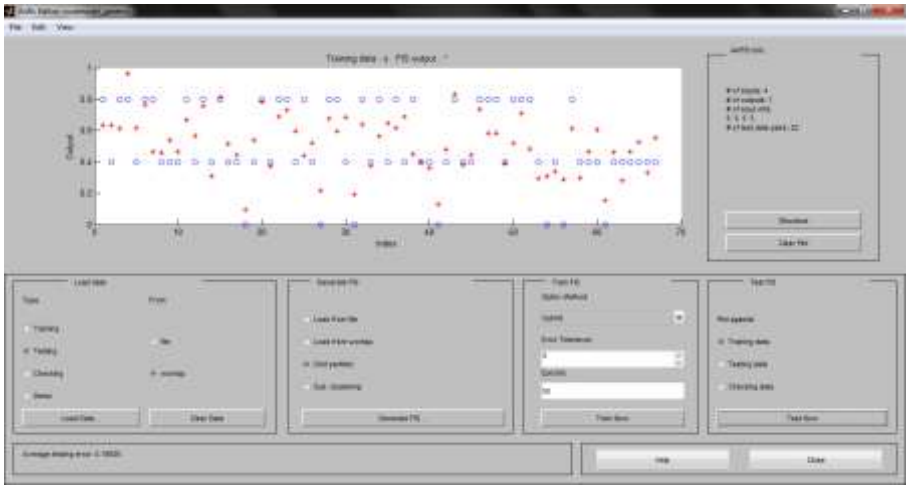
Appendix B- 13: Training versus Testing (Fuzzy Arithmetic Mean) Datasets



Appendix B- 14: Training versus Testing (min operator) Datasets



Appendix B- 15: Training versus Testing (fuzzified averages) Datasets



Appendix C 1: Cyber-Security: Vulnerabilities & Threats on SMEs

The Philosophy underlying the study:

ISO 27005 defines Vulnerability as: a weakness of an asset or group of assets that can be exploited by one or more threats; where an asset is anything that can have value to the organization, its business operations and their continuity, including information resources that support the organization's mission".

Most vulnerability methods are "overly binary" in outlook, i.e. something is either vulnerable or it is not. For this study we shall look at the fuzzy aspects of vulnerability so as to address all necessary and possible attributes of cyber-security vulnerabilities. It must be noted that there are vulnerabilities without risk; i.e. when the affected asset has no value.

The Vulnerabilities survey shall address the following attributes – their Type, Source and Severity:

- *a weakness in a system that can be exploited to violate the system's intended behavior relative to confidentiality, integrity and availability;*
- *vulnerabilities are inherent in the design, operation, or operational environment of a system;*
- *vulnerabilities result from errors of omission, error of commission, and operational errors during the life of a system.*

Open ended Questions! If necessary please provide as much information as appropriate.

1. What services do you provide? (please list 5)

2. How many of your ICT positions are dedicated to security?

3. What is the estimated loss from security events, in US$, over the last 1 year period?

4. What is the number of unauthorized access detected in the past year?

5. Do you have Acceptable Use policy document?

6. Is the policy document signed by all end-users?

7. Do you have Remote Access Policy document?

8. Do you have a recycle bin or a paper shredder?

9. How are data sheets or documents trashed in the organization?

10. Who is responsible for collecting the company's trash? (e.g. a contractor or an in-house dept.)

This Questionnaire is aimed at investigating the impact of cyber-security vulnerabilities on SMEs in developing economies. Please take a few moments to answer the following questions. **Thanks!**

11. Please indicate the number of employees in your organization.
a) less than 10 b) 10 – 49 c) 50 – 99 d) 100 – 250 e) over 250

12. How would your business be affected if your systems or network were compromised or harmed?
a) minor cosmetics b) some repairs needed c) major repairs d) devastating e) unrecoverable damage

13. What techniques are used to authenticate users?

a) no authentication b) single factor (e.g. user ID + password) c) hardware second factor (e.g. smartcards) d) software 2nd factor (e.g. digital certificates + tokens)e) 3rd factor (e.g. biometrics)

14. Do you have data classification policy?
a) No, not necessaryb) somewhat c) under preparationd) drafted policy e) yes, clearly defined

15. Do you scan your systems regularly with updated software? (such as anti-virus, spyware detection)?
a) not at all b) seldom c) once d) often e) very often

16. Do you scan all email attachments and files downloaded from the Internet?
a) not at all b) seldom c) once awhile d) often e) always

17. How often do you backup your important files and data?
a) never b) once a while c) monthly d) weekly e) daily

18. Does the security spending generate the expected returns?
a) not at all b) slightly c) somewhat d) very e) extremely

19. What is the percentage of network devices that are security compliant?
a) less than 10% b) 10 – 49% c) 50 – 79% d) 80 – 99% e) 100%

20. How secured are you against hackers trying to break into your web server?
a) not secured b) slightly secured c) secured d) very secured e) extremely secured

21. How secured are you against your colleagues finding out your password and using your credentials to do something unethical?
a) not secured b) slightly secured c) secured d) very secured e) extremely secured

22. How secured are you against viruses or worms coming in to your system via email?
a) not secured b) slightly secured c) secured d) very secured e) extremely secured

23. How secured are you from the liability of having an employee surf inappropriate websites?
a) not secured b) slightly secured c) secured d) very secured e) extremely secured

24. How secured against an employee copying your sales data onto his USB hard drive or taking away personal, financial information about your customers?
a) not secured b) slightly secured c) secured d) very secured e) extremely secured

25. How secured are you against your server crashing and bringing all business or productivity to a catastrophic halt?
a) not secured b) slightly secured c) secured d) very secured e) extremely secured

General Information!

- Critical – greatest impact (with extreme disruption) on business; must be present for the business to operate;
- Vital – necessary in order for the business to resume operations beyond contingency recovery stage;

- Important – minimal near-term impact on business if disrupt, but essential for normal operations;
- Minor – no real impact to business over the near-to-mid-term ;
- Very Minor – insignificant impact and considered as non-essential services.

Using the criteria above, Please List 5 key assets of your organization and rate them in relation to the impact on your business should that asset be attacked or exploited.

Assets	Very Minor	Minor	Important	Vital	Critical

PLEASE CHECK the appropriate possibility of occurrence or likelihood. Thanks!

Vulnerabilities/ Threats	*Possibility of Occurrence (Likelihood)*				
	Very Low	*Low*	*Medium*	*High*	*Very High*
Infrastructure					
sabotage or interruption of DNS server					
sabotage or interruption of mail server					
sabotage or interruption of print server					
sabotage or interruption of HVAC					
sabotage or interruption of power plant					
Fire in the co-location facility					
Flood damage to infrastructure					
Communications Systems					
interrupt or denial-of-service for voice, data and/or video services					
exploit or theft of telecom services (voice, data,video)					
unauthorized access to electronic transmissions (wireless, voice, data, etc.)					
unauthorized disclosure of data					
unauthorized modification of data					
Disruption of ns1, DNS, NAT servers					
Human					
unauthorized facility access					
end-user safety					
Products & Services					
sabotage or tampering with products or service					
Brands & Reputation					
tampering with product or service					

Vulnerabilities/ Threats	*Possibility of Occurrence (Likelihood)*				
	Very Low	*Low*	*Medium*	*High*	*Very High*
unauthorized information					
compromise or disclosure of corporate information					
other malicious modification of internal or external information (website, press release or other info sources)					
misinformation or incorrect news					
internet chat room or email based sabotage					
Other Assets & Resources					
theft or reallocation of company assets					
modification of systems					
materials of offensive purposes					
exploitation of company expertise or experts for criminal gains					
`					

Appendix C 2: Expert Opinion Elicitation on Cyber-security

Expert Opinion Elicitation on Cyber-Security

Page One

Dear Valued ICT Expert Thank you for taking time to participate and to share your views with us in this survey. You have been specially selected as an ICT Expert for your candid opinions and/or perception relating to cyber-security threats and their impact on organizations. Please take a few moments to answer the following questions. Note: This survey is for academic research and the answers shall be treated with confidentiality. Should you have any questions about the survey, please feel free to email the researcher at ezer@cmi.aau.dk or ezer@es.aau.dk or call +45-5162 7120 or Skype: "ezeeer". Thanks! Best Regards, Ezer

1. What is your highest level of education?

- professional certificate
- diploma
- first degree
- second degree
- third degree

2. How many years have you worked in the ICT sector?

- less than 1 year
- between 1 and 4 years
- between 5 and 9 years
- between 10 and 15 years
- over 15 years

3. What level of management are you?

- associate
- senior associate
- manager
- senior manager

- ○ chief officer

4. What is your level of responsibility?

- ○ follow & assist
- ○ apply & enable
- ○ ensure & advise
- ○ initiate & influence
- ○ strategize & inspire & mobilize

5. What is the level of independence for your job function?

- ○ dependent
- ○ consult before action
- ○ ability to delegate
- ○ decisions with approval
- ○ decisions without approval

6. Please make a choice in respect of the type of impact should a particular threat affect an asset.

	Fire, Flood, Earthquake *	Power Failure *	Sapm *
Router	-- Please Select --	-- Please Select --	-- Please Select --
DNS Server	-- Please Select --	-- Please Select --	-- Please Select --
Web Server	-- Please Select --	-- Please Select --	-- Please Select --
Email Server	-- Please Select --	-- Please Select --	-- Please Select --
Core Switches	-- Please Select --	-- Please Select --	-- Please Select --
Databases	-- Please Select --	-- Please Select --	-- Please Select --

7. Depending on business and in the event of an attack or failure of any asset, what would be the response?

	Criticality *	Urgency *
Router	-- Please Select --	-- Please Select --
DNS Server	-- Please Select --	-- Please Select --
Web Server	-- Please Select --	-- Please Select --
Email Server	-- Please Select --	-- Please Select --
Core Switches	-- Please Select --	-- Please Select --
Databases	-- Please Select --	-- Please Select --

Thank You!

Thank you very much for taking our survey. Your responses are very important to us. Ezer; center for Communications, Media & Information technologies (CMI); dept. of Electronic Systems; Aalborg University, Copenhagen.

Appendix –D: 5.1.1. Fuzzy Sets & Logic

Sets are generally represented by enumerating its members or elements. A general set X, with n members, for instance, is represented by $X = \{x_1, x_2, x_3, \ldots\ldots, x_n\}$. There are various methods used in set representation or notation; e.g. $x_i \in X$; $\forall\ i = 1, 2, \ldots\ldots, n.$ or $X = \{x \mid x_i, i = 1, 2, \ldots\ldots, n\}$ or $X = \{x_i \mid i \in I\}$, where I is the set of integers.

Note that, the set with no members is defined as the Empty set or Null set, and it is denoted by $\emptyset$.

Let X and Y be two sets, such that $X \subseteq Y$, then X is said to be the subset of Y. If $X \neq Y$, and some members of Y are not involved with X at all, then $X \subset Y$ and X is said to be a proper subset of Y [148].

Sets can also be defined by the number of elements or members involved, called Cardinality |X|. e.g. a set $X = \{x_1, x_2, x_3, x_4, x_5\}$ has cardinality $|X| = 5$. The set X can have $2^{|X|}$ possible combinatorial subsets, defined as the power set of X and its cardinality is denoted by $|P(X)| = 2^{|X|}$.

So for $X = \{x_1, x_2, x_3\}$, its power set is the collection of subsets in X including the set itself, given by $P(X) = \{\emptyset, \{x_1\}, \{x_2\}, \{x_3\}, \{x_1, x_2\}, \{x_1, x_3\}, \{x_2, x_3\}, \{x_1, x_2, x_3\}\}$

i.e. $|P(X)| = 2^{|X|} = 2^3 = 8$, subsets constituting the power set of X.

Unlike classical crisp sets, fuzzy sets have grade of belonging or membership functions. So, a fuzzy set is a mapping $\mu : X \rightarrow [0,1]$, where X is any set called the domain and [0,1] the range, i.e. μ is thought of as a characteristic or membership function [6] [5]. In summary, a member of a fuzzy set must satisfy the following conditions [47]:

Fuzzy Logic

Prof. Lotfi A. Zadeh [6] introduced the fuzzy sets theory as an approach in treating uncertainties. He posited that whereas probability deals with the uncertainty of occurrences due to randomness, possibility deals with the uncertainty of vagueness and he espoused the essence of graded membership functions. Fuzzy sets can practically and quantitatively represent vague concepts. Fuzzy sets theory caters for imprecision and vagueness and has wide applications in engineering and sciences.

The utility of fuzzy sets theoretic is seen in the use and application of fuzzy data which is usually expressed subjectively in natural languages with human reasoning. The perceived uncertainties inherent in the metrics used in many systems and applications are appropriately handled and analyzed using fuzzy sets theory [6] [258] [46] [259] .

The fuzzy logic theory is just a prolongation of conventional logic where partial set membership could exist, rule conditions could be satisfied partially, and system outputs are calculated by interpolation [6]. Fuzzy logic is thought of as a bridge over the precision-based classical crisp logic and the imprecision of real world and its human reasoning [5].

Fuzzy logic is an attempt to represent the human reasoning and to approximate its qualitative linguistic and subjective nature. In order to apply fuzzy logic to model real world problems, the knowledge must be structured. That is, the subjectivity inherent in the knowledge would be "normalized" or made objective. By so doing, the fuzzy linguistic terms are treated with the same standard treatment. Generally, human knowledge is fuzzy; it is usually expressed in linguistic terms such as "young", "secured", "vulnerable" – which are fuzzy in nature. The linguistic terms are constructed to form fuzzy sets. Fuzzy logic treats every logical system as a fuzzified system with parameters estimated by degrees of "contribution" [209]. Fuzzy logic is first and foremost multi-valued logic and its grade of membership facilitate the capture and inclusion of most system attributes and constructs.

Membership Function (MF)

One key issue with fuzzy set theory is how to define the appropriate membership functions of the fuzzy sets. A membership function defines the extent of compatibility of a fuzzy linguistic variable with the fuzzy concept, that is, to what degree is the variable or term a member of the concept or phenomenon [47]. In practice, a number of approaches are used including, using definitions by the model expert, using data from the system to be modeled to generate them, or by trial-and-error.

Bilgic & Turksen [210] posited that the several options available for the membership functions estimation are based on one's interpretation of fuzziness as a concept. Some schools of thought have held the likelihood view, random view, similarity view, utility view and measurement view [210]. Depending on one's persuasion, a particular view may be used for the estimation of membership values. Bilgic & Turksen [210] explain each of the views in details, but here's a brief illustration of each view. For instance, considering a fuzzy statement "the PC is secured" with membership value of 0.85. Bilgic & Turksen [210] illustrated that:

- likelihood view – indicates that 85% of a sampled population declared that the PC is secured;
- random view – indicates that 85% of a given population described the PC as secured;
- similarity view – indicates that the PC's security is estimated away from the prototypical PC which is "truly" secured to the degree of 0.15;
- utility view – indicates that 0.85 is the utility value of asserting that the PC is secured; and
- measurement view – indicates that in comparison with other systems or PCs, and measured per a prescribed scale, the PC is secured at 0.85.

This research deals with non-numerical quantities, for instance *"Integrity"*, which cannot be measured against a numerical scale. An example of such a universe could be the quintuples {Very-Low, Low, High, Very-High, Extra-High}. The notion of fuzzy sets is transparent and highly intuitive as it captures the essence in which a real world is perceived and described [42].

The following are definitions of some commonly used nomenclature in this thesis and literature, in general. Figure 5-1 illustrates some key fuzzy concepts.

> *Definition 5-1: Membership Function:* Let X be the set with members or elements x, then a fuzzy set A defined in X is given by the duality or the ordered pair (x, $\mu_A(x)$); where $\mu_A(x)$ is the characteristic or membership function for the fuzzy set A. i.e. $A=\{(x,\mu_A(x))\,|\,x\in X\}$. The membership function $\mu_A(x)$ defines the grade of membership of the members x into the set A. It indicates the degree or extent of compatibility with the fuzzy concept [47]. For a typical fuzzy set A, $\mu_A(x)$: x ⟶ [0, 1], such that $\mu_A(x) = 0$ implies that the "member" doesn't belong to the set A, whereas $\mu_A(x) = 1$ implies full membership.

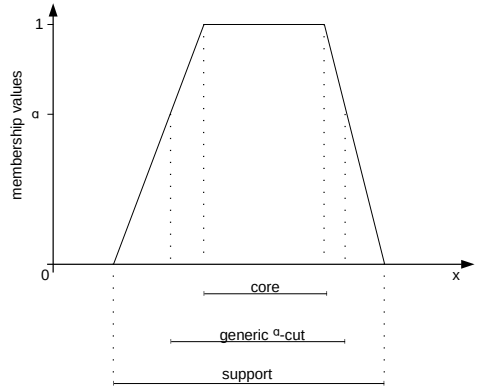


Figure 5- 1: Illustration of Fuzzy Sets, Membership Functions & Key Concepts

Definition 5-2: Domain: defines the total allowable range of values for a fuzzy linguistic term; usually a set of real numbers, which increase monotonically[20] [47].

Definition 5-3: Fuzzy Partition: A number of fuzzy subsets defined by n-tuple { y_1, y_2, y_3, ……., y_n} are said to be the fuzzy partition of X if and only if (IFF): $Y \neq X$ and $y_i \neq \emptyset \ \forall \ i = 1, 2, \ldots, n$ and

$$y_i \cap y_j \neq \varnothing \ \ \forall i \neq j \ \exists \ x \in X; \ \ \sum_{i=1}^{n} \mu_{y_i}(x) = 1.$$

Definition 5-4: Universe of discourse or universe, U: the universe defines the characteristics and total allowable range of all possible values assigned to the linguistic variables. U may be discrete or continuous, and may have ordered or non-ordered elements.

Definition 5-5: Support of membership function (written supp(A)): The support of a fuzzy set A is the set containing all the members with membership function values greater than zero (0) and given by $\sup p(A) = \{x \in X \mid \mu_A(x) > 0\}$.

Similarly, a *fuzzy Singleton* is a fuzzy set that has only one element or a single member which has a membership function value $\mu_A(x) = 1$.

Definition 5-6: *Alpha-cut sets or α-cut:* Let $\mathbf{A}$ be a fuzzy set in the universe of discourse, $\mathbf{X}$. Let α be a number belonging to the fuzzy unit interval [0, 1], which is a threshold restriction. Then α-cut of $\mathbf{A}$, denoted by $\mathbf{A}_\alpha$, is a crisp set with all elements of $\mathbf{A}$ with membership function values in $\mathbf{A}$ greater than or equal to α. i.e. $\mathbf{A}_\alpha = \{x : \mathbf{A}(x) \geq \alpha\}$ or $\mathbf{A}_\alpha = \{x : \mu_{\mathbf{A}}(x) \geq \alpha\}$. The α-cut concept finds applications in engineering and science, as it facilitates the execution of fuzzy rules and intersection of fuzzy sets [18] [47]. This is an important facility that controls the execution of fuzzy rules as well as the intersection of multiple fuzzy sets.

A strong α-cut is defined as $\mathbf{A}_{\alpha+} = \{x : \mathbf{A}(x) > \alpha\}$ or $\mathbf{A}_{\alpha+} = \{x : \mu_{\mathbf{A}}(x) > \alpha\}$. If $\alpha = 1.0$, then the crisp set α-cut is called the CORE set of the fuzzy set $\mathbf{A}$. For ease of statistical inference and interpretation, a nested set of quartile α-cut is defined, such that $nested \ \mathbf{A}_\alpha = \{x : \mathbf{A}(x) \to \alpha \geq \alpha_i\}; \forall i = 1,2,3,4,5$ or α receives the values 1, 0.75, 0.50, 0.25, 0. When $\alpha = 0$, the α-cut set defines the SUPPORT set of the fuzzy set $\mathbf{A}$. For α values 0.75, 0.50, 0.25, the sets are defined as the upper quartile set, mid-quartile set and the lower quartile set, respectively. When $\alpha = 0.5$, α-cut set is called the Crossover point; that is $\mu_{\mathbf{A}}(x) = 0.5$.

Definition 5-7: Convex Set: a fuzzy set A is convex if and only if (IFF) for any $(x_i, y_i) \in X$ such that $x = (x_i \mid i \in N)$ and $y = (y_i \mid i \in N)$, where N is the set of natural numbers in U; and for any point $z \in X$ and $\mu_X(z) \geq \min(\mu_X(x), \mu_X(y))$; $z = (\lambda x_i + (1 - \lambda) y_i \mid i \in N), \ \forall \lambda \in [0, 1]$.

[20] A function f defined on a real interval with arguments x_i, such that $f(x_i)$; $i \in I$, f exhibits the tendency of monotonicity, if:

- $x_1 \prec x_2 \Rightarrow f(x_1) \prec f(x_2)$, f is said to be increasing monotonically; and
- $x_3 \prec x_4 \Rightarrow f(x_3) \succ f(x_4)$, f is said to be decreasing monotonically.

Definition 5-8: Fuzzy Number: a fuzzy number is an imprecise quantity, expressed as a fuzzy set in the set of non-negative real numbers, R^+, used to define a fuzzy interval with normalized and convex membership function. For example, fuzzy numbers are used to realistically represent the real world statement "the PC is secured by 0.85" as follows:

- (0.75, 0.85, 0.95) - as a triangular fuzzy number;
- (0.75, 0.80, 0.90, 0.95) - as a trapezoidal fuzzy number; and
- (0.65, 0.85, 1.0) - as a bell-shaped fuzzy number.

There are various types of characteristic or membership functions, usually defined as discrete or continuous, and by their characteristic shapes. The following are the most common and applicable ones to this study [211] [148]:

i. discrete membership function $A = \sum_{x_i \in X} \mu_A(x_i) / x_i$

ii. continuous membership functions $A = \int_X \mu_A(x) / x$

a. increasing monotonic membership function $f(x \mid a,b,c) = \begin{cases} 0 & \forall\ x \le a \\ 2(\frac{x-a}{c-a})^2 & \forall\ a \le x \le b \\ 1-2(\frac{x-a}{c-a})^2 & \forall\ b \le x \le c \\ 1 & \forall\ c \le x \end{cases}$

b. decreasing monotonic membership function $f(x \mid a,b,c) = \begin{cases} 1 & \forall\ x \le a \\ 1-2(\frac{x-a}{c-a})^2 & \forall\ a \le x \le b \\ 2(\frac{x-a}{c-a})^2 & \forall\ b \le x \le c \\ 0 & \forall\ c \le x \end{cases}$

iii. continuous piece-wise membership function

a. triangular membership function $\mu_A(x) = \begin{cases} \frac{x-a}{b-a} & \forall\ a \le x \le b \\ \frac{x-c}{b-c} & \forall\ b \le x \le c \\ 0 & otherwise \end{cases}$

b. trapezoidal membership function $\mu_A(x) = \begin{cases} \frac{x-a}{b-a} & \forall\ a \le x \le b \\ 1 & \forall\ b \le x \le c \\ \frac{x-d}{c-d} & \forall\ c \le x \le d \\ 0 & otherwise \end{cases}$

c. Bell-shaped membership function $\mu_A(x) = ke^{-(\frac{x-a}{b})^2}$, where parameters a represents the mean, b is non-zero, and k is a height delimiter of the curve.

Appendix –D: 5.1.2. Fuzzy Set Operations

Generally, fuzzy set operations are used in dealing with fuzzy numbers or membership values for applicable manipulations of linguistic terms within the fuzzy variables. There are so many fuzzy set operations, but this sub-section enumerates the key ones that are used frequently in this study. Any relevant operators that are not defined hereunder are defined in context when applicable.

The following basic Zadeh fuzzy set operators are worth noting:

i. union set C = A ∪ B, such that $\mu_{A\cup B}(x) = \max(\mu_A(x), \mu_B(x)) \Rightarrow$
$\mu_C(x) = \max(\mu_A(x), \mu_B(x))$ or $\mu_C(x) = \mu_A(x) \vee \mu_B(x)$

ii. intersection set C = A ∩ B, such that $\mu_{A\cap B}(x) = \min(\mu_A(x), \mu_B(x)) \Rightarrow$
$\mu_C(x) = \min(\mu_A(x), \mu_B(x))$ or $\mu_C(x) = \mu_A(x) \wedge \mu_B(x)$ and

iii. complement set $\overline{A}$, such that $\mu_{\overline{A}}(x) = 1 - \mu_A(x)$

iv. normalization, NORM (A): $\mu_{NORM(A)}(x) = \mu_A(x) / \max(\mu_A(x)); \ \forall \ x \in X.$

Note that, the Zadeh min-max operations are commutative; that is the propositions can be interchangeable without affecting the output function or value.

The following illustrations are used in applying Zadeh's [6] extension principles for triangular fuzzy numbers X = {a, b, c} and Y = {e, f, g}.

i. Addition of two fuzzy numbers: $(a,b,c) \oplus (e, f, g) = (a+e, b+f, c+g)$

ii. Multiplication of two fuzzy numbers: $(a,b,c) \otimes (e, f, g) \cong (ae, bf, cg)$

Aristetolian crisp set theory has two laws of non-contradiction and excluded middle, to ensure sanctity with set operations; i.e. $\mathbf{A} \cap \overline{\mathbf{A}} = \varnothing$ and $\mathbf{A} \cup \overline{\mathbf{A}} = U$ respectively. Original Zadeh fuzzy set operators for union, "max" and intersection, "min", were based on algebraic sum and product respectively. Interestingly, under fuzzy set theory:

- there's no law of non-contradiction, i.e. $\mathbf{A}_f \cap \overline{\mathbf{A}_f} \neq \varnothing$
- there's no law of excluded middle, i.e. $\mathbf{A}_f \cup \overline{\mathbf{A}_f} \neq U$

The fuzzy set operations of min, max and compliment violate these laws. Literature exists in support of alternative fuzzy set theoretic operators. These are useful in building practical fuzzy models, especially as regards fuzzy intersection and complement [47]. Notable amongst them are the triangular-norm (or t-norm) for fuzzy intersection and triangular-conorm (or t-conorm, a.k.a. s-norm) for fuzzy union, which are based on axioms[21]. Adopting the symbolic operands ⊤ and * for t-norm, and ⊥ for t-conorm, the following conditions are defined:

- $\bullet \ (x,y) \leq \min(x,y)$ and $\perp(x,y) \leq \max(x,y)$
- $\bullet \ (x,y) = \bullet \ (y,x)$ - commutative condition for t-norm;
- $\perp(x,y) = \perp(y,x)$ - commutative condition for t-conorm;
- $\bullet \ (x,0) = 0; \ \bullet \ (x,1) = x$ - boundary condition for t-norm;
- $\perp(x,0) = x; \ \perp(x,1) = 1$ - boundary condition for t-conorm.

Usually, t-norm and t-conorm operands are operated on the membership function values, $\mu_A(x)$. Lee, K.H. [148] posited that for practical purposes the generic symbolic * is used in model designs when it is not certain whether the operand will be t-norm or t-conorm. This approach facilitates easy review of the model design.

Besides the fuzzy set operations afore-mentioned, there exist others called compensatory operators as they compensate for the Zadeh minimum, maximum and complement operators.

Let f be a function so-called as the class operator, representing a class of set theoretic transformations, on fuzzy sets A and B in X and Y respectively; then generally:

- Intersection - $A \cap B = A \square B = f_{AND}(\mu_A(x), \mu_B(y), k)$
- Union - $A \cup B = A \square B = f_{OR}(\mu_A(x), \mu_B(y), k)$
- Complement - $\overline{A} = f_{COMP}(\mu_A(x), k)$

Where k is a generic algebraic transformer, which may be applied as a measure of fuzziness in the model [47]. Note that, the simplicity or complexity of these operators is dependent upon the functional transformations of k. Examples of the simple transformers class operators are the bounded sum and product, as well as the mean (or averaging) operators [47]. The utility of a particular class operator in a fuzzy model is dependent upon model expert's experience, the problem at hand (of course) and the effects of fuzzy propositions [63] [47].

Larsen [63] illustrates the utility of mean operators by applying them to importance weightings in multi-criteria fuzzy decision-making. He distinguishes between the use of AND (minimum) and OR (maximum) operators with his multiplicative and implicative operators respectively, as applied to importance weighting generalized means. The Yager class is a typical example of the complex class operators. The Yager classes of intersection and union operators are suitable alternative operators of the Zadeh minimum (AND) and maximum (OR), by facilitating the flexible adjustment of key fuzzy concepts or propositions on a case-by-case basis [47].

Appendix –D: 5.1.3. Fuzzy Relations & Graphs

Let a ∈ X and b ∈ Y be defined such that a relation R is also defined by R = {(a, b) | a ∈ X, b ∈ Y}

[21] An axiom is a premise assumed to be true in a domain of analysis, and it is used as a basis for inference or deduction.

where R is said to be the binary relation of the set $X \square Y$; $\square$ is a generic set operator on the sets X and Y. It implies that $\forall\ (a,b) \in R,\ R \subseteq X \square Y$ (i.e. R is a subset of the product set $X \square Y$).

By extension, if X and Y are fuzzy sets, i.e. X, Y ∈ [0, 1] then the relation R is such that

$$\mu_R : X \square Y \rightarrow [0,1] \text{ and } R = \{((a,b), \mu_R(a,b)) \mid \mu_R(a,b) \geq 0,\ a \in X,\ b \in Y\}.$$

For fuzzy binary relations, $\mu_R(x,y)$, if $\mu_R(x_1,y_1) \geq \mu_R(x_2,y_2)$, then (x_1,y_1) is said to be more strongly related or more influential than (x_2,y_2).

For any two sets A and B, there are four methods or approaches of representing the relationship between them; namely, bipartigraph, coordinate diagram, matrix and directed graph (digraph) [148].

i. Bipartigraph – uses arcs or edges (c.f. directed graph);
ii. Coordinate diagram – represents a graph with A on the abscissa axis (x-axis) and B on the ordinate axis (y-axis);
iii. Matrix – represents the members or elements in an array; i.e.

$$\mathbf{m}_{ij} = \begin{cases} 1,\ (a_i, b_j) \in R \\ \quad \forall\ i = 1,2, \ldots\ldots, m;\ j = 1,2, \ldots, n; \\ 0,\ (a_i, b_j) \notin R \end{cases}$$

iv. Directed graph or Digraph – represents elements as nodes and the relations between the elements as directed edges.

A fuzzy vector is a set V : $v_i \longrightarrow [0, 1], \forall\ i = 1, 2, \ldots\ldots,\ n$. Typically, V is called a row vector if V is a *1xn* set or V is called a column vector if V is an *nx1* set. A fuzzy matrix is so defined as a collection of fuzzy vectors, i.e. a fuzzy matrix $\mathbf{M}_{mxn}$ is given by $\mathbf{M}_{mxn} = (\mathbf{x}_{ij});\ \forall\ i = 1,2, \ldots\ldots, m \text{ and } j = 1,2, \ldots\ldots, n;$ where m and n are the number of rows and columns respectively. The members of the matrix are given by the membership values of the relationship.

The following matrix operations apply:

i. $X + Y = \max(X_{ij}, Y_{ij})$
ii. $X \square Y = \min(\max(X_{ij}, Y_{ij}))$
iii. Fuzzy scalar product is given by αX, where α is scalar such that $0 \leq \alpha \leq 1$. This operation is useful in the computation of fuzzy weighted averages or means, where the weighting factor may be a scalar quantity.

Appendix –D: 5.1.4. Fuzzy Rule-based Systems

Fuzzy logic is concerned with the inherent imprecision of describing the fuzzy concepts themselves, rather than the inaccuracies or noise associated with the metrics [47].

Fuzzy systems consist of a series of conditional and/or unconditional fuzzy statements, correlation, implication, and aggregation methods and decomposition or defuzzification techniques. The fuzzy statements (or rules) are fired in "parallel processing paradigm", except that some rules have no significant degrees in their premises and so fail to contribute to the outcome [47].

A typical fuzzy system is premised on the following basic concepts and stages in a fuzzy modeling, as depicted by Figure 5-2.

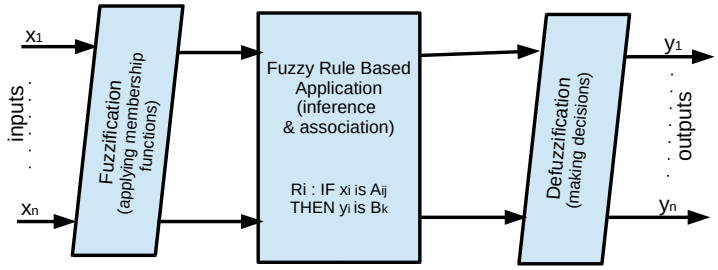


Figure 5- 2: Block Diagram of a Fuzzy System

First, it defines basic building blocks of linguistic variables and terms by fuzzifying the data. Fuzzification is the process of applying membership functions and numeric values to the linguistic variables and terms, respectively.

For each term of an input linguistic variable, a membership value $\mu_{A_{ij}}(x)$ is given. Illustrating with the statements "the router is vulnerable" and "the vulnerability is high", a fuzzy linguistic variable "Vulnerable" is defined and a linguistic term "high", from the fuzzy set {very low, low, medium, high, very high} is involved. The fuzzy statements "the router is vulnerable" and "the vulnerability is HIGH" are typical propositions that are used in formulating fuzzy rule-based models.

There are several kinds of fuzzy rules used to construct fuzzy models. These fuzzy rules are classified into various types depending upon their consequent form. The generic fuzzy rule base, with fuzzy sets A and B, is of the form:

IF (Antecedent) THEN (Consequent); or R : IF x is A, THEN y is B.

In practice one of the following rule bases is applied:

- Constant consequent: $\mathbf{R_i : IF\ X_1 \text{ is } A_{i1} \text{ and } \ldots\ldots\ldots \text{ and } X_n \text{ is } A_{in},\ THEN\ Y \text{ is } C_i}$
- Linear consequent: $\mathbf{R_i : IF\ X_1 \text{ is } A_{i1} \text{ and } \ldots\ldots\ldots \text{ and } X_n \text{ is } A_{in},\ THEN\ Y \text{ is } b_0 + b_1x_1 + \ldots + b_ix_i}$
- Fuzzy set consequent: $\mathbf{R_i : IF\ X_1 \text{ is } A_{i1} \text{ and } \ldots\ldots\ldots \text{ and } X_n \text{ is } A_{in},\ THEN\ Y \text{ is } B_i}$

where X_i's and Y denote input and output variables respectively. The AND is a standard logic operator.

The antecedent or premise linguistic terms A_{ij} are parameterized fuzzy sets whose shape is determined by a few parameters or membership functions, such as Triangular fuzzy sets, Trapezoidal fuzzy sets, Gaussian fuzzy sets, etc. This study employs the fuzzy set *consequent* type as dictated by the empirical data and in support of the problem of interest or model.

The next stage is the application of the fuzzy rule bases to the model for analysis. This process is commonly referred to as the Fuzzy Inference engine. Here conclusions or consequents are drawn from existing facts and available knowledge [48]. The inference engine examines the rules based on a predetermined order. It uses the available knowledge from premises or antecedents to determine the consequent statements. The process is iterative and it goes on until predetermined output values or variables are known.

Kirschfink & Lieven [49] categorized the inference process into three (3); namely *aggregation, implication and accumulation;* and brief illustrations are adopted from [49]:

> "*Aggregation is the calculation of the fulfillment of the whole rule, based on the fulfillments of the individual premises. This process generally corresponds to the logical AND operator of the individual premise expressions."*
>
> *"Implication, based on the certainty factors of the premises, calculates the corresponding degree of certainty for the conclusion. This is called the degree of fulfillment. This step represents the conclusion of the logic statement '**IF** A **THEN** B'."*
>
> *"Accumulation is the process of unifying the various conclusions resulting from the varied degrees of fulfillment for the same consequent. It is usually carried out using the logical OR operator." [paraphrased by researcher]*

Lee, K.H. [148] espouses two (2) key fuzzy implication functions with the definitions below:

i. Mamdani Fuzzy Implication Function – interprets the relation with the minimum operator, i.e.

$$R_m = A \text{ x } B = \int_{X\times Y} \mu_A(x) \wedge \mu_B(y) \Big/ (x,y) \qquad [5\text{-}23]$$

By extension, the Mamdani inference method uses the min operator for implication and the max-min operator for the composition. That is, for the generic rule

$R_i : IF\ x_1 \text{ is } A_i \text{ AND } x_2 \text{ is } B_i, \text{ THEN y is } C_i;\ \forall\ i = 1,2, \ldots..,n;$ then

$$R_i = (A_i \text{ AND } B_i) \rightarrow C_i \ \Rightarrow\ \mu_{R_i} = \mu_{(A_i \ AND\ B_i \rightarrow C_i)}(x_1, x_2, y) \Leftrightarrow$$

$$\mu_{R_i}(y) = \mu_{C_i}(y) = [\mu_{A_i}(x_1) \text{ AND } \mu_{B_i}(x_2)] \rightarrow \mu_{C_i}(y)$$
$$= [\mu_{A_i}(x_1) \wedge \mu_{B_i}(x_2)] \square \mu_{C_i}(y)$$
$$= \alpha_i \square \mu_{C_i}(y)$$

$$where\ \alpha_i = [\mu_{A_i}(x_1) \wedge \mu_{B_i}(x_2)]$$

ii. Larsen Fuzzy Implication Function – interprets the relation with the dot product operator, i.e.

$$R_l = A \text{ x } B = \int_{X\times Y} \mu_A(x) \square \mu_B(y) \Big/ (x,y) \qquad [5\text{-}24]$$

Similarly, the Larsen inference method uses the dot product operator for implication, and the max-product operator for the composition; i.e.

$R_i: IF\ x_1 \text{ is } A_i \text{ AND } x_2 \text{ is } B_i, \text{ THEN y is } C_i;\ \forall i = 1,2, ...,n;$ then

$$R_i = (A_i \text{ AND } B_i) \rightarrow C_i \ \Rightarrow \ \mu_{R_i} = \mu_{(A_i \ AND \ B_i \rightarrow C_i)}(x_1, x_2, y) \Leftrightarrow$$

$$\mu_{R_i}(y) = \mu_{C_i'}(y) = [\mu_{A_i}(x_1) \text{ AND } \mu_{B_i}(x_2)] \rightarrow \mu_{C_i}(y)$$
$$= [\mu_{A_i}(x_1) \wedge \mu_{B_i}(x_2)] \square \mu_{C_i}(y)$$
$$= \alpha_i \square \mu_{C_i}(y)$$
$$where\ \alpha_i = [\mu_{A_i}(x_1) \wedge \mu_{B_i}(x_2)]$$

Appendix –D: Fuzzy Modeling:

Let z be a fuzzy output solution variable, then there exists a fuzzy set Z, such that

$$\mathbf{Z}_i \square z_i = f(y_i) \qquad [5\text{-}25]$$

Where y_i are the consequent propositions; f is a fuzzy implication transfer function, that evaluates the consequent propositions. Typically, the implication transfer function correlates the semantic labels from the rules to generate a compatible fuzzy output solution [47]. It must be noted that in fuzzy modeling, this is done in consideration of various factors, such as empirical data, linguistic variables and terms, fuzzy rules or propositions, and the associated control conditions, in a cohesive manner.

From equation [4-3], membership values are correlated and aggregated (usually by AND or OR connectors) as the implication transfer function is updated to create the output solution space [47]. Cox [47] illustrates this with two (2) generic transfer functions; namely the monotonic reasoning transfer function (or monotonic selection) and the fuzzy compositional rules transfer function.

The monotonic selection is the "simplest" fuzzy inference whereby fuzzy consequences are evaluated "proportionally" in association with the output space Z_y.

i.e. $R_i:$ IF x is A, THEN z is Y or $z = f(\{x, A\}, Y)$ or $Z_y = f(\mu_A(x), \delta_y)$

where $\mu_A(x)$ is the membership function value of x in A and δ_y is the corresponding value of the consequent associated with the output domain Z_y [47]. It must be noted that this approach does not employ any compositional nor decomposition methods.

On the other hand, the compositional rules inference approach correlates and aggregates the antecedents in respect of each contribution that is more than the pre-defined "current" α-cut.

Cox [47] posits that there are two key methods of fuzzy compositional inference systems: - the min-max method, and - the fuzzy additive method; which differ only by the mode of updating the solution outputs.

The min-max rules of Implication: This approach restricts the consequents by evaluating the minimum membership value and then updates the output by taking the maximum of the minimized fuzzy consequents. i.e.

$\mu_{cfs}(x_i) \square \min(\mu_{pt}(x_i), \mu_{cfs}(x_i))$ and $\mu_{sfs}(x_i) \square \max(\mu_{sfs}(x_i), \mu_{cfs}(x_i))$.

The fuzzy Additive Rules of Implication: This approach differs from the min-max in the updating of the fuzzy solution variable by applying the bounded-sum operation to the fuzzy output region; i.e.

$\mu_{cfs}(x_i) \square \min(\mu_{pt}(x_i), \mu_{cfs}(x_i))$ and $\mu_{sfs}(x_i) \square \max(1, \mu_{sfs}(x_i) \oplus \mu_{cfs}(x_i))$.

Note that, the addition is bounded by the unit interval [0, 1] to ensure that the output remains within the fuzzy set.

One drawback with the min-max inference approach is that only rules with membership values more than the α-cut threshold contribute to the solution output. This is overcome by accumulating all contributions of each proposition [47].

Defuzzification means dropping a "plumb-line" to some point on the underlying domain. At the point where this line crosses the domain axis the expected value of the fuzzy set is read. Thus, the defuzzification functions are aimed at "finding" the best point in the fuzzy output solution space. Essentially, it implies that all "defuzzification algorithms are a compromise with or a trade-off between the need to find a single point and the loss of information that such a process entails" [47].

There are two main categories of fuzzy inference systems (FIS), namely, Mamdani FIS and the Takagi-Sugeno-Kang (TSK) or as it is usually referred to as Sugeno FIS [59] [60] [61]

The Mamdani FIS was introduced by Mamdani and Assilian in 1975 [59]. It is characterized by both fuzzy inputs and fuzzy output(s). As in all fuzzy inference systems, the crisp input is fuzzified into a set of linguistic variables. The fuzzy inference engine processes the fuzzified variables with corresponding fuzzy IF-THEN rules and draws fuzzy conculsions. These are then defuzzified and converted onto crisp value(s) as output(s).
On the other hand, the Sugeno FIS, which was first introduced by Takagi and Sugeno in 1985 [61], and later refined by Sugeno and Kang in 1988 [60], has only fuzzy inputs, but gives out crisp output, either as a constant or a linear relation. So similar fuzzification is undertaken by the inference engine and then a crisp output is given without the need for defuzzification.

Appendix –D: 5.2 Neural Networks Theory

An artificial neural network (ANN) or neural network, for brevity, is an artificial intelligence program or algorithm, an information processor with computational approach that imitates the way the brain handles and stores information. Artificial neural networks brain-like attributes facilitate the ability to learn, adapt and automatically classify similar 'classes' together [208]. ANN is an information processor with capability to receive, process and transmit information signals, and usually used in cognitive, perceptual and control applications [212]. Also, neural networks can execute those functions on massive and complex datasets [213] [214].
Artificial neural networks are generalized models of human cognition, based on the following assumptions, that:

- Information processing occurs at many simple elements called Neurons;
- Signals are passed between neurons over connection links;
- Each connection link has an associated multiplicative weight, which, in a typical neural network, multiplies the signal transmitted to reproduce synaptic effect[22];
- Each neuron applies an activation function (usually non-linear) to its net input (sum of weighted input signals) to determine its output signals.

A neural network is characterized by [223]:

- Its pattern of connections between the neurons, defining the network structure, called its Architecture;
- Its method of evaluating and updating or determining the weights on the connections, through calibration or learning, called its Training session or Learning Algorithm; and
- Its Activation Function; examples of which are threshold function, piece-wise linear function and the sigmoid function.

The Input-output training data is fundamental for these networks as it conveys the information which is necessary to discover the optimal operating point.
Figure 5-3 depicts the functions of a basic neural network, consisting of the following:

- An input, with weight(s) assigned to it, such as a set of inputs $X = \{x_1, x_2, ..., x_n\}$ with corresponding weights $W = \{w_1, w_2, ..., w_n\}$, which are small arbitrary values set during model initialization and are also updated during training sessions, and a bias or threshold value, b, which is a constant, sometimes represented by a special input x_0 and may take the value of unity (1).
- An input summation function, that computes and aggregates all input signals to the neuron; i.e.

$$N = \sum_{i=1}^{n} x_i w_i + b$$

- An activation, which is a transfer function transforming the neuron's firing strength, and its an argument of the output function; and
- An output, which is the resultant signal from the neuron based on its activation strength and given by

$$O_j \square a = f(x_i w_i + b) \qquad [5\text{-}26]$$

[22] Synaptic Effect is the ability of the neurons to raise or lower electrical potential of the neuron based on a threshold, in order to send (fire) a signal or not (Abraham, 2005).

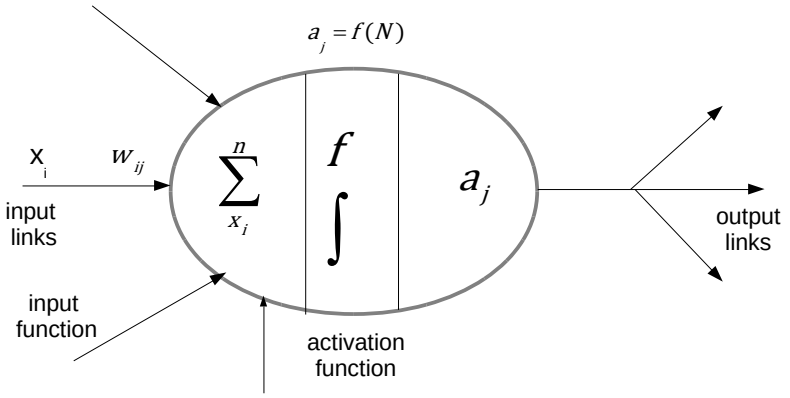


Figure 5- 3: Basic Neural Network Diagram

There are various functions that f can use, such as binary step function, linear threshold function, sigmoid function, etc. The most common is the sigmoid function which is given by

$$f(x) = \frac{1}{1+e^{-\sigma x}} = (1+e^{-\sigma x})^{-1} \qquad [5\text{-}27]$$

where σ is the steepness parameter, which is usually set to unity, i.e. σ = 1. For most practical modeling the derivative of the activation function is implemented in the learning algorithm and the sigmoid is used because of its simple derivative [208], i.e. $f'(x) = f(x)[1-f(x)]$.

Appendix D: Transfer Function

Artificial neural network (ANN) is partly dependent upon and influenced by its transfer functions. Transfer functions influence the selection of weights on the connections, which in turn are the strengths of influence of neurons. Typically, there are three (3) main categories of transfer functions:

- linear (or ramp) transfer functions – applied for linear neurons such that the output activity is linearly related to the total weighted output;
- threshold transfer functions – applied such that at a given level of total inputs the output is determined from one of two levels based on a set threshold values;
- Sigmoid transfer functions – applied such that the input – output variation is monotonically increasing or decreasing.

It is noted that the sigmoid neurons are relatively closer approximation to real world neurons than those of linear and threshold, accounting for its practical utility.

As an illustration, the ANN performs a task by first loading the network with input patterns, together with the desired output patterns (in a supervised mode). The network is tuned to endeavor to match the actual output with that of the desired output. This is repeated as the network approximately determines the desired output until the best possible match is determined.

Appendix D: Characteristics of ANN

The architecture of a neural network is characterized by the connection types of its neurons. Generally, neurons can only connect with other neurons of adjoining layers, and it can be full or partial connections. Full connections implies that all neurons from one layer interconnect with all neurons in the other layer.

Two (2) key architectures are defined by the nature of input-output mapping, be it:

- auto-associative network, whereby a set of inputs are mapped unto itself such that signals flow both ways, and inputs and outputs are not distinct. These types of networks usually have no external "training" and are often referred to as unsupervised or self-organizing networks; or
- hetero-associative network, whereby a set of outputs are produced by mapping a set of inputs, such that the outputs are either closely related (in what is known as "nearest neighbor recall") or in a similar fashion (in what is known as "interpolative recall").

Basically, neural networks learn through the weights estimation; two (2) key approaches are distinguished. Although both types solve the same sorts of problems, they do so in different ways.

- Fixed or static networks – weights do not change and remain static a priori; Static neural networks do not change their structure once they have been created and operate on a fixed number of classes.
- Adaptive or dynamic networks – weights change as the network operates and the change is deployed for solving the problem at hand [223]. Dynamic neural networks, on the other hand, can change their

structure and can operate in an environment where the number of classes is not fixed; with its learning algorithms categorized into two (2):

- *Supervised learning* – uses an "external teacher" to learn to associate each input to its corresponding and expected output. Note that, upon learning, the network is given test dataset for verification or prediction or classification. Examples of supervised learning techniques include least mean square, error-connection and reinforcement learning.
- *Unsupervised learning* – on the other hand, uses no "teacher" and its learning is based on "self-tutoring", and it is so commonly referred to as "self-organizing". Note that, here the learning and the testing (be it prediction or classification) are concurrent.

Enumerated below are some characteristics and capabilities of ANNs:

i. Non-linearity – the ability to interconnect non-linear neurons, with distribution throughout the network;
ii. Input-output mapping – the ability to learn its functions using input-output datasets or "with" a teacher, called supervised learning; and as well, learn its functions with only input dataset or "without" a teacher, called unsupervised learning;
iii. Adaptivity – ability to iteratively update weights or adapt the network parameters to the changes in the network environment to facilitate achieving the target output;
iv. Confidence – ability to make decisions with a high sense of confidence;
v. Fault tolerance – robustness in data acceptance, and the ability to perform well in spite of mis-firing, missing data or corrupted data;
vi. Generalization – ability to produce the best output when presented with a new input dataset;
vii. Parallel processing – ability to process massive data with neurons firing simultaneously.

Typical drawbacks of ANN are large amounts of data required, few analytical aids, over-fitting, non-trivial tasks can be computationally expensive, etc. ANNs usually are incorporated with other systems, since data output from the ANN ought to be reformatted into a human readable format.

Appendix -D: 5.2.1. Multi-Layer Neural Network

Most practical applications of the neural networks are usually a multilayer neural network. A basic multilayer neural network consists of at least 3 layers, as shown in figure 5-4. The first layer interacts with the system inputs and it's called the *Input Layer*, an intermediate layer (or layers), called the *Hidden Layer*; and the final layer, in a fully interconnection manner, which interacts with the output system of processed data, called the *Output Layer*.

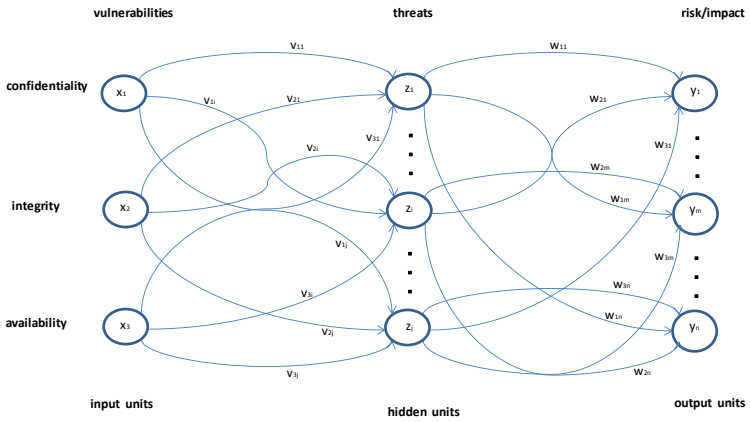


Figure 5- 4: A Schematic Multi-Layer Neural Network

Depending on the problem at hand, the number of hidden layers may be more than one. The more hidden layers there are the more complicated the network becomes.

The generic neural network operation involves the following key steps:

- loading of inputs into the system – feeding input dataset for training, usually called feed-forward;
- computation of error gradients;
- updating weights and feed-back with updated weights (back-propagation);
- adjusting learning rate;
- applying stopping controls or conditions, such as desired least squares error, desired accuracy, elapsed epochs, etc.;
- re-loading with test datasets for system verification and validation.

Appendix –D: 5.2.2. Training, Verification & Validation

As indicated earlier on, the ANN has the fundamental capability to learn or to be trained. Learning with ANN takes place through a couple of learning techniques. Typically, the techniques involve applying various learning rules and/or learning algorithms, which could be supervised or unsupervised, or a combination of the two. In practice, there may be separate learning and production phases of ANNs. Both learning and production could be concurrent in an unsupervised or self-organizing system, whereas production is carried out after learning in a supervised system.

The weights are updated during training and various methods are employed. The most widely used method is the back-propagation neural (BPN) algorithm, and that is also employed in this study.

Appendix –D: 5.2.2.1. Back-propagation Neural (BPN) Algorithm

The back-propagation neural (BPN) algorithm is the most commonly used training algorithm to determine the weights. It works by adjusting the weights of each neuron. Initially, the rate of change of activity error of neurons is computed, which is the difference between the desired output and the actual output. This is done by computing the derivative of the error on the weights. That is, slight variation or changes in error as the weights change. Consider an output neuron j, then the error is given by the difference

$$e_j(n) = d_j(n) - o_j(n) \quad [5\text{-}28]$$

where $d_j(n)$ and $o_j(n)$ are the desired output and the computed or actual output for the j[th] neuron respectfully.

Various functions are used for computing errors, but the most common is the sum of squared errors. So for a given output neuron, the error is computed as

$$E(n) = \frac{1}{2}\sum_{j \in Y} e_j^2(n) \quad [5\text{-}29]$$

where Y is the set of output neurons.

The weighted sum of errors is given by

$$E_{av}(n) = \frac{1}{N}\sum_{n=1}^{N} E(n) \quad [5\text{-}30]$$

Assuming the gradient descent rule is employed in evaluating the optimal weights with minimal cumulative error. Then, the error of neurons in the hidden layer is computed by evaluating the weights between the hidden and output layers. These weights are multiplied by the computed error (the difference calculated earlier on). This process of evaluating the weights is repeated for the input layer (or any other adjoining layer) in opposite (backward) direction from the output. Thus the name of the algorithm as Back-propagation neural algorithm. Extensive treatments are given in [212] [223] [255] [208].

It must be noted that, the error gradients at output and hidden layers are different. The error gradient of the hidden layer is given by the cumulative errors of each hidden neuron, which is computed as the product of the activation function and the weighted sum of the errors emanating from the output layer. Assuming non-linear sigmoid activation function;

$$\delta_j(n) = e_j(n) \cdot f'(W_j(n)) = e_j(n) \cdot f(W_j(n)\{1 - f(W_j(n))\} \quad [5\text{-}31]$$

Assuming m number of neurons previous output, the weights are given by

$$W_j(n) = \sum_{i=0}^{m} w_{ji}(n) \cdot o_i(n) \quad [5\text{-}32]$$

But $O_j(n) = f(W_j(n))$, now computing the derivative $\frac{\partial E(n)}{\partial w_{ji}(n)}$, with the small change $\Delta w_{ji}(n)$ applied to the weights $w_{ji}(n)$

$$\frac{\partial \mathrm{E(n)}}{\partial w_{ji}(n)} = \frac{\partial E(n)}{\partial e_j(n)} \cdot \frac{\partial e_j(n)}{\partial O_j(n)} \cdot \frac{\partial O_j(n)}{\partial W_j(n)} \cdot \frac{\partial W_j(n)}{\partial w_{ji}(n)} \quad [5\text{-}33]$$

But $\frac{\partial E(n)}{\partial e_j(n)} = e_j(n);\ \frac{\partial e_j(n)}{\partial O_j(n)} = -1;\ \frac{\partial O_j(n)}{\partial w_j(n)} = f'(W_j(n));\ \frac{\partial W_j(n)}{\partial w_{ji}(n)} = O_i(n);$

So

$$\frac{\partial E(n)}{\partial e_j(n)} = -e_j(n) \cdot f'(W_j(n)) \cdot O_j(n) \quad [5\text{-}34]$$

Now $\Delta w_{ji}(n)$ is proportional to $\frac{\partial E(n)}{\partial w_{ji}(n)}$; which is $\Delta w_{ji}(n) = -\eta \cdot \frac{\partial E(n)}{\partial w_{ji}(n)}$ implying

$\Delta w_{ji}(n) = \eta \cdot e_j(n) \cdot f'(W_j(n)) \cdot O_i(n)$, from equation [4-11]; and η is the learning rate, such that $\eta \in (0,1]$

.

This value needs to be carefully selected to provide the best results; too low and it will take ages to learn, too high and the adjustments might be too large and the accuracy will suffer as the network will constantly jump over a better solution and generally get stuck at some sub-optimal accuracy. In practice, it may be selected automatically by the algorithm (e.g. MATLAB ANFIS).

Given that the local gradient is given by $\delta_j(n) = -\frac{\partial E(n)}{\partial W_j(n)} = -\{\frac{e_j(n)}{\partial O_j(n)} \cdot \partial e_j(n) \cdot f'(W_j(n))\}$

Substituting $\frac{\partial e_j(n)}{\partial O_j(n)} = -1$, the basic local gradient becomes

$$\delta_j(n) = e_j(n) \cdot f'(W_j(n)) \quad [5\text{-}35]$$

The weights are then updated as follows: $w_{ji}(n) = w_{ji}(n) + \Delta w_{ji}(n)$; where $\Delta w_{ji}(n) = \eta \cdot \delta_j(n) \cdot O_i(n)$.

The gradient descent method is deemed to be generally slow in reaching appropriate convergence. To enhance the process a momentum is introduced. Momentum ξ is a constant such that ξ ∈ [0, 1) introduced as a factor to update the weights using the previously updated weight in computing the current weight; i.e. if the updated weight for time t is $w_{ji}(n)^t = w_{ji}(n)^t + \Delta w_{ji}(n)^t$, then at (t+1) the weight is given by

$w_{ji}(n)^{t+1} = w_{ji}(n)^{t+1} + \Delta w_{ji}(n)^{t+1} + \xi \cdot \Delta w_{ji}(n)^t$.

Generally, ANN executes an iterative process or cycle of learning, called epoch. During each epoch the system propagates a set of inputs through, whilst computing the global error. For the BPN, an epoch involves a feed-forward process of propagating the inputs through the hidden and output layers, and then a back-ward propagation of the computed error to update the weights. This iteration goes on until a global minima is achieved. The errors may be computed in a batch mode or in solo (individual) mode [208].

Appendix –D: 5.2.2.2. Validation & Verification

Validation is to ascertain that model will perform in accordance with desired performance criteria. It is the process of testing the ANN with similar dataset as that of the training dataset. Validation is generally required for any modeling for which performance assessment is desired or important.

One challenge of ANN is possible over-fitting or over-learning of the training dataset. That is, a situation in which the ANN has achieved small training error, but can't generalize on new dataset accurately. Various schemes or methods exist to perform validation in neural networks.

- Test-set Validation scheme: here, the sample set may be split into two (2) or three (3) mutually exclusive sets; such as 75% training dataset and 25% testing dataset, or into training, validation and testing datasets. The training dataset is used primarily for learning and adaptation, whilst the testing dataset is applied for verification of the model performance, accuracy and acceptance [260] [208].
- Leave-One-Out Re-sampling Scheme: given an N samples, (N-1) are used for training and are repeated for N times. Then, the one (1) sample left-out is used for testing and average test error is computed as

  $E_{test} = \frac{1}{N}\sum_{j=1}^{N} E_{test_j}(n)$, where E_{test_j} are the validation errors for the N epochs [208].
- Cross-Validation Schemes: given an N samples, all N samples are first used as training dataset, and then randomly split a number, say m, mutually exclusive subsets. The ANN is then re-trained with those batches for 'm' times. This scheme combines these m "neural networks" into a composite ANN. The performance of the composite is validated against the others as a means of verification [260] [208].

In practice, there different schemes of cross-validation, such as full cross-validation and segmented cross-validation, and they are executed automatically based on one's selection of a scheme or algorithm. For example, this study employs full cross-validation in the ANFIS modeling.

Appendix –D: 5.3. Hybrid Neural & Fuzzy Systems

The choice of methodology is usually dictated by the dataset available for the model. If the data are pairs of numbers, neural method may be most suitable, and if the data are rules, the fuzzy methods may be most suitable. Neural methods provide learning capability, whereas fuzzy methods provide flexible linguistic interpretation [55]. Integrating these two methodologies in modeling, can lead to better analysis that take advantage of the strengths of each methodology and at the same time overcome some of the limitations of the individual technique.
There are many ways in which these methods can be combined. One such possibilities is by introducing fuzzy concepts within neural networks – that is, at the levels of inputs, weights, aggregation operations, activation functions and outputs [55].
Generally, fuzzy logic can encode expert knowledge directly using rules with linguistic variables, it usually takes a lot of time to design and tune the membership functions that quantitatively represent these linguistic variables. Neural networks learning techniques can automate this process and subsequently reduce development time and cost while improving performance. This process makes it easy to interpret and explain the resulting output as a typical fuzzy system.

Appendix –D: 5.3.1. Neuro-Fuzzy Modeling

The world is full of uncertainties, the information obtained from the environment, the notions used and the data resulting from observation or measurement are, in general, vague and imprecise [29]. Thus, formal description of the real world problems or some aspects of it, is in essence, only an approximation and an idealization of the actual state.
Since it is sometimes impossible to develop a mathematical model which adequately addresses all aspects of the system, researchers may use over-simplified assumptions which may lead to inappropriate decision making [51] [52].