CYBER-SECURITY

* *Implications on SMEs in Developing Economies*
* *the case of Ghana*

By Ezer Osei Yeboah-Boateng\* & Reza Tadayoni\*\*

\*Doctoral Student at Center for Communications, Media & Information Technology (CMI), Aalborg University, Copenhagen

\*\* Associate Professor at CMI, Aalborg University, Copenhagen

Contact Author: Ezer Yeboah-Boateng: ezer@cmi.aau.dk

**Abstract**

*The objective of this paper is to analyze the security aspects of Internet service delivery to SMEs, and the policy and regulatory implications of cyber-security in the “fragmented” structural environment in a developing economy. The ubiquitous interconnectivity provides the primary conduit for exploiting vulnerabilities on a widespread basis. Small & Medium Enterprises (SMEs) sector is crucial to attaining long term and sustainable economic growth in developing economies. The ubiquitous Internet permeates every facet of human endeavor, not only to the technologically developed countries, but also increasingly prevalent in developing countries. Whereas some argue that the pace of the growth of the cyberspace should continue without governmental restrictions, others, from another perspective, argue that these interconnectivities should be actively regulated through domestic and international laws. The latter thinks that non-regulation of the cyberspace could have grave cyber-security concerns and that is likely to inhibit the current growth and development gains. This research analyzed the various policies and frameworks in respect of secured interconnectivity, adherence to governance, risk and compliance issues in a best-practice fashion. Inferential analysis reveals that there are some cyber-security implications on SMEs in a fragmented policy and regulatory environment. The findings are discussed and interpreted to provide highlights of these policy and regulatory challenges.*

# 1. Introduction

Motivation for studying cyber-security policy and regulatory implications on SMEs in developing economies was inspired by the ubiquitous interconnectivity, and the sensitive nature of data and transactions carried across these networks. The first decade of the 21st century has witnessed massive and unprecedented growth in the Information & Communications Technology (ICT) sector of the global economy, creating a virtual marketplace. This growth necessitated many reforms world-wide. To realize the full benefits of the digital revolution, users must have confidence that sensitive information is secured, commerce is not compromised, and the infrastructure is not infiltrated.

The US President’s Information Technology Advisory Committee (PITAC) posits that innovations in ICT have created a whole new industry through the “ubiquitous interconnectedness – first exhibited by the Internet.” PITAC continues that “that is indeed good news. The bad news is that ubiquitous interconnectivity provides the primary conduit for exploiting vulnerabilities on a widespread basis.” (PITAC, 2005)

This revolution of interconnectivity has also brought with it an increased potential of opportunities, including risk and uncertainties, especially for those cyber-criminals who can now cause harm with catastrophic impact from afar, while equipped “with only a computer and the knowledge needed to identify and exploit vulnerabilities.” (PITAC, 2005)

The SME sector is crucial to attaining long term and sustainable economic growth. They create employment to various sectors of the economy and are forefront in the adoption of technology. While exploitation of ICTs is critical to building the economy, a myriad of cyber-security challenges confront SMEs, which are both technological and human-centric in nature.

“Cyber-security policy needs to start from a clear and empirically grounded understanding of the nature of the problems before possible solutions can be devised.” (Bauer & van Eeten, 2009).

The ubiquitous Internet permeates every facet of human endeavor, not only to the technologically developed countries, but also increasingly prevalent in developing countries. Whereas some argue that the pace of the growth of the cyberspace should continue without governmental restrictions, others, from another perspective, argue that these interconnectivities should be actively regulated through domestic and international laws. The latter thinks that non-regulation of the cyberspace could have grave cyber-security concerns and that is likely to inhibit the current growth and development gains.

UNGA 57/239 clearly stated, “As a result of increasing interconnectivity, information systems and networks are now exposed to a growing number and a wider variety of threats and vulnerabilities which raise new security issues for all.” (UNGA, 2002) “The vulnerability created by these gaps affects not only utility services, but also databases and systems that maintain a variety of sensitive and confidential information.” (Moteleff, J. et al, 2003)

In this study we conducted a survey and followed-up with interviews of some strategic stakeholders. Existing policies were reviewed with the view to identify some cyber-security challenges confronting SMEs. Their answers were analyzed and those constitute the findings of this paper.

In this paper, we discuss the research question and methodology, followed by the review of related works in cyber-security, particularly its impact on SMEs, its policy and regulation, its implications, and stakeholder perceptions. We give an overview of the SMEs contribution to the Ghanaian economy, the market situation and the technologies used for Internet service delivery in Ghana. We then present the empirical data collected and its analysis. We conclude with a discussion of the results and offer a few recommendations on the way forward and further research work.

## 1.1 Key Issues & Hypothesis

This research sets out to investigate on the security aspects of Internet service delivery to SMEs, in particular, and its associated policy and regulatory implications in a fragmented regime.

This is premised on the fact that threats to cyber-security emanate from 2 main sources: namely, direct cyber-attacks from the cyber-criminals and the interconnected network-of-networks. “When infrastructures are interconnected, new vulnerabilities might arise from the common links, failures might propagate through the different systems, intrusion and disruption in one provoke unexpected threats to others.” (Chaturvedi, M. et al., 2009). It is this interconnection where the ICTs play a major role and that is the import of this paper.

The issue is “how are these interconnectivities regulated, some of which are cross-border originated?” Since the de-regulation of the telecom environment in Ghana, what has been the impact of cyber-security policy and regulation on SMEs? Over a decade after the de-regulation, what are the security-related challenges with internet service delivery?

Are there any impacts and inhibitions to growth of the industry due to multiple inter-connectedness and its cyber-security implications? Which stakeholders are responsible for vulnerability incidents, and how are incidents handled?

This exploratory research will test if cross-border provisioning and service provider type have any effects on cyber-security. Cross-border ICT-enabled services are said to be services provided from one country to another over the Internet, telecommunications and data networks. Here cyber-security implications refer to challenges associated with service provision, risk, protection, trust, incident handling, standards and solutions, etc. The null hypothesis is:

 H0: there are no cyber-security implications on SMEs in a fragmented policy and regulatory environment.

The alternative hypothesis is:

H1: there are cyber-security implications on SMEs in a fragmented policy and regulatory environment.

Note that, H0 and H1 are mutually exclusive.

The analysis will use the sample data collected to evaluate the null hypothesis. Using Chi-square test statistic, we find the significance level of 0.05 or the p-value of 95% probability. If the value of the test statistic is unlikely, based on the null hypothesis, we will reject the null hypothesis.

## 1.2 Methodology

In this research, we have adopted the following definitions of SMEs. Businesses with less than ten employees as a Micro Enterprise, between ten and fifty as Small Enterprises, and between fifty to two hundred and fifty employees as Medium-sized enterprises. This definition is consistent with other similar studies (Kapurubandara & Lawson, 2006) and forms the basis for selecting SMEs for the study.

We reviewed existing policies and frameworks, with the view to identify some challenges as a result of fragmentation, and also to identify cyber-security vulnerabilities confronting SMEs in Ghana. The study administered an objective-based structured questionnaire to security functionaries and chief-level (C-level) officers of 320 SMEs in Ghana. Using face-to-face surveys, we targeted ICT-based SMEs, financial organizations and government agencies, which were selected by a simple random sampling. Based on the respondents, some stakeholders were identified for further strategic level interviews. Especially, we interviewed strategic stakeholders such as the Ministry of Communications (MoC), National Communications Authority (NCA), Ghana ISPs Association (GISPA), Ghana Investment Fund for Electronic Communications (GIFEC), etc.

Their answers were analyzed and those constitute the findings in this paper. We shall test the null hypothesis by subjecting it to some sort of empirical scrutiny to determine if it is supported or refuted by the data collected from the field. It must be noted that 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.

# 2. Literature Review

## 2.1 Cyber-Security – impact on SMEs

The SME sector is crucial to attaining long term and sustainable economic growth (Ministry of Foreign Affairs, Denmark, 2009) (Baldwin, J. et al, 2001) (Lange, T. et al, 2000). ICTs have proven to be vital in improving the efficiency and expanding the market reach of SMEs as well as in establishing new ways for SMEs to obtain and make the most effective use of business information.

Literature reveals that there are “... opportunities that ICT provides for SMEs in developing countries..” (Heeks & Duncombe, 2001). (Kolodgy, C. et al, 2002) emphasized that service providers have recognized the need of SMEs to security and have created appropriate business models with security features. Some provide a full range of security solutions and technologies services. (Kolodgy, C. et al, 2002) posit that SMEs face various cyber-security challenges as a result of interconnections, which expose SMEs to hacking and other malwares. Even when SMEs procure security solutions, they are then exposed to administrative and other operational overheads.

A poorly secured network is “potentially the weakest link” in the cyber-security chain. (Anderson & Moore, 2006) (Allison & Strangwick, 2008). For example, malware in an out-of-date network can become a botnet through which other systems could be attacked. (Bauer & van Eeten, 2009) agreed with the externality effects of cyber-security. They said that ISPs are usually not proactive in identifying and removing botnets in view of the cost implications. They continued that the situation causes SMEs to under-invest. (Ogut, H et al, 2005) developed a model of interdependent risk of cyber-security breach across firms, and concluded that this interdependent risk leads to under-investment.

## 2.2 Cyber-Security Policy & Regulation

(Subramanian, 2008) emphasized that the ubiquitous Internet permeates every facet of human endeavor, not only to the technologically developed countries, but also increasingly prevalent in developing countries. Whereas some argue that the pace of the growth of the cyberspace should continue without governmental restrictions, others, from another perspective, argue that these interconnectivities should be actively regulated through domestic and international laws. The latter thinks that non-regulation of the cyberspace could have grave cyber-security concerns and that is likely to inhibit the current growth and development gains.

 “Security threats were initially viewed as mostly technological problems; in recent years, the perspective has broadened to include economic issues and aspects of user behavior” (Anderson & Moore, 2006). (Udotai, 2007) emphasized that ”a successful strategy must take into account disparate national legal systems” and fragmented policies. Interconnectivities have been mission critical infrastructure and that any disruption would grave impact on a country’s economy and national security. It is therefore pertinent that “technology alone cannot secure the critical information infrastructure” needed to ensure confidentiality, integrity and availability; actual laws, drafted for cyber-security purposes must be enacted, he concluded.

(Denning, 2003) posits that “security is never foolproof. Further, some security technologies are also employed as attack technologies. Password crackers and software tools that scan networks for vulnerabilities are good examples. While system owners use them to find and fix their own problems, their adversaries use them to find security holes, which are then exploited in an attack.”

(Thomas, 2009) posits that “cyberspace is not coterminous with national borders”. He continued that the interconnected network is a disaggregated realm where different components of the threat and its response can impact multiple networks in a borderless fashion, where regulation is still the “exception rather than the rule”.

## 2.3 Cyber-Security Implications

Virtually any element of cyberspace can be at risk, and the degree of interconnection of those elements can make it difficult to determine the extent of the security measures needed. (ITU, 2005)

(Sonnenreich, W. et al, 2006) posit that ”it’s very difficult to obtain data about the true cost of a security incident (single loss expectancy (SLE)).” Typically, companies don’t track security incidents; they focus on fixing the problem rather than assessing the incident cost. Effects of botnets are anticipated to grow as networks become more powerful and high-speed interconnectivities become inevitable. Though, newer technologies with new powerful defenses may be introduced, (Hammock, 2010) posits that, cyber-security researchers assume that the current situation is, primarily, due to adverse effects of interconnectivities. Future researches should focus on reducing uncertainties and improving on the quality of vulnerability measurement.

New threats emanate as entities get interconnected. Attacks occur within and across national boundaries; with cross-border nature of cyber-security making it difficult for stakeholders to unilaterally securitize (*ref. Copenhagen School*) emergent cyber-threats. It becomes apparently necessary for nation-states to protect their interests by working together. (Thomas, 2009) emphasizes that similar policy strategies used to foster regional integration in other sectors could be adopted for cyberspace. According to (Thomas, 2009) cross-border threats can emanate from entities, be they corporations or state agencies, against each other from any part of the world.

## 2.4 Cyber-Security – Stakeholder Perceptions

(McFadzean, E. et al, 2007) found that the “decision-makers” perception of both internal and external risks has a major impact on cyber-security. These attitudes, opinions and values have an effect on the perceivers’ actions and decision making processes (Barnett & Vaicys, 2000) (Brewer, 2002) (Frey, 2000). (McFadzean, E. et al, 2007) inferred that, “decision-makers’ perception of risk” is co-related with their roles and actions, and influences their cyber-security strategy”. Some research works indicate that perceived risk is quantifiable and predictable (Slovic, 1987) (Johnson & Tversky, 1984).

Whereas the interconnectivities promote opportunities for end-users to have socio-economic benefits, they also pose potential threats. Threats undermine user’s confidence, while security and privacy breaches threaten user’s trust. Stakeholder’s awareness and understanding of the relevance of a secure Internet infrastructure are paramount. They involve a holistic approach, which encompass legislative, regulatory, law enforcement and technological aspects. (Multi-Stakeholder Policy Dialogue)

(Farahmand, F. et al, 2008) integrated perceptions of risk, benefit, and incentives and developed a framework that aligned stakeholder perceptions of cyber-security risks.

# 3. Technology Market, and policy framework

In this chapter the technological, market and policy/regulatory framework in which the Ghanaian SMEs operate are discussed and analyzed.

## 3.1 Technology

### 3.1.1 Access Technologies

The prevailing broadband technologies in Ghana are ADSL, VSAT, Wireless Internet Services, Mobile/Cellular broadband. Optical Fiber Cable (OFC) communication is mainly employed in carrier services as such backbone or backhaul for heavy traffic over long distances, which is cost-effective than copper and microwave technologies.

Cellular companies (Celcos) are also providing broadband Internet access using their networks. Celcos use 3G networks employing technologies such as EvDo, HSDPA and UMTS. The services are delivered with Internet enabled cell phones, USB 2.0-based modems or dongles, and mobile broadband routers.

Wireless Internet Service Providers (WISPs) are popular broadband option for Internet access due in part to lack of copper or fiber. WISPs employ mainly line-of-sight (LOS) technologies, which may hamper connectivity in some areas with tall buildings, hilly and heavily foliated terrain. There are other challenges such as security, throughput, reliability due to interference from other wireless devices and weather. Cost to customers is also a challenge as most prospective customers require a pole or mast to facilitate installation.

Technologies employed here include IEEE 802.11b using 2.4 GHz (unlicensed) - transmission speed up to 11 Mbps; IEEE 802.11a using 5 GHz - transmission speed up to 54 Mbps; IEEE 802.11g using 2.4 GHz (unlicensed) - transmission speed up to 54 Mbps; IEEE 802.16d (fixed WiMAX) – license required. Others employ Multichannel Multipoint Distribution Service (MMDS) – using 2.5-2.7 GHz (license required) with 10 Mbps transmission speed per channel.



### 3.1.2 Broadband Wireless Access

The NCA is currently considering applications from interested parties for the award of 5 spectrum licenses for the Broadband Wireless Access (BWA) services in the 2.5 GHz band. There would be 3 slots of 30MHz bands for paired spectrum, and 2 slots of 2X15 MHz bands for unpaired spectrum. The tenure shall be 10 years and nationwide coverage. It is anticipated that winners of the cosmetic auctioning will deploy WiMax technologies with capabilities to offer triple-play services.

The ISP association, GISPA is liaising with some members to form synergies and consortia to bid as they mobilize resources.

### 3.1.3 E-1 (2Mbps) Fiber Service Delivery to SMEs

These services are typically carrier-to-business, whereby ISPs procured wholesale E-1 broadband services and in turn retail to the consumers. These services are relatively expensive, and are provisioned based on SLAs executed between the Telcos and the ISPs for a given period. The ISPs are guaranteed uptime, committed bandwidth, QoS and blocks of static IP addresses. In Ghana, E-1 services are symmetrical and that fractional services are not provisioned. Ghana has presently Internet feed from SAT-3, co-owned and managed by Vodafone Ghana, and MainOne Fiber cable, owned and managed by MainOne Limited. There is also national backbone fiber network owned and managed by National Communications Backbone Company (NCBC), a Vodafone Ghana subsidiary.

### 3.1.4 VSAT Cross-border Service Delivery to SMEs

Very Small Aperture Terminal (VSAT) earth satellite hubs relay broadband data from the satellite company to customers. VSAT is usually among the most expensive broadband Internet access, but certain companies use it as either the primary (or only) service or as secondary (backup) service. Marginally, costs have come down in recent times and sometimes position VSAT as a competitive option. It however, has high latency relative to other technologies and may not be suitable for some applications, including VPNs.

### 3.1.5 Security Solutions from ISPs

SMEs, as well as large corporations, connected to the Internet face risks and vulnerabilities. The cyber-security objectives of the ISPs are to prevent unauthorized access to systems and information, to protect their systems and that of customers against malwares, to meet compliance and regulatory standards, and to prevent interference with data transmission. Most ISPs have firewalls, Intrusion detection systems (IDS), and enterprise-wide anti-virus. Security solutions offered to SMEs are dependent on choices from the entities. Most SMEs opt for VPN tunneling solutions to safeguard their systems and data.

(Reece, 2007) posits that stakeholders feel safe and secured with enterprises that deliver solutions alongside ensuring the end-user’s privacy is guaranteed. He continues that effective cyber-security requires that enterprises recognize the value of stakeholder’s information and develop appropriate policies to safeguard the data.

## 3.2 Market

SMEs play key developmental roles in Ghana’s economy. They create employment to various sectors of the economy and are forefront in the adoption of technology.

According to (Fida, 2008) most large corporations have their origins from SMEs. He posits that “SMEs are different from large scale enterprises in three main aspects; uncertainty, innovation and evolution.”

“Empirical studies have shown that SMEs contribute to over 55% of GDP and over 65% of total employment in developed countries. SMEs account for over 60% of GDP and over 70% of total employment in developing countries.” (Fida, 2008)

In Ghana, available figures according to the 2003 Industrial census indicate that SMEs contribute about 67% to employment and 55% to GDP. (Industrial Statistics, 2006)

Available statistics from the Registrar General, which is collaborated from the Industrial Statistics division, Ghana Statistical Service (GSS) and the Association of Ghana Industries (AGI) indicate that SMEs constitute about 80 to 90% of all businesses. The definition used falls within the scope of this paper as a subset as the medium enterprise is pegged at 100 employees. According to (Mensah, 2004) “this target group has been identified as the catalyst for the economic growth of the country as they are a major source of income and employment.”

The following institutions facilitate business activities with a focus on SMEs: National Board for Small Scale Industries (NBSSI), Ghana Investment Promotion Council (GIPC), Association of Ghana Industries (AGI), Ghana Regional Appropriate Technology & Industrial Service (GRATIS), Private Enterprises Foundation (PEF), etc.

## 3.3 Policy and regulatory framework

### 3.3.1 Current Regime

The current regime has relied on a fragmented, but structured arrangement, which has been in place over a decade ago, and has not kept pace with major and recent developments in ICT markets. Today, almost a handful of regulatory bodies, a few independent regulatory organizations, and some governmental security agencies share responsibility for overseeing the ICT services industry. As the trend in ICT and cyber-security challenges continue to evolve, Ghana, as a developing nation and a pace-setter in sub-Saharan Africa, must rise up to the occasion.

### 3.3.2 Policy Review

Here, we reviewed and analyzed the existing regulations and policies (from 1996 through 2010) in respect of secured interconnectivity, adherence to governance, risk and compliance issues in a best-practice fashion. We related the review to some comments from the various stakeholders interviews.

Four unstructured, in-depth, face-to-face interviews were conducted with strategic stakeholders using the narrative interview technique (Bauer, 1996). The interviews lasted an average of forty-five minutes.

*Table of recent Acts & Policies of ICT in Ghana.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Policy/Act** | **Description** | **Key Purpose(s)** | **Security Implications** | **Remarks**  |
| **Act 524 (repealed by Act 769, 2008)** | The National Communications Authority (NCA) Act 1996 | To establish the NCA a regulator | Data transmission interception; electronic communications interference; data protection; safeguard the secrecy of communications; personal data protection. | No stringent regulation on cross-border providers; no regulation on technology deployment |
| **L.I. 1719** | Arrangement of NCA regulations, 2003 | To provide universal access | Privacy; secrecy of communications; | Monitoring of operators |
| **Policy 2005** | National Telecoms Policy | To provide universal access to all citizens; to provide private licensed VSAT systems & International data networks; | Customer information violations & misuse; incidents of outages; unwarranted use of customer information. |  |
| **Act 769** | NCA Act 769, 2008 | To establish the NCA as central regulator; To regulate the provision of communications services in Ghana. |  |  |
| **Act 771** | National Information Technology Act 771, 2008 | To regulate ICT provision; to ensure quality ICT provision; to promote standards of efficiency; to ensure high QoS. |  | Periodic checks on operators to ascertain QoS |
| **Act 772** | Electronics Transactions Act 772, 2008 | To remove & prevent barriers to e-communications & transactions; to give legal backing to e-commerce; to promote e-gov’t services; to develop safe, secure & efficient environment. | Interception; confidentiality, integrity & non-repudiation implied; availability (denial of service). | Data protection Act is under preparation; inclusion of issues on electronic signature, consumer protection, archival, etc. |
| **Act 775** | Electronic Communications Act 775, 2008 | To establish GIFEC fund for provisioning of UA & US. | Interceptions; confidentiality; |  |
| **Act 786** | Electronic Communications (Amendment) Act 786, 2009 | Amendment to Act 775; to provide a minimum rate for International in-coming electronic communications traffic |  |  |

### 3.3.3 Challenges of the regime

Several key challenges in cyber-security markets and products in recent times have highlighted significant limitations in the existing regulatory system. It will suffice to mention just a few.

* The (Internet Crime Compliant Center (IC3), 2009) 2008 Internet Crime report listed Ghana as amongst the top 10 perpetrator countries;
* ”Sakawa” menace (“sakawa” is a local term coined for Internet fraud where unsuspecting victims are lured into parting with monies[[1]](#footnote-1).
* Business outsourcing processing (BPO) opportunities in Ghana warrant that special attention be accorded data protection and consumer privacy issues;
* Introduction of online banking by banks warrants special attention to best practice security standards and solutions;
* Provisioning of Internet services by mobile telecoms operators, etc.

Key regulatory challenges facing SMEs are difficulties in complying with regulations, especially in a fragmented regime; inadequate funds to invest in security and necessary products; and lack of qualified security personnel.

# 4. Empirical Analysis & Results:

## **4.1 The Data**

As mentioned earlier we administered an objective-based structured questionnaire to security functionaries and chief-level (C-level) officers of 320 SMEs in Ghana. The parameters in the questionnaire were the following:

##

## The results are presented in the following table:



The variables being analyzed here are nominal categorical data, where there is no inherent order to the categories. For nominal categorical variables, the mean, median and standard deviation statistics are not meaningful. (Ho, 2006) (Heeringa, S. et al, 2010) The independent variables are the Service Provider Type and VSAT Facilities; the rest are dependent variables.

## 4.2 Description of Procedure for Data Collection

The research engaged a team of undergraduates from the University of Ghana, Legon, to administer the survey. Using face-to-face surveys, we targeted ICT-based SMEs, financial organizations and government agencies, which were selected by a simple random sampling. We solicited their views on key cyber-security related issues.

The study administered an objective-based structured questionnaire to security functionaries and chief-level (C-level) officers of 320 SMEs in Ghana. 150 respondents (46.9%) were received; of these 120 (37.5%) used Internet for business purposes and were included in the analysis. We had strategic stakeholder interviews with the Ministry of Communications (MoC), Ghana Investment Fund for Electronic Communications (GIFEC), Ghana ISPs Association (GISPA), National Communications Authority (NCA), etc.

We organized and interpreted unstructured data, resulting from the interviews. We first, grouped meaningful text segments, or created tags. Then we regrouped similar text segments or created categories. These were used in either affirming known results from the survey or used in explaining the rationale behind those results.

## 4.3 Data Limitations & Problems

The research had some challenges including ”missing” values resulting from non-responses to certain questions. There were instances when respondents had to be given a second questionnaire since the first one had been misplaced. There were other challenges associated with getting interviews with key stakeholders, especially the government sector stakeholders.

## 4.4 Empirical Results

This section outlines initial areas of action to help the stakeholders achieve a more coherent policy and regulatory framework towards secured interconnectivities. It does not present typical policy guidelines per se; instead it articulates some concerns that need to be factored into a viable policy framework for cyber-security solutions. This section structured the specific findings and options for action under five key objectives:

1. To assess the availability and use of cyber-security standards and solutions by SMEs in Ghana;
2. To estimate the extent of security breaches, its occurrences, and whether or not the breaches are reported;
3. To estimate the perception of cyber-security in Ghana by SMEs;
4. To estimate the extent of involvement of cross-border (and/or) commercial presence providers in Ghana; and
5. To assess the stakeholder responsibility for ensuring cyber-security.

## 4.5 Interpreting Results

Using statistical analysis tools (STATA & SPSS), we generated statistics, details of which are attached as tables and figures in the Appendices.

In most techno-economic researches, the probability or significance level is set at ≤ 0.05, and we have chosen 0.05. In statistical terms, we say that the observed outcome is statistically significant **if** the probability of the difference occurring by chance is less than five times out of a hundred (i.e., we conclude that something else other than chance has affected the outcome). (Ho, 2006)

The results are used in examining, explaining, confirming, refuting, and/or enriching information from the hypothesis. We herewith use empirical data to either build up our hypothesis or to reject the null hypothesis. (Casley & Kumar, 1988) noted that surveys “can be used to disprove a null hypothesis” or to indicate that the hypothesis hold true. A number of tests are available to determine if the relationship between 2 cross-tabulated variables is significant. One of the more common tests is Chi-square. Typical advantage of Chi-square is that it is appropriate for almost any kind of data.

Using the 5-key objectives, we deduct as follows:

1. Are service providers offering and/or using any cyber-security standards and solutions for SMEs in Ghana? 30.5% said their service providers adhered to security standards or best practices. Interestingly, 58.6% SMEs received security solutions from their providers.
2. What is the extent of security breaches and its occurrences? Are the breaches being reported? 54.1% SMEs either covered up incidents or never reported any breaches. 30.1% SMEs had lost data due to either viruses or network outages.
3. What is the perception of cyber-security in Ghana by SMEs? 20.5% SMEs perceived the Internet in Ghana to be secured; 24.2% indicated that their systems were protected, whereas 34.6% perceived the Internet to be risky and unsecured; 37.7% also perceived their systems and networks at risk of cyber-attacks.
4. What is the extent of involvement of cross-border providers in Ghana? 4.7% SMEs use VSAT facilities or services and 5.2% use foreign service providers. This shows that cross-border and commercial presence providers are relatively not prevalent with SMEs.
5. What is the extent of stakeholder responsibility in ensuring cyber-security? 53.9% SMEs owned up the responsibility of ensuring cyber-security to their systems; 34.4% however, were not sure which stakeholder has that responsibility.

The following sum up the rest of the results:

* 80.0% SMEs use Internet or visit the web for business purposes;
* 69.0% SMEs use the Internet daily;
* 60.4% SMEs patronizes in online transactions very often or often;
* On the factors that ensured service provider trust, 22.8% opted for SLA, 22.0% for security policy, 27.6% for track record, whilst 27.6% were unsure.

Further analysis on the cross-border and commercial presence providers revealed that, 58.3% owned up company responsibility for cyber-security; 83.3% received security solutions from their providers, only about 42% adhered to security standards or best practices.

Using chi-square statistics, the following were inferred based on 0.05 significance level:

* Factors ensuring service provider trust had a significance of 0.708 or 29.2% probability as being true or not due to chance;
* Loss of data due to viruses or network outage had a significance of 0.095 or 90.5% probability as being true or not due to chance;
* Cyber-security solutions from the providers had a significance of 0.052 or 94.8% probability as being true or not due to chance;
* All other variables had significance within the range of 0.000 and 0.004.

# 5. Conclusion & Discussion:

Generally, this research is an attempt to address one or more of the following issues with a given segment of the business population in Ghana:

* Are there cyber-security implications on SMEs in developing economies in a fragmented policy and regulatory environment?
* How are these interconnectivities regulated, some of which are cross-border originated?
* What has been the impact of cyber-security policy and regulation on SMEs?
* What are the challenges of Internet service delivery on SMEs in respect of security, governance, risk and compliance?
* What are the enablers and inhibitors to growth of the industry due to multiple interconnectedness and its cyber-security implications?

In view of the broad scope of cyber-security policy and regulation, drawing general conclusions may be inappropriate. Nevertheless, we shall comment briefly on some specific features of the research which are quite striking.

Cross-border and commercial presence providers constitute about 5% of the SMEs we surveyed. Security standards and best practices are not adhered to; security solutions are not adequate; internet and systems protection are not adequate; averagely, about 35% SMEs perceived Internet service delivery in Ghana as risky, unsecured and vulnerable to cyber attacks.

We can infer that governance, risk and compliance issues require the policy-makers urgent attention. Obviously, there are some cyber-security implications on SMEs as a result of fragmented policy and regulation. These may not have been necessitated by the cross-border and commercial presence providers. We therefore reject the null hypothesis and deduce that there are *some* cyber-security implications on SMEs in a fragmented policy and regulatory environment of a developing economy.

Though, this study was from academic research perspective, the lessons drawn could assist policy-makers weigh various regulatory reform proposals vis-a-vis cyber-security trends, and consider ways in which the current regulatory regime could be optimized.

We commend the on-going policy initiatives on data protection, but would advice the incorporation of explicit clauses to address the totality of cyber-security dimensions as per the ITU-T Recommendation X.805. We also recommend the establishment of CERT to cater for cyber-disaster preparedness and recovery programs. In essence policy makers should endeavor to consolidate existing policies or frameworks in favor of a coherent policy that would explicitly address cyber-security vulnerabilities with SMEs in mind, and to position the SMEs to compete in the cyber-market. There is also the need to appropriately manage the “cross-border” and “commercial presence” providers to ensure adequacy of cyber-security solutions, implementations and compliance.

We recommend that stakeholders be incentivized to report incidents, and to invest in cyber-security solutions. We also recommend that policy makers should examine in detail the impacts and inhibitions to growth due to multiple inter-connectedness and its cyber-security implications. Obviously, this calls for further research work into examining the impact of cyber-security vulnerabilities with SMEs.

Since cyber-security threats are no longer perceived as mainly technological in nature, but also human centric, awareness programs and dissemination of knowledge on user behavior could be beneficial to SMEs. Finally, arguably cyber-security could be perceived as “public good”, and from that perspective, governments should provide leadership, with public-private-partnerships being forged.

# 6. References

Allison & Strangwick. (2008). Privacy Through Security, Policy & Practice in an SME. In R. Subramanian, *Computer Security, Privacy & Politics: Current Issues, Challenges & Solutions.* IRM Press.

Anderson & Moore. (2006). Information Security Economics - and Beyond. *Science* , 610-613.

Baldwin, J. et al. (2002). *The Trend to Smaller producers in Manufacturing in Canada & US.* Center for Economic Studies, US Census Bureau.

Barnett & Vaicys. (2000). The moderating effect of individual's perceptions of ethical work climate on ethical judgments & behavoral intentions. *27* (4), 317-362.

Bauer & van Eeten. (2009). Cyber-security: Stakeholders incentives, externalities & policy options.

Bauer, M. (1996). The Narrative Interview - comments on a technique for qualitative data collection. *London School of Economics & Politics* .

Brewer, B. (2002). *Perception & Reason.* Oxford University Press.

Casley & Kumar. (1988). *The Collection, Analysis & use of Monitoring & Evaluation Data.* Oxford.

Chaturvedi, M.M. et al. (2009). *Cyber Security Infrastructure in India: A Study.* Delhi: Indian Institute of Technology.

Denning, D. (2003). Cyber-Security as an Emergent Infrastructure. In R. Latham, *Bombs & Bandwidth: The Emerging Relationship between IT & Security.* The New Press.

Farahmand, F. et al. (2008). Incentives & Perceptions of Information Security Risks. *Twenty Ninth International Conference on Information systsems.* Paris.

Fida, B. A. (2008). The Importance of SMEs in Economic Development. Banking, Finance & Accounting Community.

Frey, B. (2000). The Impact of Moral Intensity on Decision Making in a business context. *26* (3), 181-195.

Hammock, M. (2010, June). A Review of the Economics of Information Security Literature. *Social Sciences Research Network (SSRN)* .

Heeks & Duncombe. (2001). *Technology Planning in ICT: A Handbook for Enterprenuers in Developing Countries.* University of Manchester, UK.

Heeringa, S. et al. (2010). *Applied Survey Data Analysis.* CRC Press, Taylor & Francis Group.

Ho, R. (2006). *Handbook on Univariate & Multivariate Data Analysis & Interpretation with SPSS.* CRC, Taylor & Francis Group.

Industrial Statistics. (2006). *National Industrial Census, 2003.* Ghana Statistical Service (GSS).

Internet Crime Compliant Center (IC3). (2009). *2008 Internet Crime Report.* Bureau of Justice Assistance.

ITU. (2005). *A Comparative Analysis of Cyber-security Initiatives Worldwide.* International Telecommunications Union (ITU).

Johnson & Tversky. (1984). Representations of Perceptions of Risk. *Experimental Pschology* , 55-70.

Kapurubandara & Lawson. (2006). Barriers Adopting ICT & e-Commerce with SMEs in Developing Countries: An Exploratory Study on Sri Lanka. CollECTeR '06.

Kolodgy, C. et al. (2002). *Meeting the Grwoing Security Needs of Small & Medium sized Enterprises: SME Security Solutions.* IDC.

Lange, T. et al. (2000). SMEs & Barriers to Skills Development: A Scottish Perspective. *24* (1), 5-11.

McFadzean, E. et al. (2007). Perception of Risk & the Strategic Impact of existing IT on Information Security Strategy at the Board level. *31* (5), 622-660.

Mensah, S. (2004). A Review of SME Financing Schemes in Ghana. UNIDO Regional Workshop of Financing Small & Medium Scale Enterprises.

Moteleff, J. et al. (2003). *Critical Infrastructures: what makes an infrastructure critical?* US Congressional Research.

*Multi-Stakeholder Policy Dialogue*. (n.d.). Retrieved 2010, from www.intgovforum.org

Ogut, H et al. (2005). Cyber Insyrance & IT Security Investment: Impact of Interdependent Risk. *4th Workshop on the Economics of Economics Security.*

PITAC. (2005). *Cyber-Security: A Crisis of Prioritization.* National Coordination Office for Information Technology Research & Development.

Reece, J. (2007). *Forget About Security & Privacy: Focus on Trust.* Retrieved June 2010, from CIO: www.cio.com/article/112051/

Slovic, P. (1987). Perceptions of Risk. *Science* *, 236*, 280-285.

Sonnenreich, W. et al. (2006, February). Return on Security Investment (ROSI) - A Practical Quantitative Model. *38* (1).

Subramanian, R. (2008). *Computer Security, Privacy & Politics.* Hershey, New York: IRM Press.

Thomas, N. (2009). Cyber Security in East Asia: Governing Anarchy. *Asian Security* *, 5* (1), 3-23.

Udotai, B. (2007). Framework for Cyber-security in Nigeria. Directorate of Cyber-security.

UNGA. (2002). *GA 57/239, Creation of a Global Culture of Cyber Security.*

# I. Appendices

## I.1 Tables & figures

### I.1.1 Variable description

###

### I.1.2 Histogram











## I.2 Chi-Square Test RESULTS

|  |
| --- |
| **Test Statistics** |
|  | Internet Usage | Frequency of Internet Usage | Type of Service Providers | VSAT Facilities | Online Transactions |
| Chi-Square | 54.000a | 74.977b | 222.552c | 106.116d | 90.701e |
| Df | 1 | 2 | 2 | 1 | 4 |
| Asymp. Sig. | .000 | .000 | .000 | .000 | .000 |
| a. 0 cells (.0%) have expected frequencies less than 5. The minimum expected cell frequency is 75.0. b. 0 cells (.0%) have expected frequencies less than 5. The minimum expected cell frequency is 43.0. c. 0 cells (.0%) have expected frequencies less than 5. The minimum expected cell frequency is 44.7. d. 0 cells (.0%) have expected frequencies less than 5. The minimum expected cell frequency is 64.5. e. 0 cells (.0%) have expected frequencies less than 5. The minimum expected cell frequency is 26.8. |
| **Test Statistics** |
|  | Security Standards | Security Solutions | Internet Protection | Cyber Risk | Data Losses |
| Chi-Square | 114.588f | 3.781g | 14.232h | 68.377i | 4.707j |
| Df | 3 | 1 | 2 | 2 | 2 |
| Asymp. Sig. | .000 | .052 | .001 | .000 | .095 |
| f. 0 cells (.0%) have expected frequencies less than 5. The minimum expected cell frequency is 32.8. g. 0 cells (.0%) have expected frequencies less than 5. The minimum expected cell frequency is 64.0. h. 0 cells (.0%) have expected frequencies less than 5. The minimum expected cell frequency is 31.7. i. 0 cells (.0%) have expected frequencies less than 5. The minimum expected cell frequency is 40.7. j. 0 cells (.0%) have expected frequencies less than 5. The minimum expected cell frequency is 44.3. |
| **Test Statistics** |
|  | Incidents Handling | Stakeholder Responsibility | Service Provider Trust | Service Provider Trust | Risk Perception |
| Chi-Square | 11.099k | 137.078l | 1.390m | 9.765n | 11.449o |
| Df | 2 | 4 | 3 | 4 | 2 |
| Asymp. Sig. | .004 | .000 | .708 | .045 | .003 |
| k. 0 cells (.0%) have expected frequencies less than 5. The minimum expected cell frequency is 43.7. l. 0 cells (.0%) have expected frequencies less than 5. The minimum expected cell frequency is 25.6. m. 0 cells (.0%) have expected frequencies less than 5. The minimum expected cell frequency is 30.8. n. 5 cells (100.0%) have expected frequencies less than 5. The minimum expected cell frequency is 3.4. o. 0 cells (.0%) have expected frequencies less than 5. The minimum expected cell frequency is 42.3. |

1. Ref: [www.theghanaianjournal.com/2009/05/04/the-sakawa-menace](http://www.theghanaianjournal.com/2009/05/04/the-sakawa-menace) [↑](#footnote-ref-1)