Aalborg Universitet

AALBORG UNIVERSITY
DENMARK

Of Social Engineers & Corporate Espionage Agents

How Prepared Are SMEs in Developing Economies?

Yeboah-Boateng, Ezer Osei

Published in:
Journal of Electronics & Communications Engineering Research

Publication date:
2013

Document Version
Early version, also known as pre-print

Link to publication from Aalborg University

Citation for published version (APA):
Yeboah-Boateng, E. O. (2013). Of Social Engineers & Corporate Espionage Agents: How Prepared Are SMEs in Developing Economies? *Journal of Electronics & Communications Engineering Research*, *1*(3), 14-22. [2]. http://www.questjournals.org/jecer/papers/vol1-issue3/B131422.pdf

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

? Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
? You may not further distribute the material or use it for any profit-making activity or commercial gain
? You may freely distribute the URL identifying the publication in the public portal ?

Take down policy
If you believe that this document breaches copyright please contact us at vbn@aub.aau.dk providing details, and we will remove access to the work immediately and investigate your claim.

Downloaded from vbn.aau.dk on: December 04, 2020

Quest Journals
Journal of Electronics and Communication Engineering Research
ISSN:2321-5941 Volume1 ~ Issue 3 (2013) pp: 14-22
www.questjournals.org

Research Paper

Of Social Engineers & Corporate Espionage Agents: How Prepare Are SMEs in Developing Economies?

Ezer Osei Yeboah-Boateng, Ph.D.[1]

Received 18 November, 2013; **A**ccepted 02 December, 2013© The author(s) 2013. **P**ublished with open access at **www.questjournals.org**

ABSTRACT: *The purpose of this study is to create the awareness of cyber-security threats due to social engineers and corporate espionage agents, and to offer some mitigation measures aimed at minimizing the impact of insider attacks on SMEs in developing economies. Loyal and trusted employees can pose enormous and catastrophic cyber-risks to SMEs, in view of their insider-ness, access privileges and knowledge of the systems as well as associated inherent vulnerabilities. Cyber-security functionaries and chief-level officers were surveyed on various metrics of insider attacks and incidents. The findings indicate that financial and ICT oriented SMEs are mostly targeted, and the impact range from loss of sensitive data, loss of corporate resources, loss of market share as well as loss of customer and investor confidence. Since most social engineers capitalize on the end-user vulnerabilities and their sense of social norms, effective mitigation measures offered are human centric in nature. Personal and corporate factors that are likely to motivate employees to become espionage agents ought to be addressed. Periodic and on-spot systems audit are to be carried out to effectively monitor any unnecessary and inappropriate access escalations. Policy on separation of duties must be enforced.*

Keywords *-Social engineering, corporate espionage agents, threats, vulnerabilities, SMEs, Developing Economies.*

I. INTRODUCTION

Many more Small-to-medium-sized enterprises (SMEs) today utilize information and communications technologies (ICTs) opportunities as vital business tools. ICT as an enabler is used to create innovative business operations, user-friendly products and services, as well as customer-centric strategies [1].

Unfortunately, a myriad of challenges threaten the survivability of SMEs, especially those in the developing economies and emerging economies. Numerous threat agents attack SMEs systems and networks. Upon successful attacks or intrusions, most SMEs loose revenues, customer and investor confidence, resources, as well as credibility[1].

The above notwithstanding, SMEs are saddled with costs such as those related to the security breaches, including lawsuits, costs of mitigation measures, and even the possibility of business closure.

With advancements in technologies, computers have become more powerful and complex than the very early von Neuman computers. SMEs have become more reliant on computers and the Internet for storage and processing of valuable data. At the same time, end-users remain unsophisticated; the average user remains the weakest link in the cyber-security chain. End-users indiscriminately install pirated software and visit questionable websites, even though it violates corporate Internet Acceptable Use policy. Mallery[2] strongly advocates for stringent measures in addressing the threats associated with untrained and unwary end-users.

Cyber-security is actually a business concern and not really a technological problem as perceived by most business managers and even IT administrators. It is more of a people issue than it is technical. For example, insiders are perceived to be more detrimental to the business than the traditional external intruder.

An insider is defined as an individual or entity with authorized credentials or access to the organizational resources. The entity is perceived or presumed to be trustworthy. However, this assumed responsibility is usually abused when the entity violates any of the security properties, either intentionally or inadvertently. The insider threats are numerous. For example, employees may exploit any lapses or weaknesses in the organization to doctor the payroll; or may assume or assign themselves with privileged access to critical, sensitive or confidential information or systems. A number of insider threats include espionage, sabotage,

*Corresponding Author: Dr. Ezer Osei Yeboah-Boateng
EZi Technologies, Accra, Ghana

terrorism, etc. [3]. The insider threats may take the form of illicit communications, fraud, access to confidential information and systems, etc.

Some key or pertinent questions begging for redress are as follows:

- Do SMEs know who their corporate enemies (or even "frienemies") are?
- To what extent would insider threats affect SMEs business, if unauthorized entities got their data sheets or pricing strategy?
- What are the characteristics of SMEs insiders in developing economies?
- To what extent do employees take corporate assets home without express permissions? (-It places corporate assets at risk; do employees use public access venues (PAVs) and are they governed by any policies?

Basically, information is said to have a price tag. This informationvalue is ascertained through cyber-security asset classification. For instance, in business typical classifications include public, sensitive, private or confidential. Whereas, in governments, information is labelled as unclassified, restricted, confidential, secret or top secret[1].

The problem of insider threat has been with us since the inception of computer usage and insider threat is estimated to be posed by about 95% of legitimate (authorized) users [4][5][6]. The goal is to create awareness of the enormity of insider threat to SMEs and offer some proactive measures to deal with them.

Fundamentally, there are 3 types of insider attacks, namely misuse of access privileges, bypass of defence mechanisms, and malfunctioning of access control[7].Misuse of access privilege is a bit difficult to detect. Here, legitimate end-users with permissible access to the systems may use the privilege for nefarious activities. For instance, a switching engineer at the telephone switching could set a customer's account to non-billable status as he could for a maintenance line. Or, for a Marketing Executive with an ISP who declares a customer bill as part of protocol accounts. It's almost impossible to prevent or detect such actions with only technological measures. It may be feasible to monitor and audit unusual processes and query abnormal occurrences.

Every organization needs to deal with a number of categories of securityincident.These can vary considerably in their nature and impact on the organization.Typically, insiders may be involved in the full range of computermisuse activities, including:

- Viewing and transmitting pornography;
- Fraudulent use of computers; and
- Information theft.

Because of the legal implications relating to security incidents, evidence gathering, preservation, and representation are paramount. Since investigating insider incidents requires specialist skills to carry it out, often the SMEs rely on external agencies to perform the bulk of these investigations. However, expert knowledge is still required, to ensure that system administrator knows when to call on the supplier ofcomputer forensic skills and to ensure that evidence is preserved until that point[8].

Generally, the findings have indicated that SMEs are not really up-to-speed with insider attacks and most hardly affected sectors are the financial and ICT-related firms.

This paper is structured as follows: this introductory section deals with the motivation and problem formulation as well as the highlights of the key findings; the succeeding section deals with related works and state-of-the-art on social engineering, corporate espionage and risk impact on SMEs, with special emphasis on developing economies. The following section deals with the research approach and methodology; the succeeding section presents and analyzes the results of this research. The last section discusses the implications of the findings and draws conclusions.

II. LITERATURE REVIEW

Any business must endeavor to understand that building a secure organization is paramount to sustainable success. SMEs may use their security posture as a marketing tool, by demonstrating to clients that they value their custom so much that they take a very aggressive stance on protecting their information.

2.1. The Insider

There is no uniform definition for an insider and insider threats. However, certain characteristics seem to

*Corresponding Author: Dr. Ezer Osei Yeboah-Boateng
EZi Technologies, Accra, Ghana

emanate from all the definitions and propositions. Key amongst them are trustworthiness, accessibility and capability.

- Accessibility – here, legitimate access is granted to an employee who subsequently can abuse the trusted privilege. It could also be that the level of access entrusted to the entity is unlawfully elevated for nefarious acts and/or motives that are detrimental to the health of the SMEs.
- Trustworthy – here, as alluded to earlier, the so-called trusted insider is usually privy to certain information assets and may take advantage of some susceptibilities within the systems or the organization to violate the security properties. For example, an associate at the finance department may decide to alter payroll records or change some figures on a voucher when preparing a check for signature.
- Capability – this metric is captured in the fuzzy function of threat as espoused by [1]. The skillset of the attacker greatly impact on the extent and severity of damage caused by that exploit. For instance, a script kiddie and a professional hacker would definitely operate at different levels and achieve different impacts.

Indeed, the insider threats are any acts or events, whether real or potential, that adversely impact on the business operations or that violate any of the security properties, by exploiting any perceived or inherent vulnerabilities in the system design or operations or configurations, by way of unauthorized disclosure, unauthorized modification or alteration, and unauthorized interruption or interception.

2.1.1. Impact of Insider Threats

To start off, the literature on the impact of insider threats are presumed to be conservative, due to the negative impact of publicity or corporate reputational damage upon reporting of an insider incident. Estimation of the impact due to insider actions, is no different from other risk related incidences. They are usually estimated by probability and likelihood constructs in an overly binary manner [1]. But, a more thorough assessment can be made using intuitive and fuzzy qualitative approaches as in [1][9]. That assessment accounts for the attractiveness of the asset in question (i.e. asset value), the motivations of the insider, and the capabilities of the insider, utilized in taking advantage of an opportune situation or lapses.

Business today relies on computer applications and network systems to stay competitive. Any downtime resulting from compromises of any security property are seen as cost elements. So any measures aimed at ensuring availability and maintaining effective security properties, are seen as enhancing business operations.

2.2. Types of Social Engineering

Social engineering is the art of tricking or luring or manipulating end-users to reveal his password or to divulge other valuable corporate information by appealing to their sense of social norms, with the aim of gaining access to one's system [10]. This includes the art of gaining access to buildings, systems or data by exploiting human psychology, rather than breaking into or using technical hacking techniques.

Typically, a social engineer may call an employee and pose as an IT support person, and trick the employee into divulging his password, or authentication credentials or sensitive information. This threat agent exploits the vulnerability of end-users, e.g. Receptionists, to solicit access credentials. The social engineer exploits and leverages on pre-existing trust relationship amongst a victim and the assumed entity, to lure the victim to take some detrimental actions [11]. Some examples of social engineering or information gathered via telephone calls purporting to be a system administrator, or a consultant or a visitor asking to use a corporate computer, etc.

There are many forms of social engineering. One of the commonest and effective is phishing. Phishing is the means by which a victim is lured into revealing information based on the human tendency to believe in the security of a brand name because they associate the brand with trustworthiness. Corporate espionage agents or corporate spies are usually insiders such as employees, ex-employees, vendors, consultants, or contractors. Though the definition of who an insider is, is very fuzzy, relative to a resource, leading to what is known as "insider-ness" [12][13].

The corporate espionage agents are usually entities with legitimate access to corporate resources, whether wholly or partially trusted entity. Any system user or entity who has or had access to the corporate resources could turn out to be a corporate espionage agent. In view of their trusted position, they may misuse the assigned privileges or they might attempt authorized removal or deletion or sabotageof critical assets, or they could assist outsiders (that is those who do not have authorized access to some resources) in doing so. It doesn't matter whether the employee assisted intentionally or inadvertently.

*Corresponding Author: Dr. Ezer Osei Yeboah-Boateng

EZi Technologies, Accra, Ghana

2.2.1. Characteristics of Corporate Espionage Agents:

Corporate spies are characterized as being elusive, adept, and often seeking to have technological advantage and not adventure[12]. They are serious minded entities who are professional and use stealthy and superior skill set to execute their trades. They are capable of concealing the evidence of their activities, often go undetected. The motives may vary from dishonesty to disgruntled insiders, who may seek to steal, to destroy corporate sensitive data, or commit fraud, or revengefully disrupt corporate networks and /or operations[4].

Insider threats – though not well defined; they are characterized as malevolent, already trusted entity with access, privilege knowledge of systems and networks. An insider could be anyone who has the corporate "power of attorney" to act for and on behalf of the organization. "An insider is a person that has been legitimately empowered with the right to access, represent, or decide on one or more assets of the organization's structure" [14]. Boyle & Panko [12] posit that this definition enforces the notion of "insider-ness". Insiders account for a third of the computer security loss (even though, scanty data exist for which there's no consistency). Insider – an employee or member of a host institution that operates a computer system to which the insider has legitimate access, has a formal or informal business relationship; authorized to perform certain activities; - may be any properly identified and authenticated entity, e.g. Masqueraders, former insiders, using previously conferred access credentials. The question is how often do SMEs change access passwords to critical systems? Is it {once a month, every quarter, half yearly, yearly, seldom (more than a year)}. For example, most SMEs, and even some large corporations, keep the same access password to their networks for years, in spite of high employee churn rate.

Factors or motivations of carrying out corporate espionage are: - aim or intention or reason for misuse or abuse; - level of technical expertise; - system consequences of threats; - misuse of access privilege; etc.

2.2.2. Impact on SMEs:

Pfleeger[15] posited that the level of impact of insider attacks may be either positive or negative. He cites cases of intruding one's network and making it available or accessible to underserved communities or under-privileged society, as positive impact. Obviously, it is positive as far as digital inclusion of that society is concerned, or bridging the access gap of those otherwise marginalized communities. Here, it becomes a moral or ethical issue, and this is outside the scope of this paper. Even though this author is also an advocate for digital inclusion, especially to the underserved and disadvantaged in society, using unethical means to achieve "good' ends is still unethical. Pfleeger[15] continues that an insider attack purported to obtain one's data for fraudulent purposes has a negative impact.

Insider activities can significantly result in losses such as revenues, intellectual property, and corporate reputation – if the firm fails to prevent, detect and investigate insider threats[14]. Insider activities include disruption of international network operations, corruption of databases and file servers, denial of service (DoS) of resources, etc. Mills et al [14] assert that colossal amounts of dollars could be lost to stolen, lost or deleted or corrupted information, by a click of a button, whether it was intentional or inadvertent. For example, a disgruntled employee deleted files valued at US$2, 5 million[16].

SMEs have people or end-users who are called the insiders – and represent potential threats to the SMEs due to their access or trusted status or authorized authentication privileges. Insider's actions constitute some "observable" which when appropriately monitored in accordance with laid down policies can mitigate against some risks.

Mills et al [14] posit that the risk to any firm's resources can be evaluated as a function of the threats to the resource, the vulnerabilities present in the resource or its environment, and the likelihood that the threats will exploit the vulnerabilities. "To mitigate the insider threat risk (or a subset of those risks that have been deemed more critical), the organization should employ a risk management process that explicitly identifies those risks (e.g. risk assessment), evaluates cost-benefit trade-offs in selecting controls which mitigate the risk to an acceptable level (e.g. risk mitigation) and periodically reviews to assure that any changes within the organization which significantly change the organization's risk profile are accounted for in a timely and efficient manner (e.g. evaluation and assessment)[14].

Mitigation measures are aimed at managing risks to an acceptable level, usually through a combination ofprevention, deterrence, detection and response [14]. Wiles [17] posits that social engineering is the "most effective and dangerous threat to any security plan". In social engineering, the social engineer or skilled con-man capitalizes on the normal human nature of wanting to help, to empathize, to be kind, and deems that as a security weakness or vulnerability which is often exploited. Here, the untrained and unaware human nature is deemed high susceptibility.

2.3. SMEs in Developing Economies

Small and medium-sized enterprises (SMEs) consist of varied businesses usually operating in the service, trade, agribusiness, 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 usually classified by the number of employees, by annual revenue and/or by the value of their assets [1].

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)[18]. 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 [19] 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.

SMEs in developing economies are characterized by low and uncertain revenues[20]. Information systems projects in developing economies are characterized by socioeconomic changes or transformations, as they seek knowledge and skill set to the SMEs. Walsham&Sahay[21] examined various literatures in information systems research in developing economies, and underscored their relevance. The emergence of Internet facilities in developing economies has impacted positively on societies and organizations, especially in areas of connection costs, access speeds and end-users utilization [22].

Ellefsen& von Solms[22] 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 [22].

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 [23].

ITU-T [24] 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.

III. METHODOLOGY

This study comprises ofa couple of distinct investigations on cyber-security vulnerabilities, evaluating a number of issues with SMEs in developing economies.

The primary research is a part of a more comprehensive cyber-security vulnerabilities study which took into consideration the difficulties as well asconcerns in cyber-security measurements, and therefore, conducted extensive assessment to develop a suitable questionnaire to gather data[25][26]. An Online survey facility was used to administer the questionnaire and to reach out to the target population, which were chief level officers and ICT functionaries of SMEs in Ghana and Nigeria. To guarantee reputable outcomes, a cookie was setup to avoidrepetitiveparticipation [25].

Email messages with a preamble on the objectives of the study, including confidentiality of responses, and a link to the online survey portal, where the survey was administered and processed. Overall, about 500 SMEs were targeted and only 89 valid responses are used for the analysis.

The second survey was a brief expert opinions elicitation of chief officers and ICT operatives, who had gathered for a day's seminar on various ICT related issues confronting SMEs in developing economies. Here, 154 samples were asked to assess the impact of social engineering, corporate espionage activities and cyber-security incidents on their businesses; 93 responses were received which are used as the basis of analysis of the impact on SMEs as presented in the results section.

*Corresponding Author: Dr. Ezer Osei Yeboah-Boateng
EZi Technologies, Accra, Ghana

IV. RESULTS & ANALYSIS

This section presents the results and findings of the impact of social engineering and corporate espionage attacks on SMEs in developing economies.

4.1. Results & Analysis

Enumerated below are some findings from the study:

- For losses attributable to cyber-security incidences within one particular year, it was found out that 76.4% SMEs had lost at least 1000 US$, whilst over 92% had lost around US$ 10000, as shown in Fig. 1;
- Unauthorized access or intrusions – 84.3% SMEs indicated that there had been about 10 unauthorized accesses per year, whilst about 95% had around 100 intrusions per year, as shown in Fig. 2.
- The profile of the ICT functionaries and C-level officers who responded to the survey are as follows:
  - About 35.7% were senior managers or chief officers, with 64.3% having earned graduate degrees and, 42.8% had also worked within the ICT sector for over 10 years.

It is worthy to note that, the losses due to security incidents are conservation figures as most businesses do not want to report of such incidents in view of various repercussions and reputational damage.

The succeeding sections discuss the findings as they address the research questions of the study.

Do SMEs know who their frienemies are? The term "frienemies", sometimes spelt "frenemies", refer to purported friends who act as enemies. It's definition based on actions or effects of commission or omission, reflect on the insiders or corporate espionage agents. From the study, it is obvious that most SMEs are not aware that employees could turn out to become spies for their competition. Their actions may be construed as inadvertent, but most of them are likely to be deliberate with nefarious motives. They may break into SMEs systems or decrypt password, or may access resources without proper authorization. They often exploit the vulnerabilities in the organization. For instance, an employee may copy or carrycorporate confidential information without due process of permission.

The erroneous notions of hackers looking for secrets, or "there's nothing attractive about one's network", have to be discarded. On the contrary, hackers like insiders, take advantage of unprotected systems and may hack into systems for various reasons, including using infected systems as launch pads to attack others, gaining access to financial information, intellectual property, or corporate sensitive information, etc. [10].

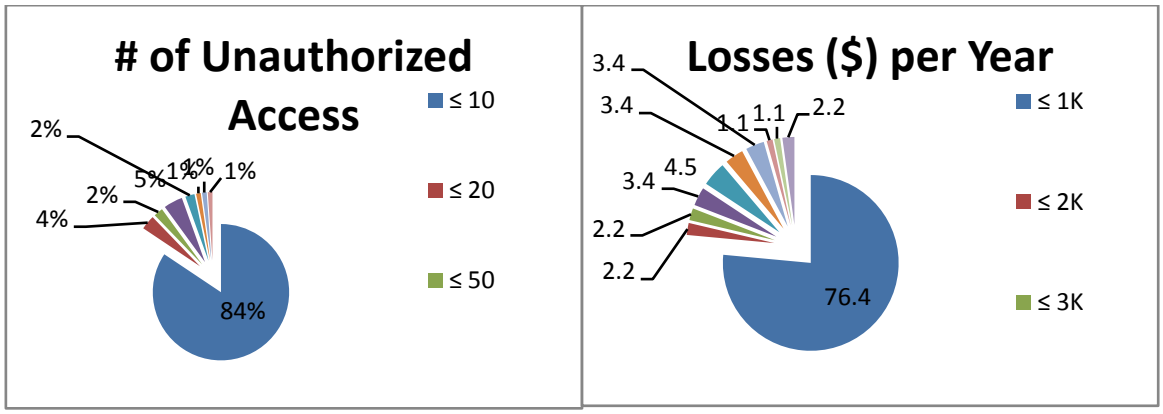
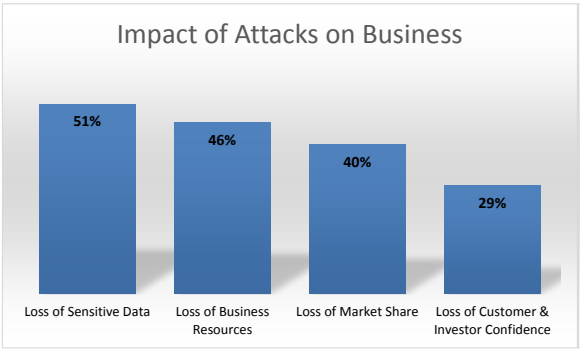


Figure 1: Number of Unauthorized Access per YearFigure 2: Losses ($) per Year

To what extent would insider threats affect SMEs business? Fig. 3 depicts the various impacts resulting from a number of insider attacks accounting for 51% loss of sensitive corporate data, 46% loss of business resources, and losses affecting customer and investor confidence. According to [27], 80% of companies surveyed admitted that they have encountered financial losses due to Internet security violations. The monetary value was estimated at US$450 million.

Similarly, they posit that cyber-attacks could make customers hesitate, doubt or worry about doing business online with the victim company. To the SMEs, that would be considerable revenue stream lost.

*Corresponding Author: Dr. Ezer Osei Yeboah-Boateng
EZi Technologies, Accra, Ghana



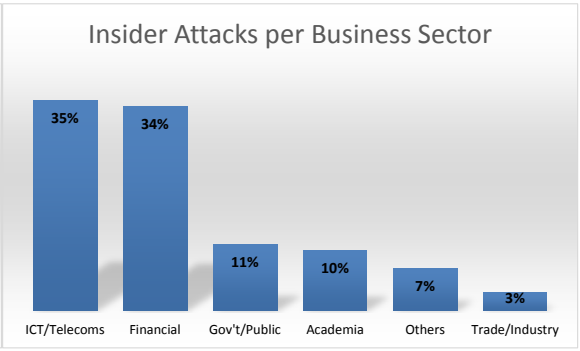


Figure 3: Impact of Attacks on BusinessesFigure 4: Insider Attacks per Business Sector

Figure 4 depicts the various sectors of business which were most impacted by insider attacks. Here, the sectors with high attacks are also deemed to have very attractive assets and of high vulnerabilities.

- ICT & Telecoms – accounts for 35% of insider attacks. This is probably expected as they have the high number of information systems and technology expertise. They often know how to suppress and possibly delete the audit trails.
- Financial sector followed closely with 34%; also not unexpected, as the sector has lots of valuables including monies that are often the key motivation for almost all nefarious espionage activities.
- Government and public sector recorded 11% of insider attacks.
- Academia – included educational institutions and research centers and accounted for 10%. Here expectation is that most of their insider attacks could be initiated by curious students who probably want to practice their skills from computer and information security lessons. It is also not uncommon for some students to attempt to hack into the school's administrative network to change their grades.
- Others – here included accountants (2.2%), lawyers (1.8%), consultants and other professionals; accounting for a total of 7% attacks.
- Trade and industry, including manufacturing accounted for only 3% attacks. This category has businesses that often using semi-automated equipment and have fewer systems connected online.

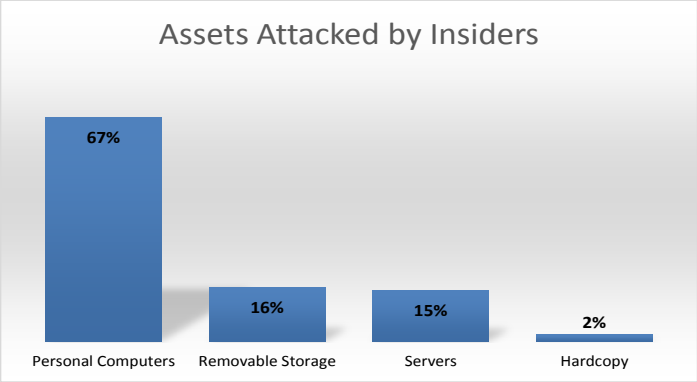


Figure 5: Assets Attacked by Insiders

Figure 5 depicts the assets that are often attacked by insiders. Here, the assets are categorized into four main groups, as follows:

- Personal computers (PCs) – include PCs, laptops, handheld devices, mobiles, PDAs and smartphones. Attacks accounted for a colossal 67% of all insiders targets.
- Removable storage – include any portable storage devices, pen drives, external hard disks, zip cartridges, etc., accounting for 16%.

- Servers – include access points, routers, servers such as network address translation (NAT), domain name service (DNS), Web, database (DB), active directory, etc., accounting for 15%.
- Hardcopy – include any printed matter or documents, which accounted for only 2%.

Saini et al [28] categorized insider attacks as follows:

- Data attacks – these included eavesdropping, interception, alteration, disclosure, transmission and theft;
- Network attacks – these include interference, inputs, transmission, alteration, deletion, unauthorized access, virus distribution, connivance, etc.
- Fraud attacks – these include frauds and forgery, falsification, modification, adjustment or rework, etc.

V. DISCUSSION &CONCLUSION

Whilst threats and threat agents change, security vulnerabilities exist throughout the life of a system or protocol, unless specific steps are taken to address the vulnerabilities.

The impact of insider and/or corporate espionage agents on SMEs could be catastrophic. SMEs in developing economies would need to re-orient their perceptions of cyber-security vis-à-vis information assets and their attractiveness. A number of factors, including policy formulation (or reformulation), as well as strict enforcement are paramount to any effective mitigation measures put forth. Some of the factors necessary for consideration are human-centered and technological in nature. For example, personal and corporate factors include addressing various motives that are likely to motivate an employee to become an espionage agent. Employees encountering financial and social challenges would need to be identified and counseled or assisted in some ways.

To minimize the likelihood of access privilege escalations, measures such as periodic and on-spot systems audits ought to be carried out, and a policy on separation of duties (SoD) ought to be enforced.

System monitoring and audits should be infused with constant employees' behavioral observation. These are likely to alert managers of any unusual behaviors, unnecessary or inappropriate access and interests in confidential assets.

Finally, SMEs must create a conducive environment for other employees to anonymously report any suspicious moves. Future studies will seek to understand some of the behavioral factors that influence loyal and trusted employees to be coerced into becoming espionage agents.

REFERENCES

[1]. E. O. Yeboah-Boateng, "Cyber-Security Challenges with SMEs in Developing Economies: Issues of Confidentiality, Integrity & Availablity (CIA)," center for Communications, Media & Information technologies (CMI), Aalborg University, Copengahen, 2013.

[2]. J. Mallery, "Building a Secure Organization," in Computer & Information Security Handbook, J. R. Vacca, Ed., Morgan-Kaufmann, Inc., 2009, pp. 3-22.

[3]. Greitzer, Frank L. & Deborah A. Frincke, "Combining Traditional Cyber-security Audit with Psychosocial Data: Towards Predictive Modeling for Insider Threat Mitigation," in Insider Threats in Cyber-security, J. H. D. G. &. M. B. Christian Probst, Ed., New York, Springer, 2010, pp. 85-114.

[4]. Federal Bureau Of Investigation (FBI), "The Insider Threat," FBI, DoJ, 2012.

[5]. T. Dugo, "The Insider Threat to Organizational Information," Auburn University, Auburn, AL, 2007.

[6]. D. B. Parker, Fighting Computer Crime, New York: John Wiley & Sons, Inc., 1998.

[7]. Salvatore J. Stolfo, Steven M. Bellovin, Shlomo Hershkop, Angelos Keromytis, Sara Sinclair & Sean W. Smith, Insider Attack & Cyber-security: Beyond The Hacker, Springer - Science Business Media, LLC, 2008.

[8]. M. Osborne, How To Cheat At Managing Information Security, Syngress Publishing, Inc., 2006.

[9]. E. O. Yeboah-Boateng, "Fuzzy Similarity Measures Approach in Benchmarking Taxonomies of Threats Against SMEs in Developing Economies," Canadian Journal on Computing in Mathematics, Natural Sciences, Engineering and Medicine, vol. 4, no. 1, pp. 34-44, February 2013.

[10]. Young, Susan & Dave Aitel, The Hacker's Handbook - Strategies for Breaking Into and Defending Networks, CRC Press, 2007.

[11]. Jacobsson, Markus & Alex Tsow, "Identity Theft," in Computer & Information Security Handbook, Morgan-Kaufmann, 2009, pp. 519-549.

[12]. Randy J. Boyle & Raymond R. Panko, Corporate Computer Security, Pearson Prentice, 2013.

[13]. David Dittrich & Kenneth Einar Himma, "Hackers, Crackers & Computer Criminals," in Handbook of Informatio Security: Threats, Vulnerabilities, Prevention< Detection & Management, vol. 3, John Wiley & Sons, Inc., 2006, pp. 154-171.

[14]. Robert F. Mills, Gilbert L. Peterson & Michael R. Grimaila, "Insider Threat Prevention, Detection & Mitigation," in Cyber-security & Global Information Assurance: Threat Analysis & Response Solutions, vol. Section I, Information Science Reference, 2009, pp. 48-74.

[15]. C. Pfleeger, Reflections on the Insider Threat: Insider Attack & Cyber-Security, 2008.

[16]. G. Kamm, "Disgruntled Worker Accused of Deleting $2.5 Million of Files," First Coast News, 2008.

[17]. J. Wiles, Techno Security's Guide to E-Discovery & Digital Forensics, Syngress Publishing, Elsevier, 2007.

[18]. D. Storey, Understanding the Small Business Sector, London: Routledge, 1994.

[19]. J. Bolton, "Report of the Committee of Inquiry on Small Firms," HMSO, London, 1971.

[20]. A. Deaton, "Savings in Developing Countries: Theory & Review," in Proceedings of the World Bank Annual Conference on Developing Countries, 1989., 1990.

[21]. Walsham, Geoff & Sundeep Sahay, "Research on Information Systems in Developing Countries: Current Landscape & Future Prospects," Information Technology for Development, 2005.
[22]. Ellefsen, I.D. & S.H. von Solms, Framework for Cyber Security Structure in Developing Countries, University of Johannesburg, 2012.
[23]. International Telecommunications Union (ITU), "International Multilateral Partnership Against Cyber Threats (IMPACT)," ITU, 2011.
[24]. International Telecommunications Union (ITU), "Guide to Cyber-security for Developing Countries," ITU, 2007.
[25]. D. Gibson, Managing Risk in Information Systems, Jones & Bartlett Learning, 2011.
[26]. Cashell, Brian, William D. Jackson, Mark Jickling & Baird Webel, "The Economic Impact of Cyber-Attacks," US Congressional Reserach Service, 2004.
[27]. PriceWaterhouseCoopers, "Information security Breaches Survey, 2006," PWC & DTI, 2007.
[28]. Hemraj Saini, Yerra Shankar Rao & T.C. Panda, "Cyber-crimes and Their Impacts: A Review," International Journal of Engineering Research & Applications (IJERA), vol. 2, no. 2, pp. 202-209, April 2012.