BOOK CHAPTER | SMEs & Rhetoric of Cyber Security

Rhetoric of Cyber Security in Small and Medium Scale Enterprises: A Conceptual Exposition.

Olanipekun, Wahid Damilola (PhD)
College of Management and Information Technology,
American International University, West Africa, The Gambia
E-mail; w.olanipekun@aiu.edu.gm
Phone: +2207026523
ORCID ID: https://orcid.org/0000-0002-9651-6655
Google Scholar ID: https://scholar.google.com/citations?user=jPJLAX0AAAAJ&hl=en

Abstract

The tremendous growth and developments facilitated by Information and Communication Technology among 21st century business organizations comes with numerous risks, resulting from their reliance on digital services and complex supply chains. One of the most notable risks concerns cybersecurity, which can take numerous forms and can have very significant negative consequences for the victims. In every economy, Small and Medium Scale Enterprises (SMEs) are seen as a pivotal instrument of economic growth and development. This paper summarizes the arguments and counterarguments within the scientific discussion on the issue of cyber security management in small and medium scale enterprises. 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. This paper in its exploratory nature employed the use of a phenomenological approach to examine the rhetoric of cybersecurity in SMEs.

Keywords: Cyber security, Digitalization, Entrepreneurship, SMEs, Sustainable Development

Introduction

The past thirty years have seen tremendous growth in the capabilities and reach of information and communication technologies (ICTs). Harwood (2014) opined that the society is increasingly dependent upon the internet and the systems delivered through it. Our critical infrastructure sector is reliant on networked environments for its daily operation. The Internet, especially, has become a critical enabler of social and economic change, transforming how government, business and citizens interact and offering new ways of addressing development challenges.

BOOK Chapter | Web of Deceit - June 2022 - Creative Research Publishers - Open Access — Distributed Free

Citation Olanipekun, W.D. (2022). Rhetoric of Cyber Security in Small and Medium Scale Enterprises: A Conceptual Exposition.. SMART-IEEE-ACity-ICTU-CRACC-ICTU-Foundations Series
Book Chapter on Web of Deceit - African Multistakeholders' Perspective on Online Safety and Associated Correlates Using Multi-Throng Theoretical, Review, Empirical and Design Approaches. Pp 239 -246. www.isteams.net/bookchapter2022.
DOI https://doi.org/ 10.22624/AIMS/BK2022-P40

Klimburg, (2012) opined that the role that Information and Communication Technology (ICT) plays in all aspects of human endeavors is well documented and evident. ICT has integrated different economies of the world, through the aid of electronics via the internet. According to the World Economic Forum's report Globalization 4.0, more organizations than ever are conducting business online (Whitehead, 2020). To carry out daily activities, people are becoming increasingly dependent on complex and dynamic cyber systems. The spate of rising preponderance of digital footprints and sophistication in cyber-attacks has prompted the urgency to intensely secure data and other organizational resources from exposure to activities of cybercriminals. Digitalized digital technologies and software applications have been interwoven at practically all human and community activity levels, from personal banking to controlling military power to coordinating a massive network of aviation traffic.

Although this integration has resulted in enormous increases in process improvement productivity, it has also been subjected to a wide variety of provocations from devious cybercriminals, groups, or even state government agencies. Such cyber threats have evolved over time to attack many cyber capabilities, like Distributed Denial-of Service (DDoS), data theft, modification to data code, computer virus attack, and a variety of other threats. There is a significant rise of the internet as a medium of business operation for Small and Medium Enterprises (SMEs), and it has exposed SMEs to the threats of Cybercrime. Over time, Information Technology (IT) has offered a range of opportunities to SMEs as the global means of communication and business operation (Amrin, 2015).

The dependency of SMEs on IT has made them vulnerable to newer IT security threats. SMEs can be one of the popular targets of cybercriminals for their affiliation with bigger companies as their clients. Hence, protecting SMEs from cybercrime and cyber security risks should be a major concern for SMEs themselves (Amrin, 2015). As our reliance on the Internet grows, our interconnected networks become more vulnerable to cyberattacks. Cyberattacks and other cyber threats can cause disastrous results, especially if a coordinated targeted attack hits multiple networks at the same time (Lu, Wang, Ouyang, Roningen, Myers & Calfas, 2018). Zhang, Wang, Liu and Wei (2021) posits that the wide spread applications of the information and communication technology (ICT) introduce higher risks on cybersecurity in modern cyber-physical systems.

SME's dependency on Information Technologies and Internet has opened the door to vulnerabilities to cybercrime. Cybercrime is one of the biggest threats to modern businesses. Hence, the cybercrime in the Small Medium Enterprises (SMEs) environment is a growing concern. The threat is particularly poignant for SMEs with limited budgets and resources to protect themselves. These vulnerabilities are making information security a critical issue for all SMEs. Unfortunately, cybercrime prevention is often neglected within the SME environment (Amrin 2015). The inadequate cyber security protection in SMEs has led to an increasing number of attacks and subsequent cyber security incidents (Whitehead, 2020).

Literature Review

Cyber Security

The Fourth Industrial Revolution and thus the new emerging threats, have established new requirements for state security, such as control and protection of information in cyberspace (Eurostat, 2021). These activities allow to counteract attacks by criminal groups and to prevent penetration by hostile entities (Górka, 2018). Therefore, cybersecurity covers a set of issues related to providing protection in the area of cyberspace. The concept of cybersecurity is related, inter alia, to the protection of the information processing space and the interactions taking place in ICT networks (Przysucha, 2020). According to the Ponemon Institute, over the course of 12 months from 2013 to 2014, 110 million Americans (about half of the country's adults) fell victim to hackers who exposed their personal information (CNN Money, 2014). In 2014 alone, the Federal

Bureau of Investigation (FBI) alerted over 3,000 US companies that they had been victims of cyber-attacks (PwC, 2015). Hackers have utilized attacks encoded on sophisticated malicious software (malware) in order to steal individuals' private information and compromise the integrity of organizations, such as the aforementioned attack on Target, and other major organizations, notably Sony and the US Office of Personnel Management (OPM). Cybercrimes are perpetrated leveraging the internet, and advancement in ICT could provide a handy tool for the proliferation of criminal activities, if not properly regulated.

Although the cyber security and its concepts change over the time, it is worth saying that it was mentioned first time in Computer Science and Telecommunications Board's report: "Computers at Risk: Safe Computing in the Information Age" (CSTB, 1991) which defined this term as: ''protection against unwanted disclosure, modification, or destruction of data in a system and the safeguarding of systems themselves'' (CSTB, 1991). When defining cybersecurity, Nissenbaum (2005) refers to three categories. Firstly, protection from dangerous, antisocial and disruptive communications and organizations that come from computer networks, secondly, protection for societal infrastructures such as for example banks, healthcare, communication media and government administration and lastly, protecting ISs from being partially or completely disabled.

According to the US Department of Homeland Security's (DHS) National Initiative for Cybersecurity Careers and Studies (NICCS) and adopted from the National Institute of Standards and Technology (NIST), cybersecurity is "the activity or process, ability or capability, or sta te whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation. Cyber security is the protection of systems in the organizations, their data and network in the cyberspace (Cyber Security Products and Services, 2016). Cybersecurity is a critical issue for many businesses. In a business or any organization, there are different threats associated with their systems, data, and networks. The threats include cyber crime, cyber war, and cyber terror (Cyber Security Products and Services, 2016).

Small and Medium Scale Enterprises

The definition of SMES is amorphous as it varies from country to country and even within the same country, it may vary from sector to sector depending on the purpose for which the definition is sort (Ogunleye, 2004). Ayaggari (2003) contends that the definition of SMEs varies according to context, author and countries. The conceptualization of the concept of SMEs depends to a large extent on a country's level of development and this makes it difficult to have a universal definition of what an SMEs are. It is however quick to note that there are some common indices of the definition such as number of employees, value of assets and turnover. The concept of SMEs is dynamic and relative (Ogunleye, 2004; Olorunshola, 2004; Otokiti, 1987).

A review of the literature on SMEs shows that the definition of SMEs significantly varies from country to country depending on factors such as the country's state of economic development, the strength of the industrial and business sectors, the size of SMEs and the particular problems experienced by SMEs (Ogunleye, 2004; Olorunshola, 2004; Otokiti, 1987). . Several institutions and agencies defined SMEs differently with parameters such as employee's size, asset base, turnover, financial strength, working capital and size of the business (Olutunla, 2001).

SMEs are firms with number of employees that is lesser than 250 and the financial annual turnover must not exceed 50 million euro (European Commission, 2003). More specifically, in the group of small enterprises belong the enterprises that employ less than 50 employees and with a financial annual turnover less than 10 million euro and in the group of the medium enterprises belong the enterprises that employ less than 250 employees and their financial annual turnover does not exceed 50 million euro (European Commission, 2003).

In every economy, Small and Medium Scale Enterprises (SMEs) appears to have been seen as a pivotal instrument of economic growth and development either in developed or developing economies. This is why SMES occupy place of pride in virtually every country or state. SMES are seen to represent an engine of growth and catalyst of socio-economic transformation in any country as they represent a veritable vehicle for the achievement of national economic objectives of employment generation and poverty reduction at low investment cost as well as the development of entrepreneurial capabilities including indigenous technology (Aremu, 2014). According to Ayyagari, Beck and Demirguc-Kunt (2007), SMEs are a core sector element for fostering the growth of economy, increasing employment and alleviating poverty. On the global level, SMEs perform more than 90 percent of the worldwide business economy (Vives, 2006).

Cyber security in SMEs

The Internet was created to expand opportunities for individuals to electronically communicate with each other without much regard to law and order. Indeed, the lack of order is one of the primary positive characteristics of the Internet, but it comes with fostering a somewhat lawless environment. Over time, more sophisticated communication networks have been created. Improved communications have created a multi-billion dollar global economy. Virtual network gateways used to protect transactions and other proprietary information has been insufficient against criminal hackers (Sinrod, Eric & Reilly, 2000).

Cyberspace has become the “Wild West” of business opportunities for companies. The explosion of growth opportunities has also created substantial cyber insecurity for such companies. Large companies have the budget and resources to manage cybersecurity risks with the ability to hire experts to provide guidance and technology to address problems on a large corporate scale. Small and medium sized enterprises (SME), on the other hand, lack the funding, knowledge, and human capital to sufficient defend itself against the various criminals (Chak, 2015).

In order to keep providing their services to customers, companies need to be able to handle large amounts of data (Solita, 2017). This data may contain critical information about the company, its products, services and customers, and it is one of the most important assets businesses have. Because of its importance, the data is a high value target for cyber criminals. It is essential for companies to keep their data and systems secured against attackers, since incidents such as data breaches may end up costing businesses millions of dollars (Ponemon Institute, 2018). Since smaller businesses usually have fewer information and system security resources, criminals are increasingly targeting them (Hiscox, 2018). There are numerous different threats that attackers create for companies, e.g. phishing, emails with malicious attachments, malware, denial-of-service attacks and data breaches (Helsinki Region Chamber of Commerce, 2016). One of the most popular attack types against SMEs (small and medium-sized enterprises) is spear-phishing, a phishing attack that targets specific individuals using previously collected information about them or their organization (Hong, 2012).

In the private sector, large corporations have the resources and funds to manage its individual cybersecurity risks and policies and respond to incidents. However, small and medium enterprises (SME) are less likely to have the same kind of budget and resources to manage their cybersecurity risks effectively while they are more likely to be targeted by criminal hackers. Companies will have to continue to rely on proprietary measures for cybersecurity while the overall framework to manage cybersecurity and cybercrimes are formulated (Chak 2015). Small and medium enterprises (SME) generally have fewer resources to mitigate risks of operating in cyberspace. SMEs are less likely to have skilled IT employees, much less a dedicated IT department to formulate IT policies to mitigate breaches, and business continuity planning. The lack of skilled employees to champion the importance of risk mitigation will also affect investments in memberships such as ISACs. More often than not, SMEs are likely to contract out active monitoring to third party companies with turnkey software or simple anti-virus software.

This can pose a risk in itself that vulnerable software offered by third party companies are likely to add exposure to data breaches if vulnerabilities can be systemically exploited or defenseless against skilled hackers. SMEs have smaller balance sheets or operating accounts to absorb direct losses stemming from cybercrimes. They are more likely to struggle from cybercrimes because they are also less likely to own adequate insurance to losses related to digital assets. While SMEs are less obvious targets, the assets and inherent vulnerabilities of SME can be attractive to criminal hackers (Weise, 2014)

Empirical Review

Osborn (2014) conducted a study on Business versus Technology: Sources of the Perceived Lack of Cyber Security in SMEs. SMEs were surveyed to establish what barriers they might face in terms of cyber security. The results were combined with publicly available information to identify how stakeholders in the SME cyber security ecosystem interact, and establish whether the perceived lack of uptake of cyber security measures in SMEs was accurate. The paper concluded by discussing how the refined understanding of the barriers faced by SMEs might influence development of future SME security solutions. Amrin (2015) conducted a study on The Impact of Cyber Security on SMEs. To achieve the aim of the study a questionnaire instrument was utilised. Sixteen SMEs from different business operations, registered in Europe, were interviewed on their recent IT security trends, cybercrime victimization, and cybercrime prevention practices.

The main findings indicate that the level of IT security of the respondent SMEs is not to a decent point. The implementation of written security policy is present in the SME environment, but it is not very common. In addition, European SMEs fall behind than Australian organizations in order to implementing IT security measures and policy. 4 out of 16 respondent SMEs reported cybercrime victimization incidents over the period 2013-2014. SMEs are simply unaware of IT-related security incidents, because victimized SME does not spread the news fearing further reputational damage. Referable to the smaller sample size, the results are inconclusive to prove any fact related to cybercrime practices.

Chak (2015) conducted a study on managing cybersecurity as a business risk for small and medium enterprises. The study analyzed three solutions for some of the major categorical problems for SMEs looking to manage cybersecurity risks without necessarily large investments in only highly technical solutions which include community policing for broad cooperation within industries, cyber insurance, and cyber hygiene. The collected data analysis that is based on interviews with IT professionals across 6 organizations in Republic of Slovakia revealed that cyber-security is yet to be developed among SMEs and it is an issue that must not be taken lightly. Results show that the IT professionals in these organizations need to strengthen and develop their security thinking and to bring their awareness to a higher level, in order to decrease the vulnerability of informational assets among SMEs.

Haverinen (2019) conducted a study on the Implementation Of Information Security Controls In Small And Medium-Sized Businesses. The research surveyed a group of Finnish companies with 10-250 employees to find out what information security controls they are using as defense measures against hostile actors. Although no alarming shortcomings are discovered, there is a lot of variation in what controls different companies are using. Whitehead (2020) in his research on Investigation of factors influencing cybersecurity decision making in Irish SME's from a senior manager/owner perspective used a qualitative approach with the aid of semi-structured interviewed to accomplish all research objectives. Five participants were selected using purposive sampling that fit the outlined criteria. A conceptual model derived from existing literature consisted of 9 themes forming the basis of questions for semistructured interviews.

Interviews were analysed using thematic analysis and findings were critically assessed in the context of extant literature. Findings from his study revealed that the six factors influencing cybersecurity investment decisions in Irish SMEs were cost, company reputation, monetary loss, awareness, regulation and expertise.

Conclusion and Recommendations

The exponential growth of an innately fluid cyberspace has also increased the complexity of which companies have to navigate while conducting business. The constant change within cyberspace has created as many obstacles as opportunities for leadership of both private and public sectors Cybercrime can no longer be considered a threat that can be effectively managed. Cyberspace is an evolving environment that provides significant opportunities and risks. SMEs have access to greater innovation, cost reduction, and marketing opportunities than ever before. The lack of governance in cyberspace has provided opportunities taken advantage by SMEs, but few are managing the risks related to the lack of law and order in cyberspace. SMEs need develop tools to manage risk because evident vulnerabilities will be eventually exploited by the criminally minded. Some of the risks can be managed by the company itself as shown with cyber hygiene and cyber insurance and another takes a collective effort such as community policing but all require awareness of what the particular risks for operating in cyberspace.

References

1. Aremu, M. A. (2014). Small and Medium Scale Enterprises As A Means of Employment Generation and Capacity Building In Nigeria, A Paper Presented at the International Conference on Management and Enterprise Development on “Intellectuals and New Strategies for Sustainability Development of the Third World” Held at Conference Center, University of Ibadan, Ibadan, Nigeria, October 5th - 8th.
2. Ayyagari, M., Beck, T. and Demirguc-Kunt, A., (2007). Small and medium enterprises across the globe. Small Business Economics, 29(4), 415-434.
3. CSTB (Computer Science and Telecommunications Board)., 1991. Computers at Risk: Safe Computing in the Information Age. Washington, DC: National Academy Press, pp. 1-320.
4. CNN Money. (2014, May 28). Half of American adults hacked this year. Retrieved from: http://money.cnn.com/2014/05/28/technology/security/hack-data-breach/
5. CSIRT, (2009). Computer Security Incident Response Team. Ministry of Finance of the SR. Available at: < https://www.csirt.gov.sk/> [Accessed 25 January 2022].
6. Chak, C.S. (2015). Managing Cybersecurity As A Business Risk For Small And Medium Enterprises. Unpublished Masters thesis, Johns Hopkins University
7. Ding, J. (2021). Cyber Resilience for Critical Infrastructure: A Systematic Review. Unpublished Masters Degree Project in Informatics with Specialization in Privacy, Information Security and Cyber Security , University of Skovde
8. European Commission, (2003). Commission recommendation concerning the definition of micro, small and medium-sized enterprises. Official Journal of the European Union 2003/361/EC. Available at: <http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:124:0036:0041:EN:PDF> [Accessed 5 June 2015].
9. European Commission, (2014). Digital Agenda for Europe: Action 29: Combat cyberattacks against information systems. European Commission. Available at: < http://ec.europa.eu/digital-agenda/en/pillar-iii-trust-security/action-29-combat-cyberattacks- against-information-systems> [Accessed 25 January 2022].
10. Eurostat (2021) “ICT security in enterprises”, Database.
11. Górka, M. (2018) “Cyberbezpieczeństwo jako wyzwanie dla współczesnego państwa i społeczeństwa [Cybersecurity as a challenge for modern society and country]”, in Dębowski T editor Cyberbezieczeństwo wyzwaniem XXI wieku [Cybersecurity as XXI century challenge] r. Łódź-Wrocław, Archaegraph Wydawnictwo Naukowe.

12. Harwood, D.I (2014). Barriers to Cyber Information Sharing. Master of Arts In Security Studies (Homeland Security and Defense) Naval Postgraduate School, Monterey, California.
13. Haverinen, L. (2019). Implementation of information security controls in small and medium- sized businesses. University of Oulu, Degree Programme in Computer Science and Engineering. Bachelor's thesis.
14. Helsinki Region Chamber of Commerce (2016), Yrityksiin kohdistuvat kyberuhat 2016. URL: https://issuu.com/kauppakamari/docs/ yrityksiin_kohdistuvat_kyberuhat_20.
15. Hiscox, A. (2018). The Small Business Guide to Cyber Attacks, 2018 hiscox cyber readiness report. URL: https: //www.hiscox.com/sites/default/files/content/2018-HiscoxCyber- Readiness-Report.pdf.
16. Hong, J. (2012). The state of phishing attacks. Commun. ACM55, pp.74–81.
17. Lu, L., Wang, X., Ouyang, Y., Roningen, J., Myers, N., Calfas, G., (2018). Vulnerability of Interdependent Urban Infrastructure Networks: Equilibrium after Failure Propagation and Cascading Impacts. Comput. Civ. Infrastruct. Eng. 33, 300–315. https://doi.org/10.1111/mice.12347
18. Nissenbaum, H., 2005. Where Computer Security Meets National Security. Ethics and Information Technology, pp. 61-73.
19. Olorunshola, J. A. (2004). "Problems and Prospects of Small and Medium- Scale Industries in Nigeria", In CBN Seminar On Small and Medium Industries Equity Investments Scheme, *http/www.CBN/Org./2004/Maritime.*
20. Olutunla, G. T.(2001). "Entrepreneurship for Economic Development: *Inaugural Lecture Series 27, Delivered at the Federal University of Technology, Akure, Thursday, 26th April, 2001*
21. Ogunleye, G. A. (2004). Small and Medium Scale Enterprises as Foundation for Rapid Economic Development in Nigeria. *In Small and Medium Enterprises Development and SMIEIS, Effective Implementation Strategies* (Ed.), By Ojo A. T., Lagos, Maryland Finance Company and Consultancy Service Ltd.
22. Osborn, E. (2014). Business versus Technology: Sources of the Perceived Lack of Cyber Security in SMEs. Technical Paper, University of Oxford Centre for Doctoral Training in Cyber Security
23. Otokit, S. O. (1987). High Technology in Small Scale Industries: A Comparative Study of Nigeria and Industrialized Countries. *Ph.D. Thesis submitted to University of Delhi*
24. Ponemon Institute, (2011). Second Annual Cost of Cyber Crime Study. Independently conducted by Ponemon Institute LLC, pp. 1-30. Available at: < http://www.hpenterprisesecurity.com/collateral/report/2011_Cost_of_Cyber_Crime_Study_August.pdf> [Accessed 8 March 2015].
25. Ponemon Institute (2018), 2018 cost of a data breach study: Global overview. URL: https://databreachcalculator.mybluemix.net/ assets/2018_Global_Cost_of_a_Data_Breach_Report.pdf.
26. Sinrod, Eric J., and William P. Reilly. (2000). Cyber-crimes: A practical approach to the application of federal computer crime laws." Santa Clara Computer & High Tech. LJ 16
27. Smith J. (1999) Information Technology in the Small Business: Establishing the Basis for a Management Information System. Journal of Small Business and Enterprise Development 4, pp. 326–340.
28. Solita (2017), Thinktank: The data revolution and business. URL: https: //hub.solita.fi/think- tank-data-revolution-and-business.
29. Vives, A., (2006). Social and environmental responsibility in small and medium enterprises in Latin America. Journal of Corporate Citizenship, 2006 (21), pp. 39-50.
30. WDI (2016); World Development Indicator (WDI), International Bank for Reconstruction and Development/The World Bank; Washington D.C, USA. https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_cyber_cle443433.pdf

31. Weise, E. (2015). Antivirus Software Powerless against Sony Hackers." USA Today. December 6, 2014. Accessed February 3, 2015. http://www.usatoday.com/story/tech/2014/12/06/sony-attack-new-era-nucleaoption/19963063/.
32. Zhang, Y., Wang, L., Liu, Z., Wei, W., (2021). A Cyber-Insurance Scheme for Water Distribution Systems Considering Malicious Cyberattacks. IEEE Trans. Inf. Forensics Secur. 16, 1855–1867. https://doi.org/10.1109/TIFS.2020.3045902