Faculty of Computational Sciences & Informatics - Academic City University College, Accra, Ghana
Society for Multidisciplinary & Advanced Research Techniques (SMART)
Trinity University, Lagos, Nigeria
SMART Scientific Projects & Research Consortium (SMART SPaRC)
Sekinah-Hope Foundation for Female STEM Education
Harmarth Global Educational Services
ICT University Foundations USA
IEEE Computer Society Nigeria Chapter

Proceedings of the 36th iSTEAMS Accra Bespoke Multidisciplinary Innovations Conference

Towards the Integration of Cyber Security Into Business Continuity Planning For Small and Medium Scale Enterprises

[1]Aboagye F.O. & [2]Longe, O.B.
[1]Doctoral Programme in Information Technology, Accra Institute of Technology, Accra, Ghana
[2]Faculty of Computational Sc. & Informatics, Academic City University College, Zccra, Ghana
E-mails: phd21s3010009@ait.edu.gh; olumide.longe@acity.edu.gh
Phones: +233244838689; +233595479930

ABSTRACT

This study aims to investigate the integration of cyber security into business continuity planning (BCP) in Small and Medium-sized Enterprises (SMEs). The research will employ a mixed-methods approach, using both quantitative and qualitative data collection methods. The study will emphasize on identifying the contemporary state of cyber security integration into BCP, analyzing the factors that influence the integration, and proposing a framework for effective integration. The theoretical framework will be based on the Theory of Planned Behavior and Resilience Theory. The data will be collected through a survey of organizations and interviews with experts in the field. Descriptive and inferential statistics, content analysis, and thematic analysis will be used to analyze the data. The results of this research will contribute to the body of knowledge on cyber security integration into BCP and inform organizational practice and policy. The findings of this study will be useful for organizations seeking to improve their cyber security and business continuity capabilities, and for policymakers developing regulations and standards in this area. The study's significance lies in its contribution to knowledge, practice, and policy by improving organizational resilience through the integration of cyber security into BCP. The findings of this research will inform practitioners and policymakers of the challenges and benefits of cyber security integration into BCP and provide practical recommendations to enhance organizational resilience against cyber threats.

Keywords: Cybersecurity, Business continuity planning, Resilience, Risk management, Information security, Data protection, Incident response, Disaster recovery, Threats

Proceedings Citation Format
Aboagye, F.O. & Longe, O.B. (2023): Towards the Integration of Cyber Security Into Business Continuity Planning For Small and Medium Scale Enterprises. Proceedings of the 36th iSTEAMS Accra Bespoke Multidisciplinary Innovations Conference. University of Ghana/Academic City University College, Accra, Ghana. 31st May – 2nd June, 2023. Pp 139-158. https://www.isteams.net/ghanabespoke2023. dx.doi.org/10.22624/AIMS/ACCRABESPOKE2023P14

1. INTRODUCTION

Companies struggle to gain and maintain a sustainable competitive advantage in today's global business environment, which necessitates objecting to business changes that must be made (Fiol, 2001). Most business organizations turn to some sort of information technology to accomplish this goal.

As a result, "as applications of information systems technology become wider and more sophisticated, firms need more formal planning processes," it is necessary to analyze many significant organizational elements before integrating information systems and information technology (IT) (McFarlan et all., 1983). Undoubtedly, one of those crucial organizational components corresponds to the cyber security industry.

Business organizations, according to Dhillon and Backhouse (2000), are no longer only valued by their physical assets but also by networks formed with other businesses, where Cyber Security has been significantly increasing in importance and existence. Although there are no manuals for organizing and putting into practice cyber security organizational measures, many businesses worldwide use various tools or policies to deal with cyberspace security to thwart external and internal cyber-attacks into their information systems (Atoum et al., 2014). The way individuals communicate knowledge, do electronic business, and generate value was changed by the internet, which is becoming increasingly vital for conducting business (Askitas & Zimmermann, 2015). Small business owners compete in the technologically advanced international e-commerce markets in the twenty-first century by using computer systems and the Internet (United States Small Business Administration, 2016).

Businesses gain greatly from advances in worldwide wired and wireless technologies, but they are also exposed to potential threats (Weber & Horn, 2017). Small- and medium-sized business (SME) owners frequently lack the IT resources and skills necessary to put new cyber security advice into practice (Harris & Patten, 2014). Particularly, SME owners frequently lack the appropriate procedures to manage the changing cybersecurity risks and information systems security threats that characterize the use of these technologies (Njenga & Jordaan, 2016).

However, for SME owners, negative losses brought on by cyberattacks may not be recoupable (Piggin, 2016). Theft or loss of sensitive information may be an expensive catastrophe for any organization (SBA, 2015). The Federal Communications Commission (FCC), 2014; Layton & Watters, 2014), list among the potential negative consequences on SME owners the loss of clients, money, and in certain cases the forfeiture of business due to high legal costs.

Kindervag et al. (2011) claim that even businesses with very mature and sophisticated cyber security systems cannot completely prevent every assault on their system, particularly if the attackers have access to both time and money. Despite this, it is crucial for all firms, whether they are large or little, to create some cyber security measures to reduce the likelihood of these kinds of assaults. According to recent studies (Watters et al., 2012), there are more cyberattacks occurring worldwide every year, and this trend is expected to continue. Additionally, as the actual assaulting techniques become less effective, cybercriminals are becoming more and more skilled in employing new techniques and tools for cyberattacks in economic activity sectors by targeting enterprises (Gostev, 2012). Despite being aware of the global trend toward increasingly sophisticated cyberattacks, organizations' unwillingness to report them prevents official statistics from determining the precise number of cyber incidents (Byres et al., 2004).

It is assumed that Ghana's circumstance is comparable to other countries. To create adequate cyber security measures, Ghana has seen a large growth in foreign direct investments from numerous foreign investors, which could increase the likelihood of cyber-attacks from outside the country. The number of SMEs in Ghana keeps growing each year, indicating the importance of SMEs to the national economy. Due to Ghana's significant concentration of SMEs, there needs to be more research done on the topic of cyber security measures for SMEs there. A further factor that makes SMEs a desirable target for cyberattacks is the frequency with which they participate in supply chains or other types of alliances with big businesses.

Organizations must establish multi-tiered security strategies that prioritize people, processes, and systems while focusing on prevention, mitigation, and reaction to manage cyber risks (National Institute of Standards and Technology [NIST], 2015). The study will examine the advantages and difficulties of including cyber security into BCP for SMEs through a combination of case studies and survey data. The results of this study will give small and medium-sized businesses (SMEs) useful advice on how to successfully include cyber security in their Business Continuity Planning (BCP) and so increase their overall resilience to cyber-attacks.

1.1Research Background and Justification

Due to the SMEs' increasing reliance on technology, it is more crucial than ever for SMEs to incorporate cyber security into their business continuity planning (BCP). As technology is used more frequently, SMEs are increasingly being targeted by cyberattacks, but many lack the resources and knowledge necessary to fully manage this danger. As a result, the demand for efficient cyber security measures and the incorporation of cyber security into BCP for SMEs has increased. An organization's road map is comparable to a framework or manual of best practices for information security. How can they be sure that their tactical configurations will have the desired effect if they have nothing to guide their strategic security decisions? Without a "roadmap," they will quickly become disoriented and take a disorganized path forward, which might leave certain parts of an organization's security dangerously undermanaged.

Without standards, it is challenging to establish the procedures for where and why security devices ought to be put in a consistent manner. As a result, many decisions about the use and implementation of security technologies are made only based on budget or in response to an event. From a "standard-of-care" standpoint, it is essentially impossible to defend against a negligent security tort because of this reactionary approach. (Protus3, 2019). Over the last two decades, information technology (IT) has advanced to the point where it is now present in practically every part of our lives. SMEs are more digitized than others around the world because they produce and market technology-based solutions, exposing them to cybersecurity threats, particularly when no controls are implemented. Organizational hazards, guidance, and technology are all affected by cyber-risk issues. According to the State of Cybercrime Report published by CyberVentures (2019), the cost of cybercrime is expected to reach $6 trillion by end of 2022.

According to Bada et al. (2019), Africa has one of the highest rates of cybercrime, which has an impact on the region's strategic, economic, and social development. According to the Africa cybersecurity report 2017 (Serianu, 2017), the cost of cybercrime in 2017 was predicted to be $3.5 billion. With a cost of $649 million, Nigeria was the country with the highest cost of cybercrime. Many small and medium-sized businesses are unconcerned about effectively implementing security requirements. As per Bada et al. (2019), fostering good security behavior among employees should be a top priority for SMEs, and building a strong security culture could solve many of the behavioral aspects that contribute to data breaches.

However, in the field of cybersecurity, several sorts of research and development have indeed been noticed, such as governments adopting a national cybersecurity policy so that all citizens are informed of cyber-attacks. However, many firms, particularly SMEs, still have substantial information security weaknesses. According to a study conducted by the European Union Agency for Network and Information Security, SMEs in France are becoming increasingly reliant on their information technology systems to provide services to customers and meet their business objectives. The use of new technologies opens new opportunities for improved business performance and operations, but it also introduces a number of security and privacy risks. These hazards have the capacity to interrupt company continuity and result in monetary, reputational, and other losses for SMEs (Manso et al., (2015)).

According to Manso et al. (2015), new information security and privacy standards should be established and suggested to assist firms in incorporating best practices into their operations and mitigating risks, which will aid SMEs in growing, competing, and innovating. According to Marsh (2015), the UK government announced the launch of the Cyber Essentials scheme, which was developed in partnership with the insurance sector. It accomplishes two goals: providing a clear statement of basic technical control system that all organizations, which include SMEs, should implement to minimize the effects of internet-based threats; and improving security that allows businesses to demonstrate to customers and others that they have taken critical precautions against cyber risk. (Marsh, 2015). Recent studies have shown that SMEs are becoming increasingly vulnerable to cyber-attacks, due to the growing reliance on technology and the limited resources and expertise available to SMEs to address cyber security threats (NIST, 2018; Cybersecurity Ventures, 2018). Research has also shown that SMEs often lack the resources and expertise to effectively address cyber security threats and that many SMEs do not have a BCP in place (National Cyber Security Centre, 2018; Small Business Administration, 2017). Furthermore, research suggests that the integration of cyber security into BCP can help SMEs better protect their vital information and systems (CERT-UK, 2016; National Cyber Security Centre, 2018). However, there is limited research on the benefits and challenges of integrating cyber security into BCP specifically for SMEs, and there is a lack of practical guidance for SMEs on how to effectively integrate cyber security into their BCP (National Cyber Security Centre, 2018). Additionally, there is limited research on how SMEs can develop a robust and cost-effective cyber security strategy (Small Business Administration, 2017).

1.1.1 Understanding Cyber Security Standards

The purpose of cyber security standards is to increase the security of vital infrastructures, networks, and information technology (IT) systems. An information technology environment's assurance and functional obligations are defined by a cyber security standard. Regularity among product developers is made possible by well-developed cyber security standards, which also act as a trustworthy yardstick for acquiring security goods (Karen Scarfone et al., 2018). Cybersecurity standards are often implementation independent and encompass a wide range of precision, from the mathematical explanation of a cryptographic method to the specifications of encryption techniques in a web browser.

A standard must take user wants into account, but it must also be realistic given that producing products that adhere to the standard requires taking cost and technological constraints into account. A standard must also have provable standards; or else, users cannot evaluate security, even when products or devices are examined in contrast to the standard.

One way to describe security standards is as a set of guidelines that ensures efficiency, accountability, and consistency for products or procedures. Standards are made to give a repeatable method of accomplishing things, just like policies govern people's behavior. Based on best practices and compliance, written standards may be used. Because of this, businesses can decide on the use of security measures in an objective manner. Standards are frequently created using "the way we've always done it" as the de facto standard. To make sure that installations and products are in line with the organization's goals, standards based on the product's use are helpful. Additionally, standards support the interoperability and performance of products.

A standard is described as "a document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines, or characteristics for activities or their results, aimed at the achievement of the maximum degree of order in a given context" by the International Organization for Standardization (ISO) (ISO, 2004). To assist enterprises in effectively managing security risk, implementing security controls that adhere to legal and regulatory requirements, and achieving performance and cost benefits, numerous standards for cyber security have been produced.

1.1.2 Cyber Security Explained

For the information technology sector, cybersecurity is essential. Information security is one of the biggest problems in contemporary society. When we think of cyber security, the first thing that comes to mind is cybercrimes, which are on the rise every day. To stop these cybercrimes, various governments and companies are taking numerous steps. Many people are still quite concerned about cyber security despite countless safeguards. The main subject of this study is the challenges that contemporary technology-based cyber security must overcome. Additionally, it places a focus on the most recent data regarding the ethics, trends, and practices in cyber security that are influencing the industry.

1.1.4 Cyber Security Techniques

1. *Access control and password security.* Usernames and passwords have always been a key component of information security. This can be one of the initial cyber security measures.
2. *Authentication of data.* The documents we get must always be validated before downloading, which entails checking to make sure they are authentic and haven't been altered. Usually, these documents are verified using antivirus software that is installed on the machines. To protect the devices from infections, a dependable anti-virus program is required.
3. *Malware scanners.* Typically, this software scans every file and document on the computer for dangerous viruses or malicious code. Examples of malicious software include Trojan horses, worms, and viruses. Malware is the term used to describe this kind of software.
4. *Firewalls.* A firewall is a piece of hardware or software that helps prevent viruses, worms, and hackers from trying to access your computer via the Internet. Every message that enters or leaves the internet is examined by the installed firewall, and those that do not follow the set security standards are blocked. Firewalls are therefore essential for the identification of malware.
5. *Anti-Virus Software.* A computer application known as antivirus software works to identify, stop, and act against dangerous software programs like viruses and worms. Most antivirus products have an auto-update capability that enables the program to download profiles of fresh infections so that it can scan for them as soon as they are found. Every system must have anti-virus software as a minimum requirement.

Nevertheless, since our culture depends so much on technology, we do as well. A growing number of risks are also posed by technology because of the opportunities it produces. As a result, industrial espionage, cybercrime, and cyberattacks have made it a target. Therefore, it must be protected at all costs. Therefore, keeping cybersecurity is crucial. As more and more products and services in our society move online and depend on us, protecting this technical infrastructure has grown to be an essential part of information systems all over the world. It must be compatible with all available technologies, hardware, software, and storage locations.

1.1.5 Business Continuity Planning

The process of developing preventative and recovery measures to handle possible hazards to a business is known as business continuity. A comprehensive plan for how an organization will be able to deal with calamities without hindering its operations or suffering excessive loss is created using business continuity planning. An organization can prepare for future incidents that could have a detrimental impact on its operations by creating a business continuity plan. Tragedies do happen. We shouldn't underrate the power of nature. Disaster is inevitable and will happen. Losses could come from this. Planning enables us to be prepared to handle such events. Even while developing a plan may appear challenging, stressful situations place a lot of pressure on people to make decisions and act under duress. Always be prepared for the unexpected. We now have insurance, which is necessary for enduring a catastrophe. But it's always important to have a plan.

The process of developing preventative and recovery measures to address possible hazards to an organization is known as business continuity planning (also known as business continuity and resiliency planning). The strategy considers any scenario that could have a negative impact on operations, such as a disruption in the supply chain or the loss or damage of vital infrastructure (such as large pieces of equipment, computer, or network resources). The advantages of a business continuity plan are numerous. When a calamity strikes, the firms will continue to run because of the business continuity plan that is already in place. The cost of disruptions can be decreased with a business continuity plan. The ability to ensure risks that would otherwise be unacceptable is made possible by having a business continuity plan. Business continuity could save a life. Effective business continuity plans have been proven to both save lives and stop significant income loss.

The process of developing a framework for preventing and recovering from potential risks to a corporation is known as business continuity planning (BCP). In the event of a disaster, the strategy ensures that workers and assets are protected and that operations can resume swiftly. Business Continuity Planning is usually done in advance and requires input from key stakeholders and employees. A list of goods and equipment, data backups, and backup site locations is frequently included in a Business Continuity Plan. In addition, the BCP will identify plan managers and include contact information for disaster responders, critical personnel, and support site suppliers. Plans may explain how corporate services can be maintained in the event of both short-term and long-term outages.

Business Continuity Planning necessitates the identification of all risks that may have an impact on the company's processes, making it an essential component of the risk management strategy. Natural catastrophes, fire, flood, or weather-related occurrences, as well as cyber-attacks, are all potential threats. Business Continuity Planning is an important part of any business. Threats and interruptions suggest a revenue deficit and increased operating costs, which leads to a decrease in productivity. Insurance cannot be relied upon by any firm because it does not cover all expenses or the loss of customers to the competition. Businesses face a variety of obstacles.

There are also potential risk issues that could cause significant hindrance, if not outright disaster, if they occur. It's enough to keep any entrepreneur awake at night, worrying about the future. Effective planning is the key to reducing risks, avoiding catastrophe when feasible, and planning for how to manage and recover when setbacks occur. Having a Business Continuity Plan in place is critical, whether you're dealing with computer security or natural calamities. Most Small and Medium Enterprises in Ghana rely heavily on the internet, and any disruption to it will result in the cessation of their most critical operations and operating regions. As a result, SMEs must be prepared for any technology disruptions that may arise because of unplanned incidents. A well-structured business continuity strategy can assist a company in dealing with any unexpected situations.

1.1.6 Key Elements of Business Continuity Planning

- *An Organized Team:* In an emergency, people shouldn't be unsure who is in charge. Form a team for company continuity with representatives from all departments and locations. These individuals will oversee managing the organization's response to both small-scale and larger-scale emergencies as well as the local response to local events. Employees should continue to be involved in planning and testing throughout the year to keep the plan current and build the familiarity they will need to perform under pressure during an actual emergency.
- *A comprehensive plan:* At every site where you conduct business, consider the potential sorts of disruptions. Determine what you would need to do to preserve your most important processes after considering the worst-case scenario. Ranking recovery priorities based on factors such as revenue, legal implications, brand difficulties, consumer protection, etc.

should be done before mapping this priority to applications, people, facilities, and equipment.

- *Effective testing:* Review and update your strategy at least once every year, and preferably more often, to account for changes to your operational structure, business priorities, and other factors.
- *Communication of Emergency:* Make a toolkit that includes all available methods of communication, such as telephone, email, public address, intranet, instant messaging, texting, and the company website. Make sure you're ready to provide a consistent message to the public through press releases, social media updates, and spokesperson interviews. Draft sample emergency messages in advance so they can be changed quickly during an actual disaster.
- *Safety of Employees:* The safety of all the employees must never be underestimated.
- *Uninterrupted Use of Company Resources:* It's crucial to retain workers employed to preserve data, ensure customer satisfaction, and maintain efficiency. People can now work wherever it is secure and practical to do so, including at home, at a hotel conference room, at a friend's house, or anywhere. In this situation, organizations that already support remote work styles are far ahead of the curve. People just continue to utilize the same remote access tools they typically do, just in a different physical setting, rather than having to adjust to disaster mode as an altogether new way of working.
- *Continuous Operations:* Operations of the organization should not be interrupted.

1.2 Research Field and Subject of Study

This thesis's potential research focus is information technology and cyber security, more specifically the planning and management of business continuity. The integration of cyber security into business continuity planning for small and medium-sized enterprises (SMEs) is the topic of this study. The study's objectives include understanding the BCP methods currently used by SMEs, identifying the benefits of incorporating cyber security into BCP, and offering helpful advice for SMEs to strengthen their resistance to cyber-attacks. The development of a cost-effective cyber security strategy for SMEs is another goal of this research.

1.2.1 Objectives of the Study

The main goal of this thesis is to study how Small and Medium-sized Enterprises (SMEs) may effectively incorporate cyber security into their business continuity planning (BCP) and increase their overall resilience to cyber threats. It also offers practical advice for SMEs on how to do this. This goal is probably going to be divided into more focused goals that are connected to the research problem, such as figuring out how to effectively incorporate cyber security into BCP for SMEs, examining the advantages and difficulties of doing so, and creating a cost-effective cyber security strategy for SMEs.

Specific Objectives

In accomplishing the overall goal, the study will address the following objectives:

1. To examine current BCP practices in SMEs and identify areas where cyber security can be effectively incorporated.
2. To explore the benefits and challenges of integrating cyber security into BCP for SMEs through case studies and survey research.
3. To provide practical guidance for SMEs on how to effectively integrate cyber security into their BCP and improve their overall resilience to cyber threats.
4. To Identify and fill the research gaps in the current literature on integrating cyber security into BCP for SMEs.
5. To develop a methodology that can be used to assist SMEs in creating a cost-effective cyber security strategy.

1.3 The Research Problem Statement

Businesses are compelled to rely on technology more and more to complete daily tasks in an era of quickly advancing knowledge and technology. Although these modern technological advancements help organizations operate more productively, they also expose them to several hazards. Unfortunately, SMEs are frequently the target of cyberattacks because they are unaware of how serious these attacks are and lack the necessary security precautions (Safa et al. 2016). SMEs are more exposed to cyber danger as they adopt new technology. Businesses need to learn what cyber risk is and how much they have recently been exposed to it as it relates to their industry.Due to their small size or the belief that they have nothing worth taking, SME owners frequently do not see themselves as potential targets for cyber assaults (SBA, 2015). About 80% of SME owners don't employ proper measures to protect against cyberattacks, which is a common concern for business (Shackelford, Fort, & Prenkert, 2015).

Even though most SMEs worldwide have implemented some sort of cyber security measures, these safeguards are frequently insufficient (Byres and Lowe, 2004). However, because cyber threats evolve and change quickly, modest cyber security measures are frequently insufficient and must be periodically reevaluated and upgraded (Kindervag et al., 2011). Additionally, a lot of SMEs consistently spend money on cyber security measures, yet their Information Systems are still insufficient and dangerous for cyberattacks (Julisch, 2013). Cyberattacks are on the rise, and governments, corporations, and people will continue to be victimized on a regular basis (Desai, 2013Walker-Osborn & McLeod, 2015).

The exposure of SMEs to basic cyber security procedures, which are frequently insufficient and hence necessitate re-evaluation, places these businesses in a difficult position and prompts a desire to comprehend the guiding principles that SMEs use to develop their cyber security measures within their business continuity planning. Ghana was one of the first countries to be connected to the internet, with a high rate of adoption. The country's information and communication technology (ICT) sector has grown quickly, and it is progressively turning into an advanced technology hub. Many small and medium-sized Enterprises (SMEs) in Ghana have taken advantage of this trend and use it for their day-to-day operations and transactions. Although information technology provides many benefits to SMEs, it has also impacted the cyber security landscape, resulting in cyber risks such as hacking, data leakages, social engineering schemes, cyber fraud, SIM Box fraud, and so on.

The entire SME sector must tackle the lack of sufficient cybersecurity measures in their business continuity plans. Cybercrime dangers have increased because of digitization, specifically if limited or no safeguards are in place. To increase their organization's cybersecurity readiness, SMEs in Ghana require an effective strategy to handle cyber-risks as part of their business risks. As a result, significant elements affecting cyber-risk management in Ghanaian SMEs must be identified, and a plan must be developed to integrate them into their Business Continuity Plans. The research problem statement for this thesis on the integration of cyber security into business continuity planning (BCP) for small and medium-sized enterprises (SMEs) is.

Notwithstanding the increasing importance of cyber security in today's business environment, many small and medium-sized enterprises (SMEs) struggle to efficiently integrate cyber security into their business continuity planning (BCP). The lack of resources and expertise in cyber security among SMEs can lead to unsatisfactory protection against cyber threats and a lack of resilience in the event of a cyber-attack. The goal of this study is to comprehend the extent to which SMEs have integrated cyber security into their business continuity plans (BCP), the advantages and difficulties of doing so, and to pinpoint best practices and lessons discovered from SMEs that have effectively done so."

1.4.Research Questions

1. This study will be guided by questions to identify current practices, gaps, and to offer useful advice for SMEs. They will also aid in determining the advantages and difficulties of including cyber security into BCP for SMEs and in the development of a financially viable plan for SMEs to strengthen their resilience against cyber-attacks.
2. What are the current BCP practices in SMEs and how can they be improved through the integration of cyber security?
3. What are the benefits and challenges of integrating cyber security into BCP for SMEs?
4. How can SMEs effectively integrate cyber security into their BCP to improve their overall resilience to cyber threats?
5. What are the research gaps in the current literature on integrating cyber security into BCP for SMEs?
6. How can a cost-effective cyber security strategy be developed for small and medium-sized enterprises?

2. PRIOR RESEARCH EFFORTS

Since cyber security is developing rapidly, there has been some prior research in the field. The researcher explored the effects of cyber-attacks on industries. On cyber security implications, Yeboah-Boateng (2010) analyzed 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 writers argued that non-regulation of 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. The study’s inferential analysis revealed that there are some cyber-security implications on SMEs in a fragmented policy and regulatory environment. A structured questionnaire was used, and data were analyzed. The findings were discussed and interpreted to provide highlights of these policy and regulatory challenges.

Batola (2016) conducted research to evaluate cloud computing in Ghana; Benefits and contribution to organizational performance in the Techiman Municipality. In all, sixty (60) questionnaires were distributed to Fiagya Rural Bank and Aspet ‘A’ Company limited. The study used systematic random sampling and probability sampling techniques to ensure that participants were accessible throughout the period of study. Within this research work, the descriptive research type was used. Descriptive analysis factors like frequency tables, mean scores and percentages were generated, and their interpretations thoroughly explained and interpreted. The study found out that, the major benefits of cloud computing were improved collaboration between employers and customers, cost savings, extensive technical support from cloud providers, business continuity through disaster recovery, unlimited storage, and safety in data storage. They argued that the lack of capital and inadequate technical expertise was among the factors that prevented SMEs from reaching their potential. The study also revealed that the awareness level of SMEs on the availability and accessibility of cloud services is low.

Kofi Koranteng Adu (2018) investigated the cyber security awareness and policies within corporate organizations in Ghana. Design/methodology/approach Using both quantitative and qualitative approaches underpinned by questionnaire and document analysis, data was collected from 100 participants centered on cyber security awareness and information policies. Their study underscored that although corporate organizations had a good knowledge of IT, their awareness of cyber security remains limited. It observed that most organizations in Ghana are not integrating legal aspects into their information security policies. It proposed the need to increase the security awareness of corporate organization particularly because of the vulnerabilities they are exposed to.

They settled on the use of legal policies at the expense of the technicalities involved in setting up a robust cyber secured network that will fend off attackers and save the corporate organizations from losses.

Abdulrahim Nabihah Rishad (2019) conducted a case study focused on in-depth understanding of the cybersecurity risk management practices within the selected SME. Both quantitative and qualitative research was done. The quantitative data obtained was classified numerically for it to be analyzed. The qualitative data collected from primary sources was systematically organized to facilitate analysis. The research findings revealed that cybersecurity investment, cybersecurity management, training and awareness, cybersecurity policy programs, cybersecurity vulnerability management programs, real time network monitoring and incident management play a big role in the management of cyber-risk within SMEs. The implementation strategy developed provides a roadmap with proposed timelines to assist in the management of cyber-risk. The study demonstrated that cybersecurity framework is suitable for the SME environment but didn’t relate it to how it could be effectively fused into business continuity for the benefit of the SMEs.

2.1 Research Gap

The three pillars of security are people, processes, and technology Bada et al. (2019). There may be a reduction in exposure to an organization when these three elements operate together. Additionally, there are more solutions than ever before to address security-related challenges. A collection of guidelines for goods or procedures that promote efficiency, accountability, and uniformity are known as security standards. Standards are intended to give a repeatable method of accomplishing things, just how policies govern people's behavior. Utilizing established standards may be based on best practices and compliance. This makes it possible for businesses to implement security equipment with objectivity (Marsh 2015).

According to a review of the literature on cybersecurity management in small and medium-sized businesses, SMEs must understand the relevance of setting up their information technology infrastructure according to standard frameworks and consider the integration cyber security into their business continuity plans. After detecting risks and vulnerabilities and implementing administrative steps and comprehensive remedies, a cybersecurity risk management framework is required to ensure that a company is appropriately secured (Barlette et al. 2017). By implementing a cyber-risk management strategy, companies can mitigate cyber risks and avoid assaults by understanding their information systems' hazards and vulnerabilities.

There is not much empirical research on the successful strategies SMEs utilize to defend their companies from cyber-attacks. Although it may not necessarily be a new topic, most SMEs do not give much credence to the building of their information technology security to best practice standards (Heschl, 2007). Cyber security integration into business continuity planning is rarely implemented in SMEs' IT infrastructure. Small and Medium-sized Enterprises (SMEs) tend to be more concerned with gaining internet access in their various locations than they are with security flaws and the potential consequences of a breach.

There is a lack of readiness in Organizations thus they can no longer afford to be unprepared given the frequency and complexity of cyber crises both locally and globally. Before a breach happens, organizations must test their defenses and be prepared to act when necessary. Organizations will pay a significant price for failing to anticipate and react to breaches as they fight to get back to business. When disasters do occur, organizations must make sure they can handle crises well (Ridley et al., 2004). A thorough crisis response plan should be in place and often exercised during "calm periods" to ensure that everyone is aware of their roles and responsibilities. Incidents that are poorly handled can have a large financial impact as well as reputational damage that may be challenging to repair (Hu and Scott, 2014).

Any organization's ability to operate depends on its data. Despite the high costs of the equipment, internet connectivity, and apps, the data that resides in a data center is more valuable, and its loss can have long-lasting impacts on a business. A greater percentage of SMEs don't seem to be having secure IT architectures built to standard frameworks and integrated with Cryptography, Server redundancy and Network redundancy. They end up losing most of their data due to attacks and other incidents. Most SMEs in Ghana have very little knowledge on information technology system continuity and resilience. IT resilience is also growing, complementing redundancy. Resilience allows workloads that fail or stop responding to be restarted on other virtual machines on other servers (ISF, 2016).

In brief, we can take into consideration the following as the gaps identified in this study:

1. Lack of understanding of current BCP practices in SMEs and how they can be improved with the integration of cyber security.
2. Limited research on the advantages and challenges of integrating cyber security into BCP specifically for SMEs.
3. Scant guidance on how SMEs can effectively integrate cyber security into their BCP to improve their resilience to cyber threats.
4. The lack of research on the specific methodologies to be used for case studies and survey research.
5. Limited research on how small and medium-sized enterprises can develop a robust and cost-effective cyber security strategy.

Despite the significance of SMEs for the overall economy, neither the government nor academia have considered how frequently they are the target of cyberattacks. As a result, very little attention has been paid to the risks and hazards that cyberspace poses to SMEs in Ghana. The scarcity of focus on SMEs suggests that their cyber security management is an unexplored area that calls for and justifies more research.

2.2 Why fill the Gaps

This research is driven by several factors. Corporate network protection and information security are challenging. When attempting to create or enhance a business security program, it can be challenging to know where to begin in a field that is continuously evolving and progressing. Standards and benchmarks may not be the most interesting subject, but they might be just what a business needs when they need a place to start when figuring out how to traverse the current information technology landscape. A good security program bases its strategic decisions on a combination of best practice recommendations, understanding of an organization's risk profile, and professional assistance. However, there is a lot of constructive debate about which set of security requirements is superior or more user-friendly for SMEs.

Cyber security differs from information security in several ways, the first being that in addition to protecting information, it also covers protecting people from being targets of cyberattacks without their knowledge. Cybersecurity covers ICT infrastructure and equipment that may be accessible across computer networks, which has an extra impact on cyberattacks for the entire society in addition to information and people (Hathaway et al., 2012). Because of this, IT personnel must consider the most recent developments in cyber technology when deciding which cyber security measures to implement to safeguard information systems (Kumar et al., 2008).

Anupam Mazumdar (2018) aimed to increase SME adoption of cloud computing security expertise. Although his exploration met its goals and objectives, there are still some regions that require more research. He believes that his study barely scratches the surface of the wealth of information that is now accessible on cloud computing uptake and successful utilization. The study was unable to pinpoint every problem, thus some areas require additional research.

According to Adam Motiwala's (2017) recommendation, a central organization charged with doing research, formulating, and coordinating cyber security policy, must be established. The new organization should create a framework for putting into practice globally accepted cyber security standards, regularly benchmark the development of cyber security measures, and take into consideration creating an accreditation process for confirming the readiness of public and private organizations. Additionally, greater work should be done to coordinate and share cyber security resources among government entities.

The aforesaid considerations demonstrate that SMEs, which are the backbone of most economies globally, are in danger and up against a serious problem that requires attention on both an intellectual and practical level. Thus, the reason why these Gaps must be filled include:

1. Cybersecurity threats are increasing, and SMEs are becoming a prime target for cyber-attacks, therefore it is crucial for SMEs to have effective cyber security measures in place.
2. Business continuity planning is important for any organization, especially for SMEs, which often do not have the same resources as larger organizations to respond to disruptions. Integrating cyber security into BCP will help SMEs better protect their vital information and systems.
3. Limited research on the benefits and challenges of integrating cyber security into BCP specifically for SMEs, means that there is a lack of practical guidance for SMEs on how to effectively integrate cyber security into their BCP.
4. Filling the gaps in current literature on integrating cyber security into BCP for SMEs will provide valuable insights for researchers, practitioners, and policymakers in the field of cyber security and business continuity management.
5. Developing a cost-effective cyber security strategy for SMEs is important as they often have limited resources and budget to allocate to cyber security, therefore it is important to have a strategy that is tailored to their specific needs.
6. Overall, filling the gaps in this study will help enhance the cyber security posture of SMEs, which in turn will help to protect them from cyber-attacks and improve their overall resilience. The outcome of this study will impact enormously to the empirical literature as well as add up to the development of theories that relate to cyber security integration into business continuity planning.

3. SIGNIFICANCE OF THE STUDY

The significance of this thesis is that it will provide valuable insights and guidance for small and medium-sized enterprises (SMEs) on how to effectively integrate cyber security into their business continuity planning (BCP) and improve their overall resilience to cyber threats.
The significance of this study can have implications for theory/knowledge, practice, and policy in several ways:

Theory/Knowledge: The integration of cyber security into business continuity planning can help to advance and refine existing theoretical frameworks related to cyber security and business continuity. The findings of this thesis can contribute to a better understanding of how organizations can effectively integrate cyber security into their business continuity plans, and what factors may influence the success of such efforts. This can help to improve the overall knowledge and understanding of cyber security and business continuity among academics, researchers, and practitioners.

Practice: The findings of this thesis can also have practical implications for organizations that are seeking to improve their cyber security and business continuity preparedness. By providing insights into the best practices and strategies for integrating cyber security into business continuity planning, this thesis can help organizations to develop more effective and robust plans that are better equipped to withstand cyber threats. This can lead to improved operational resilience, reduced downtime, and better protection of critical assets.

Policy: The integration of cyber security into business continuity planning is becoming an increasingly important issue for policymakers, as cyber threats continue to pose a significant risk to organizations and critical infrastructure. The findings of this thesis can help to inform policy decisions related to cyber security and business continuity, such as the development of guidelines, regulations, and standards for organizations to follow. This can help to promote a more consistent and effective approach to cyber security and business continuity across different sectors and industries. Additionally, by developing a cost-effective cyber security strategy for SMEs, this study will also help SMEs with limited resources and budget to allocate to cyber security. The significance also includes:

1. Filling the research gaps in the current literature on integrating cyber security into BCP for SMEs, which will provide valuable insights for researchers, practitioners, and policymakers in the field of cyber security and business continuity management.
2. Helping SMEs to better protect their vital information and systems will help to reduce the risk of cyber-attacks and minimize the impact of disruptions.
3. Improving the overall cyber security posture of SMEs, which will help to protect them from cyber-attacks and improve their overall resilience.
4. Providing practical guidance for SMEs on how to effectively integrate cyber security into their BCP, which will help them to better protect their vital information and systems.
5. Contributing to the knowledge and understanding of how SMEs can develop a robust and cost-effective cyber security strategy.

3.1 Impact on Business Value

Consumers, other SME owners, third-party software providers, programmers, academics, local, state, and government agencies, as well as other SME owners, may find this research on SME owners' efficient cyber security strategies useful. Case study research on cyber security issues may offer useful knowledge that helps SME owners avoid falling victim to breaches in cyber security. In addition to potentially having a negative financial impact on SME owners, cyber security breaches also cause other management issues like employees becoming frustrated with potential negative customer feedback, system outages, and lost productivity (Hayes & Bodhani, 2013; Hua & Bapna, 2013).

Alternately, according to Gordon, Loeb, and Zhou (2016), investments in cyber security could give firms a competitive advantage by producing supplementary advantages like greater profits. Using different security protection techniques will prevent the installation of viruses, malware, and spyware on host computers and mobile devices, hence preventing most harmful computer security attacks (Egele et al., 2012; Tchakounté, 2014). Regardless of the size of their businesses, business owners should invest in data security since they could become victims of cybercrime (FCC, 2014). To establish efficient security measures to protect against cyber threats, business owners must be informed, pro-active, and aware of their surroundings (Gupta & Raj, 2013).

There are computer users whose only goal is to make money or enjoy themselves by taking advantage of a system's flaw. Both ethical and criminal computer hackers are persistent and patient in looking for openings and flaws in infrastructure; the difference between them is solely in their motivation (Chowdappa et al., 2014). Users of computers should use caution when utilizing network devices (FCC, 2014). One of the key goals for countries is to secure their internet. To put up a first line of defense against online hackers, businesses must invest in preventative solutions. To defend the world's wired environments, businesses, consumers, and governmental organizations should invest in cutting-edge solutions that are years ahead of any illegal hacking concept (Livshits et al., 2013).

3.2 Consequences for Social Change

Having the ability to protect themselves from prospective cyberattacks is one of the main problems facing SME owners (Fielder et al., 2016). SME owners now have few options for addressing cyber security flaws and putting in place efficient preventative measures. The possibility for SME owners to apply cyber security best practices to lessen or minimize future cyberattacks is one aspect of the study's potential for bringing about positive social change. The study's conclusions may give SME owners practical cyber assault defense tactics, which could boost consumer confidence and boost economic development. The implications for positive social change include providing new entrepreneurs and other SME owners with the tools and resources they need to make improvements in their local communities.

The results of this study may alter how SME owners think about cyber security measures and assist SME owners who survive cyberattacks in promoting economic growth by hiring locals and therefore enhancing the socioeconomic lifecycle. As a result of the ongoing and rapid advancements in technology, cybercrimes are becoming more prevalent and difficult to stop. The prosecution of those responsible for these cybercrimes is becoming more challenging. Sending data across a network is more and more common as a result of technological advancements, making that data more susceptible to assaults. Every day, data breaches and interceptions expose billions of sensitive pieces of information. Nowadays, a lot of firms handle and keep their confidential data in the cloud, making them open to intrusion by unauthorized parties. The requirement for enterprises to include cyber security with cryptography in their security planning is increased by this exposure. Overall, this study will have valuable implications for SMEs and the wider cyber security community and will contribute to the understanding of how SMEs can improve their cyber security posture and resilience against cyber-attacks.

4. CONCLUDING REMARKS

This study will examine the integration of cyber security into business continuity planning (BCP) for small and medium-sized enterprises (SMEs). Through a combination of case studies and survey research, the study ais to identify areas where cyber security can be effectively incorporated into BCP for SMEs, explore the benefits and challenges of integrating cyber security into BCP, and provide practical guidance for SMEs on how to improve their overall resilience to cyber threats. Additionally, the study aims to develop a cost-effective cyber security strategy for SMEs. Research has found that SMEs often lack the resources and expertise to effectively address cyber security threats, and that integrating cyber security into BCP can help SMEs better protect their vital information and systems. The study will highlight the need for practical guidance for SMEs on how to effectively integrate cyber security into their BCP and the importance of developing a cost-effective cyber security strategy for SMEs. The study will contribute to the understanding of how SMEs can improve their cyber security posture and resilience against cyber-attacks, and provides valuable insights for researchers, practitioners and policymakers in the field of cyber security and business continuity management.

REFERENCES/BIBLIOGRAPHY

1. Acedo, F.J., Barroso, C. & Galan, J.L. (2006). The resource-based theory: dissemination and main trends. Strategic Management Journal, 277, 621-636.
2. Adler, P. A. and Adler, P. (1994) Observational techniques. In Handbook of qualitative research, edited by N. K. Denzin and Y. S. Lincoln, London: Sage
3. Adner, R. & Helfat, C.E. (2003). Corporate effects and dynamic managerial capabilities. Strategic Management Journal, 2410, 1011-1025.
4. Ahmad, N., & Shamsudin, Z. M. (2013). Systematic approach to successful implementation of ITIL. Procedia Computer Science, 17, 237-244.
5. Ahmed, M.U., Kristal, M.M. & Pagell, M. (2014). Impact of operational and marketing capabilities on firm performance: Evidence from economic growth and downturns. International Journal of Production Economics, 154, 59-71.
6. Akintoye, A. (2015). Developing Theoretical and Conceptual Frameworks. Jedm.oauife.edu.ng>uploads>2017/03/07 (accessed 2017February 22)
7. Akter, S., Wamba, S.F., Gunasekaran, A., Dubey, R. & Childe, S.J. (2016). How to improve firm performance using big data analytics capability and business strategy alignment?. International Journal of Production Economics, 182, 113-131.
8. Alqahtani, S. Alamrl, A. S. Al-Muthchch, M. and Alamer, I. A. (2000) Research methods in social science with SIISS Applications. V4 Edition. Modern National Press, Riyadh.
9. Amit, R. & Schoemaker, P.J.H. (1993). Strategic assets and organizational rent. Strategic Management Journal, 141, 33-46.
10. Anderson, E., 2015. SMEs failing to guard against cyber-attacks, Government warns. The Telegraph, [online] Available at: < http://www.telegraph.co.uk/finance/businessclub/11430701/SMEs-failing-to-guardagainst-cyber-attacks-Government-warns.html>
11. Ashford, W., 2014. SMEs believes they are immune to cyber-attack. Computer Weekly, [online] Available at: < http://www.computerweekly.com/news/2240216202/SMEsbelieves-it-is-immune-to-cyber-attack-study-shows>
12. Atoum, I., Otoom, A., and Amer, A. A., 2014. A holistic cyber security implementation framework. Information Management & Computer Security, pp. 251-264.
13. Baheti, R. and Gill, H., 2011. Cyber-physical systems. The Impact of Control Technology, pp. 161-166.
    Bayrak, T., & Brabowski, M. R. (2006). Critical infrastructure network evaluation. Journal of Computer Information Systems, 46(3), 67-86.
14. Barney, J. (1991). Firm Resources and Sustained Competitive Advantage. Journal of Management, 171, 99-120.
15. Barney, J.B. (2001). Is the Resource-Based "View" a Useful Perspective for Strategic Management Research? Yes. The Academy of Management Review, 261, 41.
16. Barney, J.B. (2007). Resource-based theory.
17. Barney, J.B. (2014). How marketing scholars might help address issues in resource-based theory. Journal of the Academy of Marketing Science, 421, 24-26.
18. Bell, J. (2005) Doing your Research Project: A guide for first time researchers in education, health and social science. 4th ed. Open University Press.
19. Bernard, H. R., 1988. Research methods in cultural anthropology. Newbury Park, CA: Sage
20. Berry, C. M., Carpenter, N. C. and Barratt, C. L., 2012. Do other reports of counterproductive work behavior provide an incremental contribution over self-reports? A meta-analytic comparison. Journal of Applied Psychology, 97(3), pp. 1-24.
21. Boyatzis, R. E. (1998) Transforming Qualitative Information. Sage: Publications.

22. Bradley, M., and Vaizey, E., 2015. Cyber security 'myths' putting a third of SME revenue at risk. UK Government, [online] Available at: 81 < https://www.gov.uk/government/news/cyber-security-myths-putting-a-third-of-smerevenue-at-risk>
23. Braun, V. and Clarke, V. (2006) Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), pp. 77 – 101.
24. Brondizo, E., Leemans, R., & Solecki, W. (2014). Current Opinion in Environmental Sustainability. Texas, U.S.A.: Elsevier Press Inc. http:// dx.doi.org/ 10.1016/j. cosust.2014.11.002CC BY-NC-SALicense (accessed 2016January 26
25. BSI. (2011). 100-1:" Information Security Management Systems.
26. Bulgurcu, B., Cavusoglu, H. and Benbasat, I., 2010. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Quarterly, 34(3), pp. 523-548.
27. Bulmer, M. (1979) Concepts in the analysis of qualitative data. Sociological Review, 27, pp. 651-677.
28. Cartlidge, A., Hanna, A., Rudd, C., Macfarlane, I., Windebank, J., & Rance, S. (2007). An introductory overview of ITIL V3. The UK Chapter of the itSMF.
29. Cassell, C. and Symon G. (2004) Essential guide to qualitative methods in organizational research. Sage publications. pp. 323- 333.
30. Charlet, L. (2015). ISO Survey 2015. Retrieved from https://www.iso.org/the-isosurvey.htm
31. Choo, K. K. R., 2011. The cyber threat landscape: Challenges and future research directions. Computers & Security, pp. 719-731.
32. Cohen, D. and Crabtree, B., 2006. Qualitative research guidelines project. Available at: < http://www.qualres.org/HomeSemi-3629.html>
33. Cornford, T. and Smithson, S. (1996) Project research in Information systems: a student's guide. Published by Palgrave.
34. Crabtree, B. and Miller, W. (1999) Doing Qualitative Research. 2nd ed, London.
35. Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. Technology Innovation Management Review, 4(10).
36. Creswell, J. W., 2009. Research Design: qualitative, quantitative, and mixed methods approaches. 3rd ed. Thousand Oaks, CA: Sage.
37. Creswell, J. W., 2009. Research Design: qualitative, quantitative, and mixed methods approaches. 3rd ed. Thousand Oaks, CA: Sage.
38. Crook, T.R., Ketchen, D.J., Combs, J.G. & Todd, S.Y. (2008). Strategic resources and performance: a meta-analysis. Strategic Management Journal, 2911, 1141-1154.
39. Crotty, M. (1998) The foundations of social research: meaning and perspective in the research process. Sage Publications.
40. Davies, M. (2015). Average person now spends more time on their phone and laptop than sleeping, study claims. Daily Mail. com, Retrieved June, 4, 2016.
41. De Vos, A. S., Strydom, H., Fouche, C. B. and Delport, C. S. L. (2002) Research at grass roots for the social sciences and human professions. Pretoria: Van Schaik.
42. Denscombe, M. (2007) The Good Research Guide for small-scale social research projects. Berkshire: Open University Press.
43. Dhillon, G. and Backhouse, J. 2000. Technical opinion: Information system security management in the new millennium. Communications of the ACM, vol. 43(7), pp. 125-128.
44. Dimopoulos, V., Furnell, S., Jennex, M. and Kritharas, I., 2004. Approaches to IT Security in Small and Medium Enterprises. In AISM, pp. 73-82.
45. Dooley, L. M. (2002) Case Study Research and Theory Building. Advances in Developing Human Resources, 4(3), pp. 335-354.
46. Dunn, M. (2005). A comparative analysis of cybersecurity initiatives worldwide. Paper presented at the WSIS Thematic meeting on Cybersecurity, Geneva.

47. Dwyer, J. (1993) Outdoor recreation participation: An update on Blacks, Whites, Hispanics, and Asians in Illinois. Managing Urban and High-Use Recreation Settings. USDA Forest Service General Technical Report NC-163, pp. 119-121.
48. Fulton, S. & Krainovich-Miller, B. (2010). Gathering and Appraising the Literature. IN LoBiondo-Wood, G. & Haber, J. (Eds). Nursing Research: Methods and Critical AppraisalforEvidence-Based Prcatice (7thEdition).St. LouisMO:MosbyElsevier
49. Galliers, R. D (1992) Information systems research: issues methods and practical guidelines. Alfred Waller Ltd publishers, Oxfordshire. pp. 149-152. Gerhards, R. (2009). The syslog protocol. Netak, L. D., & Kiwelekar, A. W. (2006). Efficient network management using SNMP. Journal of Network and Systems Management.
50. Ghani, A. E. M. (2009) Buyers' Enduring Involvement with Online Auctions: A New Zealand Perspective. Master of Philosophy thesis, Auckland University of Technology.
51. Giles, K., & Hagestad, W. (2013). Divided by a common language: cyber definitions in Chinese, Russian and English. Paper presented at the Cyber Conflict (CyCon), 2013 5th International Conference on.
52. Golafshani, N. (2003) Understanding Reliability and Validity in Qualitative Research. The Qualitative Report, 8(4), pp. 597-607.
53. Gostev, A., 2012. Cyber-threat evolution: the year ahead. Computer Fraud & Security, pp. 9-12
54. Graham, R. S. (2017, October 19). The difference between cybersecurity and cybercrime,
and why it matters. The Conversation. Retrieved from http://theconversation.com/the-difference-between-cybersecurity-and-cybercrime-and-why-it-matters-85654
55. Grant,C.&Osanloo,A. (2014). Understanding, Selecting, and Integrating a Theoretical Framework in Dissertation Research: Creating the Blueprint for 'House'. Administrative IssuesJournal: ConnectingEducation, Practice and Research, Pp. 12-22 DOI: 10.5929/2014.4.2.9
56. Gyeltshen, N. (2016, June 9). BoB transfers Nu 16M based on fake e-mail. BBS Online. Retrieved from http://www.bbs.bt/news/?p=59872
57. Hakim, C. (1987) Research design. Strategies and choices in the design of social research. Boston: Urwin Hyman.
58. Hansen, L. & Nissenbaum, H., 2009. Digital disaster, cyber security, and the Copenhagen School. International Studies Quarterly, pp. 1155-1175.
59. Hart, C., 2005. Doing your masters dissertation. London: Sage.
60. Hathaway, O. A., Crootof, R., Levitz, P., Proctor, H., Nowlan, A. E., Perdue, W., and Spiegel, J., 2012. The Law of Cyber-Attack, pp. 1-71.
61. Helfat, C.E. & Peteraf, M.A. (2003). The dynamic resource-based view: capability lifecycles. Strategic Management Journal, 2410, 997-1010.
62. Herzog, P. (2010). OSSTMM 3–The open-source security testing methodology manual. Barcelona, España: ISECOM.
63. Heschl, J. (2007). Cobit Mapping: Overview Of International IT Guidance: IT Governance Institute USA http://www. isaca. org.
64. Hitt, M.A., Xu, K. & Carnes, C.M. (2016). Resource based theory in operations management research. Journal of Operations Management, 411, 77-94.
65. Imenda, S. (2014). Is There a Conceptual Difference Between Conceptual and TheoreticalFrameworks? Journalof SocialScience, 38(2):185-195
66. ISF. (2007). The Standard of Good Practices for Information Security. Paper presented at the USA: Information Security Forum ISF.
67. ISO/IEC 27001. (2005). Information technology – Security techniques – Information security management systems – Requirements. Retrieved from ISO/IEC 27002. (2005). Information technology – Security techniques – Code of practice for information security management.

68. ISO/IEC 27002. (2005). Information technology – Security techniques – Code of practice for information security management.
69. Joffe, H. and Yardley, L. (2010) Content and thematic analysis. In: Marks, David F. and Yardley, Lucy (eds.) Research Methods for Clinical and Health Psychology, Sage Publications Ltd.
70. Jouini, M., Rabai, L. B. A., and Aissa, A. B., 2014. Classification of security threats in information systems. Procedia Computer Science, 32, pp. 489-496.
71. Julisch, K., 2013. Understanding and overcoming cyber security anti-patterns. Computer Networks, 57, Elsevier B.V., pp. 2206-2211
72. Kajtazi, M., 2013. Assessing Escalation of Commitment as an Antecedent of Noncompliance with Information Security Policy. Doctoral dissertation, Linnaeus University Press, pp. 1-164.
73. Kelly, K., Clark, B., Brown, V. and Sitzia, J. (2003) Good practice in the conduct and reporting of survey research. International Journal for Quality in Health Care, 15(3), pp. 261-266.
74. Keränen, J. & Jalkala, A. (2013). Towards a framework of customer value assessment in B2B markets: An exploratory study. Industrial Marketing Management, 428, 1307-1317.
75. Kessinger, K. (2014). 2014 Global COBIT 5 Governance Study. Retrieved from https://www.isaca.org/About-ISACA/Press-room/Documents/2014-Global-COBITGovernance-Study-Data-Sheet_pre_Eng_0914.pdf
76. Killmeyer, J. (2006). Information security architecture: an integrated approach to security in the organization: CRC Press.
77. Kindervag, J., Holland, R., Balaouras, S. and Mak, K., 2011. Planning For Failure. Forrester Research Inc., pp. 1-16.
78. King, R. and Sabherwal, R. (1992) The Factors affecting Strategic Information System Applications: An Empirical Assessment. Information and Management, 23(4), pp. 217–35.
79. Kish, L. & Verma, V. (1986). Complete censuses and samples. Journal of Official Statistics, 2(4), 381–395. Retrieved from http://www.degruyter.com/view/j/jos
80. Kleinschmidt, E.J., de Brentani, U. & Salomo, S. (2007).
81. Kozlenkova, I.V., Samaha, S.A. & Palmatier, R.W. (2014). Resource-based theory in marketing. Journal of the Academy of Marketing Science, 421, 1-21.
82. Kumar, N., Mohan, K., and Holowczak, R., 2008. Locking the door but leaving the computer vulnerable: Factors inhibiting home users' adoption of software firewalls. Decision Support Systems, 46(1), pp. 254-264
83. Lai, W. & Chang, P. (2010). Corporate motivation and performance in R&D alliances. Journal of Business Research, 635, 490-496.
84. Lainhart IV, & John W. (2000). COBIT™: A methodology for managing and controlling information and information technology risks and vulnerabilities. Journal of Information Systems, 14(s-1), 21-25.
85. Leech, N. L. and Onwuegbuzie, A. J., 2007. An array of qualitative data analysis tools: A call for data analysis triangulation. School Psychology Quarterly, 22(4), pp. 557
86. Leedy, P. D. (1997) Practical Research Planning and Design, 6th Edition, Prentice-Hall Inc.
87. Lester, F. (2005). On the Theoretical, Conceptual, and Philosophical Foundations for Research inMathematicsEducation. ZDM, 37(6), 457-467.
88. Levi, M., Morgan, J., & Burrows, J. (2003). Enhancing business crime reduction: UK directors' responsibilities to review the impact of crime on business. Security Journal, 16(4), 7-27.
Levy, M., & Powell, P. (2005). Strategies for growth in SMEs: The role of information and information

89. Lewis, M., Brandon-Jones, A., Slack, N. & Howard, M. (2010). Competing through operations and supply. International Journal of Operations & Production Management, 3010, 1032-1058.
90. Li, T. & Calantone, R.J. (1998). The Impact of Market Knowledge Competence on New Product Advantage: Conceptualization and Empirical Examination. Journal of Marketing, 624, 13.
91. Lichtman, M., 2013. Qualitative Research In Education : A User's Guide. Los Angeles: SAGE, pp. 1-368.
92. Lincoln, Y. S. and Guba, E. G. (1985) Naturalistic Inquiry. Beverly Hills, CA: Sage.
93. Loch, K. D., Carr, H. H. and Warkentin, M. E., 1992. Threats to information systems: today's reality, yesterday's understanding. MIS Quarterly, pp. 173-186.
94. Lyons, P. & Brennan, L. (2019). Assessing Value From Business-to-Business Services Relationships: Temporality, Tangibility, Temperament, and Trade-Offs. Journal of Service Research, 221, 27-43.
95. Maisey, M., 2014. Moving to analysis-led cyber-security. Network Security, pp. 5-12
96. Makadok, R. (2001). Toward a synthesis of the resource-based and dynamic-capability views of rent creation. Strategic Management Journal, 225, 387-401.
97. McMillan, J. H., & Schumacher, S. (2001). Research in education: A conceptual introduction. New York: Longman.
98. McWilliams, A. & Siegel, D.S. (2011). Creating and Capturing Value. Journal of Management, 375, 1480-1495.
99. Miles, M. B. and Huberman, A. M. (1994) Qualitative data analysis. 2nd ed. London: Sage.
100. Minichiello, V., Aroni, R., Timewell, E., and Alexander, L. (1995) In-depth interviewing: Principles, techniques, analysis. Melbourne: Longman Australia.
101. Mintzberg, H. (1979) An emerging strategy of direct research. Administrative Science Quarterly, 24, pp. 105–116.
102. Montesino, R. and Fenz, S., 2011. Information security automation: how far can we go?. In Availability, Reliability and Security (ARES), 2011 Sixth International Conference on IEEE, pp. 280-285.
103. Mörtberg, C., Bratteteig, T., Wagner, I., Stuedahl, D., and Morrison, A., 2010. Methods that matter in digital design research. In: I. Wagner, T. Bratteteig, & D. Stuedahl, (eds). 2010. Exploring digital design. London: Springer Verlag. pp. 105-144.
104. Myers, C. B. (2001) A case in case study methodology. Fields Methods, 13(4), pp. 329-352.
105. Myers, C. B. (2001) A case in case study methodology. Fields Methods, 13(4), pp. 329-352.
106. Myers, M. and Avison, D., 2002. Qualitative research in information systems. Thousand Oaks, CA: Sage Publications.
107. Myers, M. and Avison, D., 2002. Qualitative research in information systems. Thousand Oaks, CA: Sage Publications.
108. Oates, B. J. (2006) Researching information systems and computing. Sage Publications Limited.
109. Order, E. (2013). Improving critical infrastructure cybersecurity. issued February, 12.
110. Patton, M. Q. (2001) Qualitative evaluation and research methods. 3rd ed. Thousand Oaks, CA: Sage Publications, Inc.
111. Performance of Global New Product Development Programs: A Resource-Based View. Journal of Product Innovation Management, 245, 419-441.
112. Putnis, P. and Petelin, R. (1996) Professional Communication: Principles and Applications. Prentice Hall. Quattrociocchi, W., Caldarelli, G., & Scala, A. (2014). Self-healing networks: redundancy and structure. PloS one, 9(2), e87986.
113. Ravitch, S. M. & Carl, N. M. (2016). Qualitative Research: Bridging the Conceptual, TheoreticalandMethodological. LosAngeles, U.S.A.:SAGEPublications,Inc

114. Richardson, R., 2008. CSI computer crime and security survey. Computer Security Institute, pp. 1-30
115. Rodriguez, C. and Martinez, R., 2013. The Growing Hacking Threat to Websites: An Ongoing Commitment to Web Application Security. Frost & Sullivan, pp. 1-25.
116. Ryan, G. W. and Bernard, R. (2000) Data management and analysis methods. In: Denzin, N. K. & Lincoln, Y.S. (Eds.), Handbook of qualitative research (2nd ed.), pp. 769- 802, Thousand Oaks, CA: Sage.
117. Saunders, M., Lewis, P. and Thornhill, A. (2009) Research Methods for Business Students. 5th ed. Prentice Hall: London.
118. Silverman, D. (2006) Interpreting Qualitative Data. 3 rd ed. London: Sage.
119. Sinclair M. (2007) Editorial: A Guide to Understanding Theoretical and Conceptual Frameworks.EvidenceBasedMidwifery 5(2):39
120. Siponen, M. (2006). Information security standards focus on the existence of process, not its content. Communications of the ACM, 49(8), 97-100.
121. Sommestad, T., Ekstedt, M. and Johnson, P., 2009. Cyber security risks assessment with Bayesian defense graphs and architectural models. In System Sciences, HICSS. 42nd Hawaii International Conference on IEEE, pp. 1-10
122. Spradley, J. P., 1979. The ethnographic interview. For Worth, TX: Holt, Rinehart and Winston.
123. Tellis, W. (1997) Introduction to case study. The Qualitative Report, 3(2)
124. Von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97-102. doi:http://dx.doi.org/10.1016/j.cose.2013.04.004
125. Walsham, G., 1995. Interpretive case studies in IS research: nature and method. European Journal of Information Systems, 4(2), pp. 74–81.
126. Weill, P. and Ross, J. W., 2005. IT governance: How Top Performers Manage IT Decision Rights for Superior Results. International Journal of Electronic Government Research, 1(4), pp. 63-67.
127. Wilkinson, S. (2000) Women with breast cancer talking causes: comparing content, biographical and discursive analyses. Feminism & Psychology, 10(4), pp. 431-460
128. Williams, C. (2007). Research Methods. Journal of Business & Economic Research, 5 (3), 65–72.
129. Wolcott, H. F. (1994) Transforming Qualitative Data: Description, Analysis and Interpretation. Thousand Oaks: Sage Publications.
130. Yin, R. K. (2009) Case Study Research: Design and methods. 4th ed. Applied Social Science Research Methods, Vol. 5. Sage Publications, Thousand Oaks, CA.
131. Yin, R., 2009. Case study research: design and methods. 4th ed. Thousand Oaks: Sage