A review of the IT security literature: Insights for practice for developing nations

Idris Fagbemi

Illinois Institute of Technology

A review of the IT security literature: Insights for practice for developing nations

Abstract

Cyber Security plays a critical role in the field of information technology. Securing the information has become amongst the biggest challenges in the present day. When thinking about IT security, the first thing that often comes to mind is “cybercrimes” that are increasing significantly daily. The different companies and governments are taking many measures towards preventing cybercrimes (Ndoh-Baidoo, Osatuyi, & Kunene, 2014). Nonetheless, cyber security remains a big concern to many, especially in developing nations. The paper mainly focuses on reviewing IT security literature for developing countries. The discussion further focuses on the latest information concerning IT security techniques, trends, and ethics that are increasingly changing the face of cyber security.

Key Words: Cyber security, social media, cybercrime, android apps, cloud computing.

Introduction

Presently, people are capable of sending and receiving any form of data that include e-mail or video only by clicking a button. However, the question that remains encompasses the safety of the data id that is transmitted or sent from one party to another. The answer lies in cyber security (Yeh, et al., 2018). Internet is rather the fastest growing infrastructure in everyday life. Within the modern technical environment, the majority of the latest technologies are increasingly changing the face of the humankind. However, because of the emerging technologies, people are incapable of ensuring effective safeguarding of private information and thus the apparent increase in cybercrimes. Presently, more than 60 percent of the total commercial transactions are conducted online; hence, the field requires a high quality of security for transparent and best transactions. The scope of cyber security does not just entail securing information in IT but also to different other fields that encompass the cyberspace.

Even the latest technologies that encompass net banking, E-commerce, mobile computing, and cloud computing also require a high level of security. The need for safety for these technologies draws from the fact that they often hold some vital information concerning individuals (Ambira, 2017). The effective enhancement of cyber security and protection of the critical information infrastructures remain vital for the security and economic wellbeing of every nation. Making the internet safer has become integral to the development of novel technologies and services as well as government policy. The fight against cybercrimes requires a more reliable and comprehensive approach. Presently, governments and the majority of the nations are increasingly ensuring the enforcement of strict laws on cyber securities towards preventing the loss of valuable information. The paper mainly reviews the IT security literature to gain insights concerning the practice for the developing nations, particularly Kenya.

Research Objectives

The Kenyan based SMEs are highly reliant on IT for their businesses operations; hence the risk posed by the failure of IT security tends to be significantly high. The main objective of this study entails establishing the perceived significant threats to information system assets in small and Medium Enterprises (SMEs) and the practices put in place to protect the information security assets. The information is critical for identifying the gaps that can be used to sensitize the SME managers concerning the security measures that should be put in place. The information will further assist the security service providers in determining the type of security services and products that should be developed and offered to the SMEs.

The specific objectives include:

- Identifying the extent to which the Kenyan SMEs relay on ICT
- Identifying the most prevalent security threats amongst the Kenyan SMEs
- Identifying the approaches adopted by the Kenyan SMEs to protect their networks, computers, and data from information security risks

Research Questions

- To what extent are the selected financial institutions reliant on the ICT systems?
- What are some of the prevalent threats to these organization's Information systems assets?
- What measures have been established by the different organizations to protect their information systems against these threats?

Literature Review

Cybercrime

Cybercrime is a term that is commonly used to refer to the diverse forms of illegal activities that use the computer as its primary means of commission or theft. The US Department of Justice expands the definition of the term to include the diverse illegal activities that use the computer for storage of evidence (Wallden & Kashefi, 2019). The growing list of cybercrimes encompasses the crimes that have been facilitated by computers such as network intrusions and the dissemination of the computer viruses alongside computer-based variations of existing crimes such as terrorism, bullying, stalking, and identity theft. The day to day technology plays a significant role in the lives of individuals, and the cybercrimes are likely to increase with the technological advancements.

Cyber Security

Privacy and security of data often serve as a top security measure that the different organizations need to take care of. The contemporary society is characterized by the maintenance of a wide range of information in digital or cyber form. The social networking sites provide a space where the users feel safe as they interact with friends and family. Concerning the home users, the cyber-criminals would continue to target social media sites to steal personal data. People need to ensure that they exercise precaution when interacting on social networking platforms and also while conducting bank transactions.

The increase in crime suggests it shows the need for increasing security measures. The study conducted by Phillips and Tanner, (2019) revealed that the majority of the organizations consider cyber-attacks a severe threat to both the data and business continuity. The study findings suggested that about 98% of the companies are maintaining or increasing their cyber security resources, and of those, half are increasing resources devoted to online attacks. A wide range of companies is increasingly preparing for when, not if, the cyber-attacks occur. Only a third of the companies are entirely confident in the security of their information and even less confident concerning the security measures of their business partners.

The majority of the SMEs mainly depend strongly on ICT to fulfill their duties. The organizations depend on a wide range of mobile applications to facilitate their activities. The study conducted by Dykstra and Spafford, (2018) revealed that there would be new attacks on the Android operating system based devices, but not on a massive scale. The fact that the tablets often share similar operating system as the smartphones imply that they will be targeted soon by some malware as those platforms. The number of malware specimens for Macs is likely to grow, though much less than in the case of the PCs. The technological advancement in contemporary society has promoted the emergence of trends that have a huge impact on cyber security.

Trends changing cyber security

Web Servers

The threat of attacks on web applications to extract data or distribute malicious codes persists. The cyber criminals often engage in the distribution of their malicious codes through legitimate web servers that they have compromised. Nonetheless, data-stealing attacks, the majority of which often get the attention of the media also serves as a significant threat to cyber security. There is a necessity for a greater emphasis on protecting web applications and web servers. The web servers often serve as the best platforms for cyber criminals to perpetrate their heinous activities. Therefore, there is a necessity for promoting safe browsing, especially in instances that involve some of the rather essential transactions to avoid falling as prey for these crimes.

Cloud computing and its services

In contemporary society, all the small, medium, and large companies are increasingly adopting cloud services. The world is slowly moving towards the clouds. The trend presents a significant challenge for cyber security as traffic can go around traditional points of inspection. Furthermore, as the number of applications that are available in the cloud grows, the policy controls for cloud services and web applications need to evolve towards preventing the potential loss of valuable information (Tarlow, 2019). Although the cloud services are increasingly focusing on developing their models, there remains a lot of issues concerning their security that require attention. Cloud bears the potential of providing vast opportunities, but it should be noted that as the cloud evolves, so is the increase in security concerns.

APT's and targeted attacks

The Advanced Persistent Threat (APT) encompasses a whole new level of cybercrime ware. For years, the network security capabilities that incorporates IPS or web filtering have played a significant role in facilitating the identification of such targeted attacks. As the attackers increasingly grow bolder and employ more vague techniques, network security must integrate with other security services to facilitate their ability to detect attacks. Therefore, there is the necessity for the diverse organizations ensuring that they improve their security techniques to prevent more threats coming into the future.

Mobile Networks

Presently, people can communicate in any part of the globe. However, for these mobile networks, security remains of great concern. The recent years have seen the firewalls, and other security measures become more porous as individuals are using devices that include PCs, tablets, phones, and other portable devices all of which require extra securities besides those that are present in the applications that are used (Lacity, Khan, & Willcocks, 2009). There is a necessity for thinking about the security issues associated with mobile networks. Furthermore, it is worth noting that the mobile networks are highly prone to the cybercrimes hence the need for a lot of care in case of their security issues.

IPv6: New internet protocol

IPv6 is the novel Internet protocol that is replacing IPv4 that has served as the backbone of the networks that are used in general and the Internet at large. Protecting IPv6 does not just entail porting IPv4 capabilities. Although IPv6 is a wholesale replacement aimed at increasing the available IP addresses, there are some very fundamental changes to the protocol that requires consideration in security policy. Therefore, it is always advisable to switch to IPv6 as soon as possible to ensure the effective reduction of the risks associated with cybercrime.

Encryption of the code

Encryption entails the process of encoding messages or information in such a way that hackers or eavesdroppers are incapable of reading it (Miedema, 2018). In the encryption scheme, the information or message is often encrypted using an encryption algorithm that in turn converts it into unreadable ciphertext (Dawson, Walker, & Cleveland, 2018). Such is usually achieved by using an encryption key that specifies how the message is to be encoded. Encryption at the very beginning level remains crucial for protecting data integrity and privacy. However, more use of encryption introduces more challenges to cyber security. Encryption is commonly adopted for protecting data in transit; for instance, data is transferred through wireless intercoms, telephones, and wireless microphones. Therefore, encrypting the code often enable one to know if there is any leakage of information.

The role of social media in cyber security

As individuals increasingly become social within the more connected globe, diverse organizations must find new ways of protecting personal information. Social media plays a significant role in cyber security and is likely to contribute a lot in personal cyber threats (Tarlow, 2019). The adoption of social media amongst the personnel is skyrocketing, and so is the threat of attacks. The fact that social networking sites serve as the most commonly used platforms daily implies their becoming a huge platform for the cybercriminals for hacking private information and stealing valuable data.

In the world whereby individuals are quick to give their personal information, there is the necessity for the diverse companies ensuring that they are just as quick in identifying threats, responding in real time, and avoiding a breach of any kind. Since these social media easily attract people, hackers often use them as bait to get information and the data that they require. Therefore, there is the necessity for individuals ensuring that they take the appropriate measures, especially in dealing with social media towards preventing the loss of their information. The ability of individuals to share information with an audience of millions is at the heart of the particular challenge that social media presents to the diverse organizations. Besides giving people the power to disseminate commercially sensitive information, social media also grants the same power to spread false and damaging information.

Cyber security techniques

Access control and password security

The concept of username and password has often served as the fundamental way of protecting information. The approach thus serves as the commonly adopted technique for ensuring cybersecurity.

Authentication of data

There is usually the need for ensuring that the documents that people receive are authenticated before downloading. The authentication process mainly encompasses checking if the documents originated from a trusted and reliable source and that they are not altered (Dawson, Walker, & Cleveland, 2018). Authentication of the documents is commonly carried out by anti-virus software installed in the devices.

Malware scanners

The malware scanners encompass the software that scans all the files and documents that are present in a particular system for malicious code or harmful viruses. The Trojan horses, viruses, and worms are amongst the malicious software that is regarded as malware.

Firewalls

A firewall is a software program or piece of hardware that assists in screening out worms, hackers, and viruses that try to reach the computer over the internet. The messages that enter or leave the internet often pass through the firewall that is present (citation). The firewall usually examines each message and blocks those that do not meet certain security criteria. The firewalls thus play a significant role in detecting malware.

Methodology

The preferential methodology for this study mainly encompasses interviews. The interviews serve as a qualitative research technique that involves interviewing a small number of respondents to explore their perspectives on a particular idea, program, or situation (KJÆRGAARD & LUND, 2017). There are three commonly adopted forms of interviews: structured, semi-structured, and unstructured. The structured interviews mainly encompass a series of predetermined questions that all interviewees answer in the same order. Data analysis is usually straightforward as the researcher bears the potential of comparing and contrasting the different answers given to the same question. The unstructured interviews are rather least reliable from a research viewpoint. The unreliability of the unstructured interviews draw from the fact that no questions are prepared before the interview, and data collection is often conducted informally. The unstructured interviews are often associated with a high level of bias and comparison of answers given by the different respondents is usually challenging because of the existing differences in the formulation of questions (Vitunskaite, Brandstetter, & Janicke, 2019). On the other hand, the semi-structured interviews often contain the components of both the structured and unstructured interviews. The semi-structured interviews often see the interviewer prepares a set of similar questions to be answered by all interviewees. At the same time, additional questions might be asked during interviews to clarify and further expand certain issues.

The choice of interviews as the preferred method of this study draws from the fact that it is associated with numerous benefits. The interviews often ensure that the researcher collects detailed information concerning the research. The interviews as a primary method of data collection usually grant the researcher direct control over the flow of the process, and they have a chance of clarifying certain issues during the process when necessary. Nonetheless, it is worth noting that the approach is associated with some drawbacks. The notable drawback associated with interviews as the primary data collection method encompasses the fact that the method includes longer time requirements and difficulties associated with organizing the appropriate time with perspective sample group members to conduct the interviews.

Study Design

The study mainly focused on investigating the practice for IT security in developing nations, particularly Kenya. The researcher thus opted for telephone interviews as the preferred method of data collection. The researcher first conducted an internet search of the reputable SMEs in Kenya and selected 10 of them. The researcher proceeded to send emails to various companies asking their willingness to participate in the study using the contact information presented in their respective web pages. Five of the companies responded positively to which the researcher scheduled telephone interviews with their respective managers. Out of the ten companies selected for the study, five participated, indicating a response rate of 50%. The semi-structured interviews seemed like the appropriate method of collecting the necessary data for the study. The telephone interviews were selected because of its numerous benefits that include the fact that it ensures the quick collection of the necessary data for the study. Furthermore, the majority of individuals usually have phones; hence, it provides an ample audience for gathering a representative sample. The telephone interviews, coupled with the semi-structured interview questions, played a critical role in facilitating the creation of personal touch that, in turn, led to the collection of valuable information for the study. Telephone interviewing is also cost-effective as opposed to other methods. The study mainly focused on the IT security amongst the SMEs in Kenya towards gaining insight on cyber security in the developing nations.

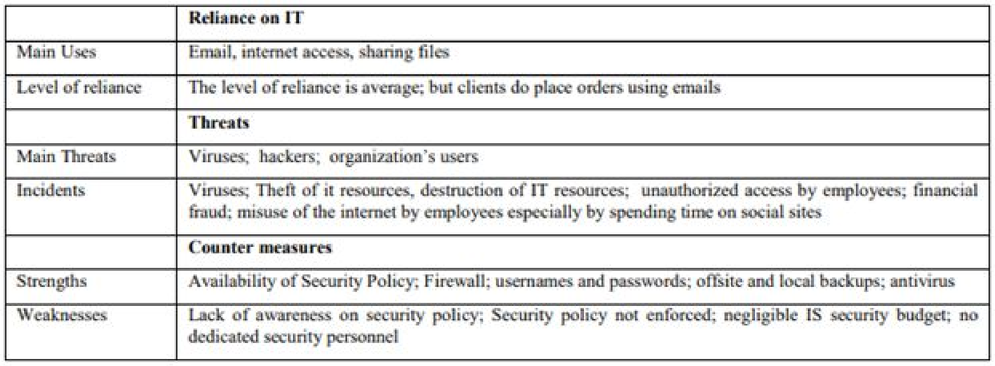
Data Analysis

Qualitative data analysis of the data was conducted. The primary objective of the analysis mainly encompassed identifying the recurring themes in data and group these into categories. The other objective entailed finding out the importance assigned to the previously identified issues by organizations. The telephone interviews were conducted to find out the presence of commonality between the efforts put forth by the different organizations in ensuring cyber security.

Results

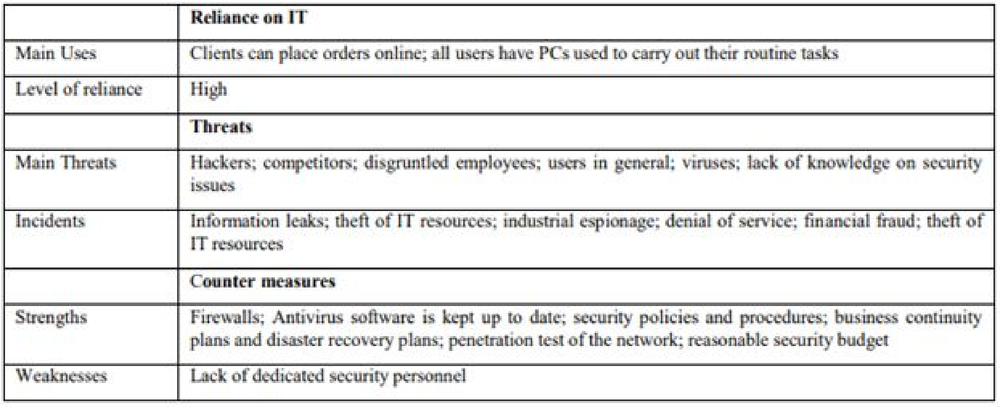
The following tables presents summaries of the information drawn from the interviewees concerning the various organizations that they serve.

Table 1. Small Financial Services Company



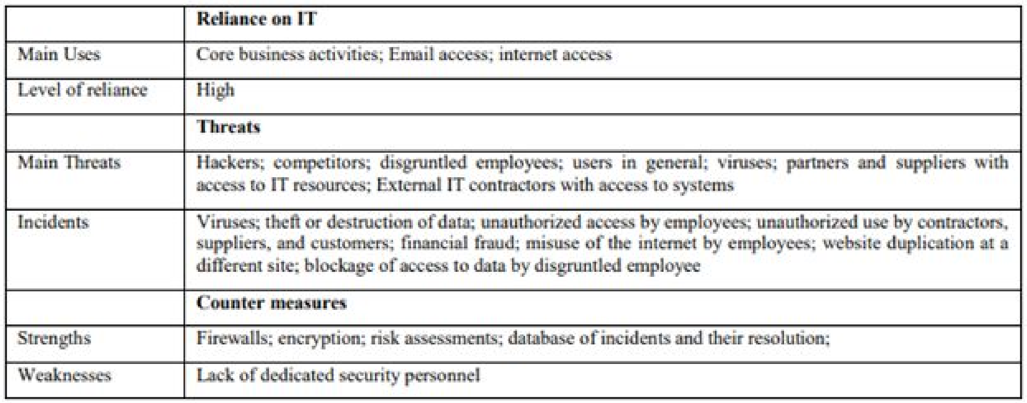
	Reliance on IT
Main Uses	Email, internet access, sharing files
Level of reliance	The level of reliance is average; but clients do place orders using emails
	Threats
Main Threats	Viruses; hackers; organization's users
Incidents	Viruses; Theft of it resources, destruction of IT resources; unauthorized access by employees; financial fraud; misuse of the internet by employees especially by spending time on social sites
	Counter measures
Strengths	Availability of Security Policy; Firewall; usernames and passwords; offsite and local backups; antivirus
Weaknesses	Lack of awareness on security policy; Security policy not enforced; negligible IS security budget; no dedicated security personnel

Table 2. Investment Bank



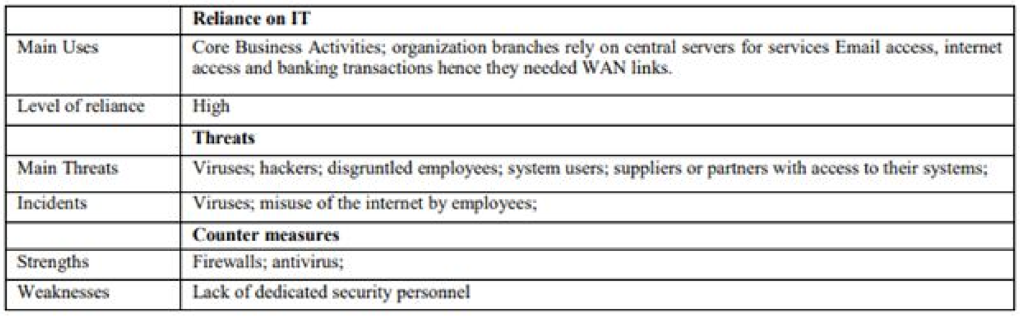
	Reliance on IT
Main Uses	Clients can place orders online; all users have PCs used to carry out their routine tasks
Level of reliance	High
	Threats
Main Threats	Hackers; competitors; disgruntled employees; users in general; viruses; lack of knowledge on security issues
Incidents	Information leaks; theft of IT resources; industrial espionage; denial of service; financial fraud; theft of IT resources
	Counter measures
Strengths	Firewalls; Antivirus software is kept up to date; security policies and procedures; business continuity plans and disaster recovery plans; penetration test of the network; reasonable security budget
Weaknesses	Lack of dedicated security personnel

Table 3. Investment Bank



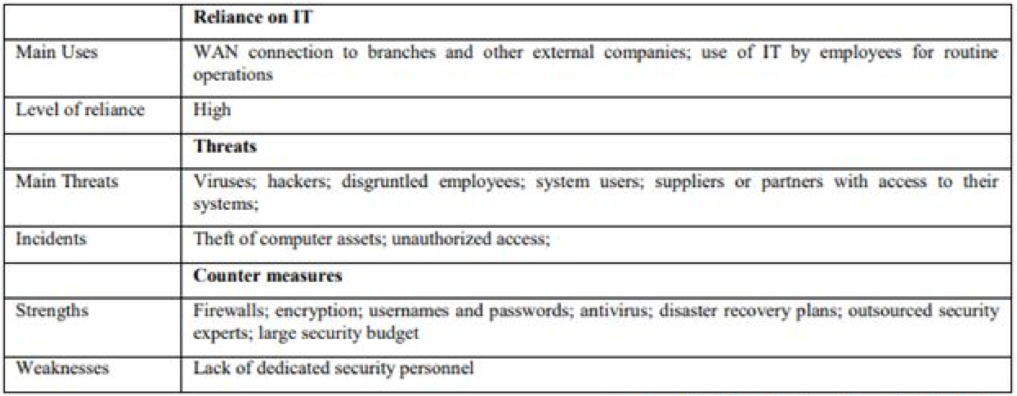
	Reliance on IT
Main Uses	Core business activities; Email access; internet access
Level of reliance	High
	Threats
Main Threats	Hackers; competitors; disgruntled employees; users in general; viruses; partners and suppliers with access to IT resources; External IT contractors with access to systems
Incidents	Viruses; theft or destruction of data; unauthorized access by employees; unauthorized use by contractors, suppliers, and customers; financial fraud; misuse of the internet by employees; website duplication at a different site; blockage of access to data by disgruntled employee
	Counter measures
Strengths	Firewalls; encryption; risk assessments; database of incidents and their resolution;
Weaknesses	Lack of dedicated security personnel

Table 4. Investment Bank



	Reliance on IT
Main Uses	Core Business Activities; organization branches rely on central servers for services Email access, internet access and banking transactions hence they needed WAN links.
Level of reliance	High
	Threats
Main Threats	Viruses; hackers; disgruntled employees; system users; suppliers or partners with access to their systems;
Incidents	Viruses; misuse of the internet by employees;
	Counter measures
Strengths	Firewalls; antivirus;
Weaknesses	Lack of dedicated security personnel

Table 5. Commercial Bank



	Reliance on IT
Main Uses	WAN connection to branches and other external companies; use of IT by employees for routine operations
Level of reliance	High
	Threats
Main Threats	Viruses; hackers; disgruntled employees; system users; suppliers or partners with access to their systems;
Incidents	Theft of computer assets; unauthorized access;
	Counter measures
Strengths	Firewalls; encryption; usernames and passwords; antivirus; disaster recovery plans; outsourced security experts; large security budget
Weaknesses	Lack of dedicated security personnel

Discussion

In all the interviews that were conducted, the viruses were regarded as a significant threat to the Information Assets. The system users, especially the disgruntled system users, were also considered as a significant threat. The hackers were also considered as a threat with all the respondents admitting to the fact that their organizations had ensured the effective placement of firewalls. The results also showed some efforts put forth by the different organizations towards ensuring the effective development of security policies despite the apparent poor implementation. Furthermore, it became evident from the interviews that there is a rather low budgetary support for IT security within the majority of the organizations. The low fiscal allocation best explains the lack of dedicated security personnel within the different organizations considered in the study. The results of the study revealed that the sophistication of the security measures established seems to increase with the level of reliance of the business on IT systems.

The results of the study show the presence of awareness amongst the diverse organizations that participated in the study concerning the significance of IT security. The responses of the participants show that the organizations that they serve has placed security measured based on their reliance on IT systems. Furthermore, the results revealed that because of the nature of the organizations, the financial fraud seemed to feature prominently amongst the reported incidences. There is the necessity for the diverse organizations ensuring that they place various measures that encompass segregation of duties towards guarding against cyber-attacks.

The loss of the computer's assets further seemed like a recurring issue within the organizations in developing nations. The considerably effective controls against the problem would include an inventory of the IT assets and physical security controls. The firewalls serve as the most commonly adopted defense against hacking. Despite the effectiveness associated with firewalls at the moment, it is worth noting that it can be improved depending on the evolution of the cyber-attacks. One of the interviewees admitted to the fact that their company had hired an external organization to perform penetration tests. Such serves as an example that should be emulated by other firms that are considering the adoption of effective security measures. Additionally, the study findings revealed that the system users served as a common threat to diverse organizations. The threat associated with the system users can be easily mitigated through campaigns targeting the users towards their sensitization on the security matters.

Additionally, the study revealed that had embraced business intelligence towards reinforcing the security of their information systems. Business intelligence mainly serves as an important tool for maintaining a competitive advantage when the company is operating on a budget or running short. The business intelligence tools further remain essential in delivering information that includes reporting and consolidation that can be targeted at high value or high-impact opportunities (Smith & Ingram, 2017). Business intelligence and analytics have in the recent times proven effective for providing an opportunity to bring forth information that is rather critical for assisting the diverse organizations in making innovative and accurate decisions within the company to sustain the competitive advantage of an organization. The effectiveness of the business intelligence further draws from the significant role that it plays in improving the quality, accuracy, and insight besides suggesting new data resources within budget and operating on a tight budget while at the same time competing. The business analytics has often proven effective in ensuring that the diverse organizations remain within budget and operate on a tight budget while at the same time maintaining a competitive advantage.

Conclusion

In conclusion, the study ensured the effective provision of insight onto information security in Kenyan-based SMEs that operate in the financial sector. The study mainly focused on the reliance of the diverse organizations on ICT. The other critical aspects considered in the study pertains the information security budgets, countermeasures, actual incidents, information security, and threats. A qualitative methodology was adopted for the research that involved the collection of data through telephone interviews.

Additionally, the study findings showed the presence of efforts established by the different organizations within the country aimed at implementing security measures with amounts of effort that correlate with the level of reliance of the organization on IT. Nonetheless, the results revealed that the limited budgets and personnel seemed to be a major handicap in the efforts aimed at improving the information security within the diverse organizations. Additionally, it became apparent that the work in this area could include attempting to find out the value of the stolen IT resources, the worth of leaked information, and whether the information had been used by the competitors or to the detriment of the organization that lost the information.

Further work in this area could include attempts at finding out the value of the stolen IT resources, the worth of the leaked information and whether the data was used by the competitors or to the detriment of the organization that suffered a breach of its data. The value of the money lost through financial fraud also necessitates investigation towards finings out the seriousness of the issue. Further studies should also focus on investigating other sectors through the expansion of the sample size adopted towards identifying whether they face similar or different threats and the countermeasures that have been put in place.

References

Ambira, C. (2017). Optimising electronic documents and records management technologies for e-government efficiency in Kenya. *Information & Records Management Society Bulletin*, (196), 37–46. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=lxh&AN=127521156&site=ehost-live

Andoh-Baidoo, F., Osatuyi, B., & Kunene, K. N. (2014). Architecture for Managing Knowledge on Cybersecurity in Sub-Saharan Africa. *Information Technology for Development*, *20*(2), 140–164. https://doi.org/10.1080/02681102.2013.832127

Dawson, M., Walker, D., & Cleveland, S. (2018). The Case for IT Training within Guinea's Ministry of Agriculture: Evaluating Performance and Usability.

Dykstra, J., & Spafford, E. H. (2018). The Case for Disappearing Cyber Security. *Communications of the ACM*, *61*(7), 40–42. https://doi.org/10.1145/3213764

KJÆRGAARD CHRISTENSEN, K., & LUND PETERSEN, K. (2017). Public–private partnerships on cyber security: a practice of loyalty. *International Affairs*, *93*(6), 1435–1452. https://doi.org/10.1093/ia/iix189

Lacity, M. C., Khan, S. A., & Willcocks, L. P. (2009). A review of the IT outsourcing literature: Insights for practice. *The journal of strategic information systems*, *18*(3), 130-146.

Miedema, T. E. (2018). Consumer Protection in Cyber Space and the Ethics of Stewardship. *Journal of Consumer Policy*, *41*(1), 55–75. https://doi.org/10.1007/s10603-017-9364-x

Miedema, T. E. (2018). Engaging Consumers in Cyber Security. *Journal of Internet Law*, *21*(8), 3–15. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=127811634&site=ehost-live

Phillips, R., & Tanner, B. (2019). Breaking down silos between business continuity and cyber security. *Journal of Business Continuity & Emergency Planning*, *12*(3), 224–232. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=135613396&site=ehost-live

Smith, F., & Ingram, G. (2017). Organising cyber security in Australia and beyond. *Australian Journal of International Affairs*, *71*(6), 642–660. https://doi.org/10.1080/10357718.2017.1320972

Tarlow, P. (2019). The Human Side of Cyber Security Breaches. *International Journal of Safety & Security in Tourism/Hospitality*, *20*, 1–4. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=hjh&AN=137083616&site=ehost-live

Vitunskaite, M., He, Y., Brandstetter, T., & Janicke, H. (2019). Smart cities and cyber security: Are we there yet?A comparative study on the role of standards, third party risk management and security ownership. *Computers & Security*, *83*, 313–331. https://doi.org/10.1016/j.cose.2019.02.009

WALLDEN, P., & KASHEFI, E. (2019). Cyber Security in the Quantum Era. *Communications of the ACM*, *62*(4), 120–129. https://doi.org/10.1145/3241037

Yeh, E., Choi, J., Prelcic, N. G., Bhat, C. R., & Heath, R. W. (2018). *Cybersecurity Challenges and Pathways in the Context of Connected Vehicle Systems* (No. D-STOP/2017/134). University of Texas at Austin. Data-Supported Transportation Operations & Planning Center (D-STOP).