Strategy and Cyber Prevention on Small Business in Africa
(COVID-2019)

Yakubu AjijiMakeri
Kampala International University of Uganda, Kampala, Uganda

COVID-19 has resulted in cyberattacks that have caused many businesses to lose monetary assets, damage their reputation, and reduce revenue. From a broader perspective, the coronavirus crisis already provides a large surcharge on Internet traffic. Most people use it not only for shopping by default but also as a serious communication channel. In addition, there is more evidence of attempts to insert malicious code, use external suppliers and outsourced technologies, create greater threats and more vulnerabilities. Through effective IT security and protocols, active management strategies, and continuous evaluation of the company’s system, small business owners can continue to do business and protect against a potential cyber attack on the company’s network. The implications of positive social change by informing managers about the results of the study are (a) preventing or reducing cybercrime, (b) protecting customer information, and (c) preventing future breaches by implementing effective social strategies.

Keywords: cyberattacks

Introduction

As globalization grows, even small businesses can transact globally through the use of data technology (IT) and these small businesses will be vulnerable to the infiltration of their networks. Therefore, cybersecurity and cybercrime cannot be considered other regulatory content or content. Cybersecurity has become a priority for all governments around the world, and there are plenty of strategies to address the emerging security issues related to the criminal use and political abuse of ICT. African countries need to think about cybersecurity as an important national and regional issue that affects their sovereignty, the security of their communities, their national security, and even their critical infrastructure. This is not the time for security to be needed. When looking at how you are doing business, take a look at what business functions and unnecessary business functions you sometimes need. It is easy to say that everything is going on there to reduce my security needs. “In some cases, this may be correct. But there are often significant risks,” adding that hackers are looking for opportunities to infiltrate into networks that use legacy applications. The purpose of this qualitative multi-case study is to explore the management strategies of small manufacturing business owners to protect their financial assets, data, and assets against cybercrime. The results of the study contribute to the managerial strategies used by small businesses to combat cybercrime. Using strategic measures and senior management support,

Yakubu AjijiMakeri, PhD, Senior Lecturer, School of Computing and Information Technology, Kampala International University of Uganda, Kampala, Uganda.
Correspondence concerning this article should be addressed to Yakubu AjijiMakeri, Kampala International University of Uganda, Kampala, Uganda.
prevention strategies ensure the safety of the company’s assets and data for hackers. With the globalization of the business, companies conduct business transactions globally through data technology (IT), which may result in unauthorized access to their networks. The common applications of IT worldwide, companies must rely on computers, mobile phones, and other devices connected to the web. Devices are hooked up to the web through the network and wireless platforms. It allows computers to collect, store, and transmit information anywhere in the world. Transaction activities using the web, financial information, and data require complex systems of security and risk management to protect the company’s most valuable assets and data. Although many organizations are making progress in IT, cybercriminals are still finding new avenues.

**Implications for Social Change**

**Cybercrime Affects Businesses, Individuals, and Society.**

Criminalizing cybersecurity sites to buy and sell stolen data, access to infected computers, and writing tools to steal knowledge (i.e. coding programs), distributing revenue to criminals, these activities are worth billions of dollars annually, thanks to the vulnerability of network vulnerabilities, lack of strategies, operational measures for prevention, and cyber attacks. With the current age of online processing, society relies heavily on information technology to provide cybercriminals. With the deployment platform to enable potential cyberbite, the social impact of cybercrimes leads to economic disruption, consumer confidence, productivity disruptions, and infiltration of national security and hence the infiltration of the country’s infrastructure. The rise of online shopping, banking, and social media, along with the use of IT, necessitates a secure Internet environment to protect viable information from cybercrime.

**Types of Cybercrime and Business Strategies**

**The Implications of Technology and Cyberbite Start to Range**

Cybercriminals are methods of obtaining important information from the business by infiltrating the firewall of their system. Customer personnel data, financial data, and assets can cause the corporation to fail. Businesses around the world use technology to process, store, and transfer information when purchasing products or services, and have financial transactions in a matter of seconds. An important concern for companies is their ability to protect their data and financial assets from potential security risks, including the use of mobile devices. In 2013, a Target System breach stole 70 million customers’ personal information and 40 million credit cards, reflecting a lack of inaccurate IT security. This section explores cyberattacks and business strategies to prevent minor attacks and other applications that increase communication and productivity. Because it allows information for unknown or untrusted systems, it helps people make sure they are not using personal machines to access their company’s sensitive assets, unless their IT team is authorized.

**Phishing and Spam by Email**

Rashi is an email authentication service that is an area of cybercrime that affects victims. Through phishing, spam practices, and schemes, cybercriminal staff can use email to obtain financial information, and consumers and businesses are exposed to fraud and fraud. In 2009, Symantec reported 12.7 trillion spam messages, accounting for 89% of all email messages. For example, through individuals, businesses and, therefore, the financial sector, cybercriminals use the email system of victims to obtain all banking information, including usernames, passwords, telephone numbers, and ATM card numbers, by communicating with the
victim (via chat, cybercriminals) available to access. They access all available information, and then transmit the victim’s money to a separate account called the Money Mule Account, which does not need to make the transaction into digital money. Cash returns within minutes, and does not leave a trace of repeat infringement; cybercrime uses a fake website which contains the URL of the fake website, which appears to be a legitimate site. Recent online banking platforms, customers, and small businesses need to check e-mail immediately by contacting a banking company for verification to prevent victims of cybercrime.

Other forms of fraudulent behavior include cybercrime in electronic fraud, which includes hiding, drug traffic, theft, and terrorism.

**Applying for an Applied Business Problem**

**Network System Administration and Budget**

Because of so many attacks, cybercriminals need international enforcement efforts. The successful attacks of cybercriminals are recognized by businessmen around the world. The existence of globalization demands strong security measures. Small businesses need to identify cybersecurity and improve their security technologies. Cyberspace Institute is recognized by companies for their market wellbeing and sustainability for their businesses. Unfortunately, companies are struggling with an inadequate budget for cybersecurity. Small businesses do not share core values in the same way as cyber-resilient companies in large organizations, because there is a lack of cost-effective budgets and consulting professionals for leadership and processes. Layered security controls to manage security risks. Companies and individuals around the world spend billions of dollars annually on cybersecurity, and computer systems are less secure than they were a decade ago. Although many organizations use cryptography to protect financial data and assets, they experience successful cyber-attacks and breach sensitive information. Better-trained employees are more at risk because of little or no technical knowledge of complex activities.

**Computer Security and Methods**

The importance of public awareness and vulnerability to cybercrime and internet and printed report by security firm Kaspersky Lab reported that between 2012 and 2013, three to seven million people were killed by phishing attacks. The House of Lords has reported the rise of cybercrime in science and technology, calling it a “new playground” for criminal activity. Harassment has occurred, and many do not report incidents. The progression of the latest malicious code created by cybercrime demonstrates the need for Internet security and therefore denies the Internet for providing the latest laws implemented by the criminal justice system. The number of people using cyberspace is individuals for private, commercial, and legal transactions worldwide. The importance of understanding vulnerability and loss leads to the importance of the mandates of Wisdom 26 that are new rules and safeguard around the world. Cybersecurity requires the implementation of appropriate controls at the federal, state, and local government levels to cover organizations, the economy, and the public. The primary concern for many countries is cyberterrorism, which poses a threat to the destruction of facility grids, financial institutions, traffic control, and other infrastructure. The sophistication of cybercrime has increased in recent years along with the skills to freeze countries. The U.S. government should take proactive steps to prevent cyber terrorism and promote prosecution standards, especially after the 911 attack on the Planet Trade Center. The importance of prosecution of cybercriminal scans helps prevent attacks at home and abroad, and requires global cooperation between domestic criminal laws and the Stockton and Homeland Security
Department to launch a national cybersecurity unit. This section addresses cyber threats to the government and the company’s computer systems, so that when a criminal gains access to a computing system without the permission of the employer, a network is aware of cybercrime is beyond the realm of across the world.

**Cybercrime Strategies and Systems Thinking and Action Theory**

Globalization and technological advancements remain a priority with the way in which businesses conduct transactions in present-day society. The systems thinking and action theory contain a layered structure (i.e., subsystems) as a part of the entire system. The subsystems work together to make sure the processes of the system perform and adapt to the changing environment. By monitoring the system, either through automatic processes or by the citizenry, the system adapts to pertinent threats to permit corrective actions. The primary concern of internal technological protection strategies includes the workers, monitoring system, raising employees’ awareness, mobile devices security, and employing rigorous subcontracting processes. If a threat is understood, the management processes can deploy preventative measures to regulate and stop further damage. If a threat is new and unknown or unexpected, management processes got to answer control and repair any damages of the threat promptly noted action is significant to confront the changes in its environment and take immediate measures to guard the system.

**Screening New Employees and Monitoring**

Organizations should enlist analytical interview techniques and screening processes to make sure the honesty of recruits. These include criminal background checks, misrepresentations of educational skills, and useful interview inquiries to reduce internal cyber theft by employees, employers should consider offering competitive wages and compensation packages reported a big management problem of not monitoring employees leads to $200 billion in losses in Africa. Small businesses experience internal scams by employees through falsified invoices for regularly order goods without consent from the organization). If the organization must implement changes to the interior environment, like employee compensation packages, it can protect itself from internal failure. No two employees are alike, and therefore the social phenomena still change, creating new adaptations to switch the system and subsystems of the interior environment. Through adaptation and evolution of the system, business leaders got to inform employees of monitoring cyber activity using time stamps, security checks, monitoring use of flash drives, and malware warnings.

**Raise Awareness**

Organizations are encouraged to supply cybersecurity training programs to show employees to acknowledge inappropriate cyber activity. The training programs should teach employees about major cyber activities, 38 like phishing, phony emails, and malware intrusions. The business should encourage employees to report unusual behavior or prohibited technologies, like portable hard drives, and suspicious behavior by outside individuals, like vendors or suppliers. Organizations got to understand the system as an adaptive whole, surviving in its environment from change and potential risks. In systems thinking theory, the function of every part, when adequately linked to at least one another, needs constant monitoring of every performance through monitoring all parts of the system. Cybersecurity awareness programs and skills training is important to guard the business against potential cyberattacks and reduce the financial burden on small businesses.

**Employ Rigorous Subcontracting Processes**

Small businesses should hunt down partners and suppliers with an equivalent risk appetite and culture of
the organization. The foremost efficient strategy for defusing cyberattacks is to use the protective technologies available and resolve issues that will present opportunities for workers, partners, vendors, contractors, and suppliers. Systems not only interface with the worldwide environment, but they also interface with one another to switch security between systems, the assumptions of 1 subsystem must guarantee the security of the opposite. The goal involves strategies to interact employee programs, for instance, acceptable and unacceptable behaviors, reminding them by protecting the organization results in protecting their jobs. Implementing strict guidelines for usage of the PC system is important for the protection of the company’s data and assets.

Cloud Computing Application

Small businesses continuously seek innovations to compete within the global marketplace thanks to changes within the economic business environment. The power to use technology requires top quality and speed of data, providing a contemporary means of communication worldwide. Through this suggestion, small businesses need safe, inexpensive ways to store critical financial data. An inexpensive manner of storing and protecting financial data and assets during a technological structure is cloud computing, whereby, buying an information structure tailored for the business’s storage platform. Small businesses lack funding for technical equipment and software to guard financial assets and data, and one inexpensive choice to store vital information is cloud technology. Notably, one primary concern is that the safety and security of cloud technology. The new technology leads organizations to question the validity of the security. Utilization of the cloud promotes further attacks, because the new storage facility is a simple target for the cybercriminal thanks to security issues. Each functional part linked to others, if unstable in its environment, is going to cause internal failure, demanding constant monitoring of performance to adapt to changes affecting the entire system.

Added Value of Systems Thinking Theory and Action

The importance of the correlation between the system and therefore the subsystems of the business environment is important for the protection of the whole system. While I discussed several different subsystems within the system, cybercrime affects several other areas of concern, like firewall protection, encryption, password protection, and lots of others. Thanks to many problematical situations, business systems research is interested not only within the thinking process but also in the proactive action resulting from the thought process. The course of action taken from the invention of problems to the recovery process remains essential to take care of and sustain the business from the likelihood of failure. Four fundamental factors involved within the system, the environment, and real-world actions include the subsequent conditions: Each department is password protected and altered regularly. The organization uses encryption software for emails handling company business. The organization allows employees to attach to the general public internet. The organization expects the blueprints from its customers protected when sent to their vendors. The organization has found out tiers to limit access to the various departments, like the accounting department and human resources. The organization has limited rights to specific information, whereby, the extremely confidential material on a separate network. The organization has limits to access different departments on specific drives. The organization does have a shared drive that only incorporates worksheets and workbooks that folks are working in daily with nonproprietary of specific information, like data entry. The accounting department is on a separate network. Employees use a Key Fob to permit employees to enter the organization’s building. The organization only allows only a few employees to possess a VPN (Virtual Private Network) to attach to the networks to access corporate resources when faraway from the office. The organization hired an IT consultant who
monitors the system 24/7. Globalization and technological advancements remain a priority within the manner during which businesses conduct transactions in present-day society. The existence of cybercrime affects business, economics, and society. Many small businesses realize the reliance thereon for his or her business practices. They understand the implication of effective IT practices to stop the failure of their systems, and in some cases, failure of the business.

**Conclusion**

Small businesses must implement cybersecurity policies to prevent breaches in their system. Companies understand their responsibility in providing clearly defined policies and therefore the goal of the business is to create trust in the workforce. A major concern for companies is the ability to protect their data and financial assets from potential security risks, including the use of mobile devices and tablets. Small businesses should not be allowed to attach their personal proprietary mobile devices to the company’s network, laptop, tablet, or other company-owned devices. Connections can cause a serious infection of a company’s network. In addition, employees should not be allowed to connect their devices to the network and access the web through the company’s network. Small businesses must constantly train new strategies of cybercriminals to accept potential breaches, inform them of the latest viruses, and prepare for potential attacks. Small businesses need to implement a response plan for cyber attacks. Security threats include opening infected emails, visiting Internet shopping sites, downloading infected files, and internet banking. Safety training programs for workers can reduce the number of breaches and infections of the company’s network. The commitment of small businesses fights cybercrime not only with cybersecurity policies, but also the education of their employees across the company. Most small businesses do not hire full-time security officers for themselves or their organizations and do not budget enough money to adopt an appropriate security plan. The security challenge is the same between the system’s hardware and software, allowing organizations to revisit their system architecture. However, small businesses can create an easy safety network and as the company grows, they expand their network from the core principles of security measures. Small businesses need to implement further processes to protect their networks.

Copy important data: Small businesses must back up all data every day, including any data that is confidential and important to the business. In the case of a breach, the information should be kept from one place only. I would like to recommend removable disk drives or a dedicated network that is not connected to the web. Keep track of equipment: Small businesses must protect departmental performance, especially those with critical data. All mobile devices, laptops require constant monitoring and removal of important information, and any stolen or lost devices should be deactivated. Organizational resilience is about operating the business while fighting back and recovering. Maintaining the level of performance of the small business requires the ability to measure.

**References**

Ambachtsheer, K. P. (2016). *The future of pension management* (pp. 1-19), May, 2016.

Awan, J. H., Memon, S., Khan, R. A., Noonarit, A. Q., Hussain, Z., & and Usman, M. (2017). Security strategies to overcome cyber measures, factors and barriers. *Engineering Science and Technology International Research Journal, 1*(1), 51-58.

Conteh, N. Y., & Royer, M. D. (2016). The rise in cybercrime and the dynamics of exploiting the human vulnerability factor. *International Journal of Computer (IJC), 20*(1), 1-12.

Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity: Risks, vulnerabilities, and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research, 6*, 31-38.
Cope, D. G. (2014, January). Methods and meanings: Credibility and trustworthiness of qualitative research. *Oncology Nursing Forum, 41*, 89-91.

DeSouza, E., & Valverde, R. (2016). Reducing security incidents in a Canadian PHIPA a regulated environment with an employee-based risk management strategy. *Journal of Theoretical and Applied Information Technology, 90*(2), 197-208.

DiMasi, D., Collier, Z. A., Heffner, K., & Linkov, I. (2015). Systems engineering framework for cyber-physical security and resilience. *Environment Systems and Decisions, 35*, 291-300.

Dodge Jr, R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. *Computers & Security, 26*(1), 73-80.

Doh, J. P., Lawton, T. C., Rajwani, T., & Paroutis, S. (2014). Why your company may need a chief external officer: Upgrading external affairs can help align strategy and improve competitive advantage. *Organizational Dynamics, 43*, 96-104.

Drissel, D. (2012). Cyberspatial transformations of society: Applying Durkheimian and Weberian perspectives to the internet. *International Journal of Technology, Knowledge & Society, 8*(3), 71-86.

Dupont, B. (2017). Bots, cops, and corporations: On the limits of enforcement and the promise of polycentric regulation as a way to control large-scale 131 cybercrime. *Crime, Law and Social Change, 67*, 97-116.

Eddolls, M. (2016). Making cybercrime prevention the highest priority. *Network Security, 2016*(8), 5-8.

Elo, S., Kääriäinen, M., Kanste, O., Pölkki, T., Uttriainen, K., & Kyngäs, H. (2014). Qualitative content analysis: A focus on trustworthiness. *SAGE Open, 4*(1).

Hoekman, B., & Mattoo, A. (2007). *Trade in services and economic development, growth (Lakeland)*, No. September, 2007.

Krebs, C. (2019). 5G: The impact on national security, intellectual property, and competition. In *United States Senate*. Retrieved from: https://www.judiciary.senate.gov/imo/media/doc/Krebs%20Testimony.pdf

Lewis, & Neuneck. (2013). *The cyber index—International security trends and reality* (p. 153).

Maynard, A. D. (2015). Navigating the fourth industrial revolution. *Nat. Nanotechnol, 10*(12), 1005-1006.

Metzger, A. (2016). *Free and open source software (FOSS) and other alternative license models: A comparative analysis* (1st ed.). Springer International Publishing.

Mohideen, F. (2016). The cyber-security state of our nation: A critique of south Africans stance on cyber-security in respect of the protection of critical information infrastructure. In *11th International Conference on Cyber Warfare and Security* (p. 235), ICCWS2016.

Perry, J. (2016). Are there any Indians left in Colombia? The indigenistamovement from 1940 to 1950. *AIBR. Rev. Antropol. Iberoam., 11*(3), 363-381.