International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

Cyberthreats: Can Small Businesses in Tanzania outsmart Cybercriminals?

Erasto Kayumbe[1], Lucy Michael[2]
[1]Information Technology & Statistics Unit, Tanzania Atomic Energy Commission, Arusha, United Republic of Tanzania
[2]Human Resource Management, Institute of Social Works, Dar es Salaam, United Republic of Tanzania

Abstract— *Tanzania is one of the fastest developing countries in the East Africa where the uptake of ICTs such as the Internet and mobile technologies in Small Businesses has risen sharply in recent years. Due to challenges brought by Cyberspace, Small Businesses must balance a rapidly evolving cyber threat vista against the need to fulfill business needs, more than ever. While discussing the rationale of protecting business information, it is therefore essential to review literature on common cyberthreats, sources and their impact to Small Business, and best practices to protect Small Businesses from Cyber attack. For a successful defence against Cyber security risks, the paper presents a framework to protect Small Businesses from Cyber attacks.*

Keyword— *Small Business, Cyberthreat.*

I. INTRODUCTION

Securing cyberspace is one of today's major challenges for Small Businesses. While Information Technology has led to significant advances in interaction and commerce, particularly through the use of Internet (Agrafiotis, 2018), it also has exposed SMEs and individuals in developing countries to online cyberthreats (Kabanda et al., 2018).

Cyber-criminals increasingly target SMEs (Basie von SOLMS, 2015) because these are perceived to have the weakest defences (Karen Renaud, 2016). While larger companies have resources to address cyber security issues, small companies often do not (Berry & Berry, 2018)

Small and Medium Enterprises sector is crucial in terms of economic process in developing economies (Kadchha et al., 2016). The "Tanzania Development Vision (TDV) 2025" highlighted small and medium-sized enterprises (SME) sector as one important contributor to the country's long-term development. In Tanzania, Small businesses are crucial to stable and sustainable economic development (United Republic of Tanzania Ministry of Industry and Trade, 2012), after all it contributes hugely to employment sector as it provides equal opportunity to any group in the society to participate in economic activities, and self employment.

There is no common acceptable definition of Small Business. The European Commission defines Small Business as an enterprise that employ fewer than 50 persons and whose annual turnover or annual balance sheet total does not exceed EUR 10 million. In Tanzania, Small Business is referred to as an enterprise whose number of employees is between 5 -49 and its Capital Investment in Machinery is above Tanzanian Shilling 5million to 200million. (SME Development Policy, p.3).

95% of the businesses in Tanzania are Small and Medium Enterprises (SMEs), and they represent about 35% of the country's GDP, according to the Tanzania Chamber of Commerce, Industry and Agriculture (TCCIA).

SMEs are less concerned with challenges like security, privacy and data loss rather; they continue to show optimism in using the potential opportunities that cloud computing presents to them. (Abubakar et al., 2014)

According to Michael (2014), One of the biggest challenge facing the adoption of technology in business is security, and the study conducted by Rohn et al. (2016) revealed that most of organizations do not have adequate information controls. Further, there is little awareness about what these threats are (Gaudenzi and Giorgia, 2017). However there is no doubt that all Small Businesses considered cyber security to be important (Lewis et al., 2014).

Cyber is the fifth and new domain of warfare, after land, sea, air and space (Tripathi, 2015). While organisations and individuals are exploiting its business benefits they need to realise that cyberspace confers the same benefits on those who wish to attack them (Lagazio et al., 2014), and Small Business need to be aware of cyberthreats and establish best practices to protect them from Cyber attack in order to prepare them for the worst in cyberspace.

Being aware of cyberthreats can help the Small Business protect its money, data and electronic devices. Also customers' information, company's banking details, pricing structure, future plans, products design and manufacturing processes should be protected, as hackers can damage them after gaining access to company's network.

This article surveys the literature with a view to elucidate common cyberthreats, cyberthreats sources and their impact to Small Business, the rationale of protecting business information and best practices to protect Small Businesses from Cyber attack.

Common Cyber Threats to Small Businesses

Cyber threat is defined as any "possibility of a malicious attempt to damage or disrupt a computer network or system" (Tarja and Martti, 2017). The U.S. Chamber of Commerce identifies the Common threats to business information which are hacking and malware, lost or stolen physical storage media, insider threat and human error, accidents and natural disasters. These threats are dangerous to all businesses including Small Business.

Other common threats to Small Businesses include ransomware, viruses and worms, phishing, trojan, spyware,

Erasto Kayumbe and Lucy Michael, "Cyberthreats: Can Small Businesses in Tanzania outsmart Cybercriminals?," *International Research Journal of Advanced Engineering and Science*, Volume 6, Issue 1, pp. 141-144, 2021.

cookies, Denial of Service, Business Email Compromise and cryptocurrency mining

Source of Cyber Threats to Small Businesses

Most security professionals would agree that the famous WWII idiom "loose lips sink ships" still holds true and that people are the main cybersecurity threat (Paulsen, 2016). The human element forms the core of cyber-attack and is the weakest link (Venkatachary et al, 2017, Bernik, 2016) which may be linked with lack of training and knowledge on cyber crimes (Agrafiotis et al, 2018, Robert & Wolfe, 2015). Little awareness about cyber threats and security are also sources of an attack (Gaudenzi and Giorgia, 2017, Alotaibi et al, 2016).

Other sources of Cyber threats include spending more time on other business matters and less on IT security and using old version systems without updating (Robert & Wolfe, 2015). Weaker practices such as creating easy passwords is also considered to be one of the sources of cyber attacks. (Alotaibi et al, 2016)

The Impact of Cyber threats to Small Businesses

The new digital age has made Cyber-attacks present a growing threat to businesses. It is of this concern that Small Businesses be aware of this type of attack by getting the right information to stay protected.

According to Score Association (2020), 60% of small businesses that fall victim to an attack shut down within six months after the breach. While that may be the most devastating result of the attack, there are other consequences that a business could experience, including, financial losses from theft of banking information and disruption of business, high costs to rid the network of threats, and damage to company's reputation after telling customers their information was compromised.

A cyberattack can significantly impact a business. In fact, people feel 'confusion, discomfort, frustration' and 'worry' (Agrafiotis et al., 2018), and can also affect consumer confidence and the perceptions of the way Consumers shop online (Das & Nayak, 2013)

Best Practices to protect Small Business from Attacks

As long as it is a small business, it is vulnerable to cyberattacks. Fortunately, there are steps that can be followed to protect the business from cyberattacks.

To keep up with today's evolving threats in cyberspace, investing in technology is a crucial step in any security strategy (Bunker, 2020), but taking a cautious, responsible and long-term approach to cyber security, combined with an emphasis on firm-wide education is the most sustainable ways to a cyber security strategy in an organisation of any size.

As stated by Venkatachary et al, (2017) Careful strategies are required to mitigate the impacts of threats in the form of cyber-attack. According to Sampaio and Bernardino (2017), to control the traffic denying access to any malicious program, Firewall host-based offer the best support. As per their evaluation pfSense and ModSecurity are proposed to be the first line of defence as pfSense is the most complete open source firewall available in the market, and ModSecurity is clearly the best open source system of Web Application Firewall available with its superior number of features and capacities.

Barrett (2018) suggests a Cybersecurity framework which consists of standards, guidelines and best practices to manage cybersecurity-related risk, to promote the protection and resilience of different sectors important to economy. The Framework helps organizations understand their cybersecurity threats, reduce the risks with customized measures, and respond to and recover from cybersecurity incidents, prompting them to analyze root causes and consider how they can make improvements.

Figure 1: Cybersecurity framework (Barrett , 2018)

The U. S. Small Business Administration also provides Cybersecurity best practices for securing Small Business. Figure 2 below provides a brief summary of these practices

Cybersecurity best practices for securing small businesses

- Train your employees
- Use antivirus software and keep it updated
- Secure your networks using firewall and encryption information
- Use strong passwords
- Multifactor authentication
- Back up your data
- Secure payment processing
- Control physical access

Figure 2: Cybersecurity best practices for securing Small Business. (U.S. Small Business Administration, 2020)

Areas of Defence against Cyberthreats

There are two areas of defence against cyberthreats: the users and electronic devices. According to Score Association (2020) the best practices to keep the business safe is to create policies by incorporating the following cybersecurity practices. Table 1 and 2 below summarize the cybersecurity practices to keep the business safe.

Cybersecurity framework for Small Businesses

Small Businesses are thriving to obtain a maximum security for their systems, that's why a framework for securing Small Businesses in Tanzania is suggested. The framework in figure 3 below identifies general steps to be used in order to secure small business against cyberthreats. First assess organizational environment to identify common cyberthreats sources to your business and the ability of the organisation to deal with them cyberthreats. Second identify and define strategies for preventing and detecting cyberthreats, then train the users (employees) on how to prevent and detect cybertheats.

International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

Table 1: Best practices for user security

Passwords	○ Use a different password for every account or website. ○ Change passwords frequently—every quarter, and use long, complex passwords. ○ Don't store passwords in an obvious place like a Post-it note on computer monitor or under the keyboard. ○ Don't share the same password among users or tell others your password.
Email Security	○ Look for obvious grammar and spelling mistakes ○ Examine the email sender's address to make sure it's correct. ○ Verify before responding to an email request for sensitive data. ○ Prohibit employees from opening outside email attachments. ○ Regular phishing awareness training is vital ○ Use email encryption when sending sensitive data
Online Safety	○ When logging onto websites—especially for sensitive purpose, such as accessing bank accounts— use two-factor authentication for an extra layer of security. ○ Verify links. Be careful of links in texts or emails, even if they seem to be from someone you trust. ○ Minimize use of cloud file-sharing. Be judicious about what you share with others on sites such as Dropbox and Google Drive. ○ Never share customer information, intellectual property information or other core business data online.. ○ In general, don't overshare online—with anyone
Outside the Office	○ Be cautious using public Wi-Fi as many networks are unsecured, meaning usernames, passwords, or files that you upload or download can be captured by crooks. ○ Keep work conversations private. ○ Restrict remote access to your business network to only necessary users. ○ Close RDP ports and enforce VPN use

Best practices for user security (1Score Association, 2020)

Table 2: Best practices for device security

Computers and Servers	○ Choose a centrally-managed, business-grade antivirus (AV) security solution so you can monitor all the devices on your network, restrict user access and enforce security policies. Consumer-grade products don't provide enough protection ○ Implement multiple layers of protection. Installing AV software on your computers alone isn't enough. Look for an all-in-one cloud solution that provides endpoint, web security and email protection. ○ Isolate payment systems. Separate your point-of-sale systems or credit card readers from the rest of your network by putting them on a separate network or firewall. ○ Restrict both physical and digital access to servers. All it takes is one malicious employee to wreak havoc. ○ Require two-factor authentication to log onto servers. ○ Update software, hardware and firmware regularly; set updates to install automatically.
All devices	Whatever device people are using be sure to: ○ Change default username /password. ○ Disable remote management ○ Restrict access to specific addresses. ○ Require two-factor authentication. ○ Update device software and firmware regularly
Mobile Devices	○ Enforce passwords or passcodes on devices. ○ Take advantage of biometric identification technology if available; it's more secure than using a password. ○ Install security software on devices and other network connected devices like printers and copiers, etc.
Wireless Routers	○ Use a separate Wi-Fi network for guests. ○ Enable encryption using (WPA2).

Best practices for device security (Score Association, 2020)

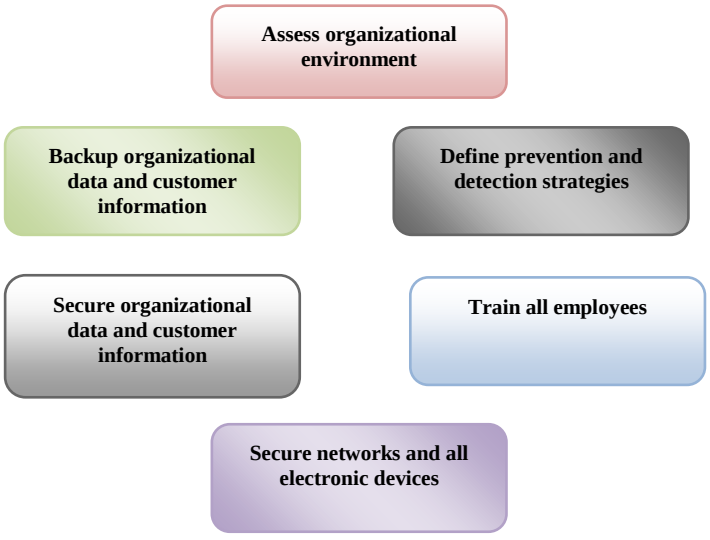

Figure 3: Cybersecurity framework for Small Businesses in Tanzania

Erasto Kayumbe and Lucy Michael, "Cyberthreats: Can Small Businesses in Tanzania outsmart Cybercriminals?," *International Research Journal of Advanced Engineering and Science*, Volume 6, Issue 1, pp. 141-144, 2021.

After training employees secure networks, all electronic devices, organizational data and customer information using appropriate measures and affordable to the organisation, then train every employee in the organisation on how to detect a vulnerable network and an infected device. The final stage is to backup organisational data and customer information in case of any cyberattack, organisational data and customer information can be recovered.

II. CONCLUSION

Due to limited financial situation in Small Businesses in developing countries like Tanzania, to eliminate or at least to mitigate the harm of the most common threats, the Small Businesses should design a security plan based on free and open source software such as antivirus software and web application firewall systems.

Regularly Train and communicate to employees on how to avoid phishing scams by showing them the common ways attackers can infect electronic devices with malware. Also teach employees how to spot and protect against cyberthreats. Install latest security software and updates, and set them update automatically on the network. Report the scam to the authority when spotted.

If hackers are impersonating the business, notify the customers as soon as possible by reminding them not to share any personal information through email or text. If it happens the customer data was stolen help to get a recovery plan.

REFERENCES

[1] UNIDO (2013) TANZANIA SME DEVELOPMENTPOLICY 2003“ten years after” Retrieved from https://open.unido.org/api/documents/5403996/download/TANZANIA%20SME%20DEVELO

[2] A.D. Abubakar, Julian M Bass & Ian Allison Robert (2014) CLOUD COMPUTING: ADOPTION ISSUES FOR SUB-SAHARAN AFRICAN SMES, EJISDC (2014) 62, 1, 1-17

[3] Venkatachary SK, Prasad J & Samikannu R (2017) Economic Impacts of Cyber Security in Energy Sector: A Review, International Journal of Energy Economics and Policy, 2017, 7(5), 250-262.

[4] Sampaio, D. and Bernardino, J. (2017) Evaluation of Firewall Open Source Software. In Proceedings of the 13th International Conference on Web Information Systems and Technologies (WEBIST 2017), pages 356-362 ISBN: DOI: 10.5220/0006361203560362

[5] Guy Bunker (2020), Targeted cyber attacks: how to mitigate the increasing risk, Network Security, Volume 2020, Issue 1,2020,Pages 17-19, ISSN 1353-4858, https://doi.org/10.1016/S1353-4858(20)30010-6. (http://www.sciencedirect.com/science/article/pii/S1353485820300106)

[6] Berry, C.T. and Berry, R.L. (2018) ‘An initial assessment of small business risk management approaches for cyber security threats’, Int. J. Business Continuity and Risk Management, Vol. 8, No. 1, pp.1–10.

[7] United States Small Business Administration (SBA) (2020) [online] https://www.sba.gov/business-guide/manage-your-business/stay-safe-cybersecurity-threats#section-header-5 (accessed 29 December 2020).

[8] Paulsen, C. "Cybersecuring Small Businesses," in *Computer*, vol. 49, no. 8, pp. 92-97, Aug. 2016, doi: 10.1109/MC.2016.223.

[9] Salah Kabanda, Maureen Tanner & Cameron Kent (2018) Exploring SME cyber security practices in developing countries, Journal of Organizational Computing and Electronic Commerce, 28:3, 269-282, DOI: 10.1080/10919392.2018.1484598

[10] Barrett M (2018) Framework for Improving Critical Infrastructure Cybersecurity. ISA Water/Wastewater & Automatic Controls Symposium (WWAC) 8-9 August 2018, Bethesda, Maryland USA [online] http://isawaterwastewater.com/wp-content/uploads/2018/08/WWAC-2018-NIST-Barrett_final.pdf (accessed on 30th December, 2020)

[11] Score Association (2020), The Small Business Guide to Cybersecurity, [online] available at https://s3.amazonaws.com/mentoring.redesign/s3fs-public/SCORE-TrendMicro-Small-Business-Guide-Cyber-Security_0.pdf. Accessed on 30th December 2020.

[12] The U.S. Chamber of Commerce (2020), Internet Security Essentials for Business 2.0 [online] available at hts://www.uschamber.com/sites/default/files/legacy/issues/defense/files/020956_PDF_web.pdf, Accessed on 29th December 2020

[13] The European Commission (2020), User guide to the SME Definition [online] available at https://ec.europa.eu/regional_policy/sources/conferences/stateaid/sme/smedefinitionguide_en.pdf. Accessed on 10th November 2020

[14] United Republic of Tanzania Ministry of Industry and Trade, (2012), Ifahamu Sekta ya Viwanda Vidogo na Biashara Ndogo, [online] Available at https://www.tanzania.go.tz/egov_uploads/documents/Ifahamu_Sekta_ya_Viwanda_Vidogo_na_Biashara_Ndogo_sw_sw.pdf Accessed on December, 2020

[15] Riyana Lewis, Panos Louvieris, Pamela Abbott, Natalie Clewley, and Kevin Jones, 2014, "Cybersecurity Information Sharing: A Framework For Sustainable Information Security Management In Uk Sme Supply Chains", Proceedings of the European Conference on Information Systems (ECIS) 2014, Tel Aviv, Israel, June 9-11, 2014, ISBN 978-0-9915567-0-0 http://aisel.aisnet.org/ecis2014/proceedings/track14/4

[16] Ioannis Agrafiotis,*, Jason R. C. Nurse, Michael Goldsmith, Sadie Creese, and David Upton (2018) A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate, Journal of Cyber security, 2018, Vol. 0, No. 0, doi: 10.1093/cybsec/tyy006

[17] Robert, D. & Wolfe, H. B. (2015). Cybercrime Concerns and Readiness for New Zealand Businesses 2014-2015. Retrieved from http://www.citrenz.ac.nz/conferences/2015/pdf/2015CITR ENZ_1_Roberts_Cybercrime_v2.pdf

[18] Igor Bernik (2016) Cybercrime: The Cost of Investments into Protection, VARSTVOSLOVJE, Journal of Criminal Justice and Security, year 16 no. 2 pp. 105–116

[19] Faisal Alotaibi, Steven Furnell, Ingo Stengel1, Maria Papadaki (2016) A Review of Using Gaming Technology for Cyber-Security Awareness, International Journal for Information Security Research (IJISR), Volume 6, Issue 2, June 2016

[20] Karen Renaud (2016)How smaller businesses struggle with security advice

[21] Eli Rohn Gilad Sabari Guy Leshem , (2016),"Explaining small business InfoSec posture using social theories ", Information & Computer Security, Vol. 24 Iss 5 pp. 534 - 556 Permanent link to this document: http://dx.doi.org/10.1108/ICS-09-2015-0041

[22] Sumanjit Das and Tapaswini Nayak (2013) Impact Of Cyber Crime: Issues And Challenges, International Journal of Engineering Sciences & Emerging Technologies, October 2013. ISSN: 22316604, Volume 6, Issue 2, pp: 142-153

[23] Tarja, R., Martti, L. (2017), Cyber Threats Mega Trends in Cyber Space, International Conference on Cyber Warfare and Security. p323.

[24] Barbara Gaudenzi & Giorgia Siciliano (2017): Just do it. Managing IT and Cyber Risks to Protect the Value Creation, Journal of Promotion Management, DOI: 10.1080/10496491.2017.1294875

[25] Lagazio M, Sherif N, Cushman M, A Multi-level Approach to Understanding the Impact of Cyber Crime on the Financial Sector, Computers & Security (2014), doi: 10.1016/ j.cose.2014.05.006.

[26] Basie von SOLMS (2015) Improving South Africa’s Cyber Security by Cyber Securing its Small Companies, IST-Africa 2015 Conference .