The Human Side of Information Security when Technical Controls Fail

Whyte Stella Tonye[1]

[1] Walden University

Received: 12 December 2018 Accepted: 4 January 2019 Published: 15 January 2019

Abstract

The misuse of information has significantly impacted negatively on both individuals and organizations security. The technical side of security controls is critical in an organization?s security system. This paper provides insight into some information security using the human side and other measures to protect the system. The paper also describes the technical control measures that are intended to meet the protection requirements of a system. Technical controls are security controls executed in the computer system. The controls provide automated protection from unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data. Since Implementation of technical controls, however, requires significant operational considerations it should, therefore, be consistent with the management of security.

Index terms—

1 Introduction

Cybercrime is a serious business ccording to Furman, Theofanos, Choong, and Stanton (2012) each year more than 9 million U.S. residents are victims of identity theft, of which cyber attacks cost about $8 billion per year causing economic damage to the nation. Not all cybercrimes are committed by strangers as is often with phishing scams (Kirlappos & Sasse, 2012; Sheng, Holbrook, Kumaraguru, Cranor & Downs, 2010). Sometimes cybercrimes are carried out by insiders with intimate knowledge of the systems and co-workers from whom they steal. Themay not be detected by computerautomated technical controls like the fire and forget scripts alone may not detect these crimes. The human side information security is critical, apart from the applied focus on technology, achieving IT security is more than just a technical problem. There is a need to increasingly involve the active participation of human to securely design, deploy, configure, and maintain the system **??**Funel & Clark, 2012).

Nigeria now embraces technology to solve its information security challenges although faced with the upsurge in cyber terrorism and corruption. The country's stage of corruption hindered national development which has become a critical challenge factor to be considered when selecting and recruiting reliable personnel as technical controls. It is important to understand that human elements and other factors could impact global threats or undermine information and national security as well as international security in the country. The awareness of these challenges and introducing appropriate policy and training will provide critical guidance to Nigeria information security and other developing countries in a way that could lead to significant long-term improvements in information security management, procedures, the overall security of facilities, organizations infrastructure, and prevent risks that may be posed by these challenges. Organizations should implement SETA programs to detect and reduce technical control failures using the human side to effect safe, secure, and unhindered application of information security **??**Dahunsi, Ariyo, Stainback, and Hall, 2017). The paper suggests a strategy for conducting SETA programs for National information security assessment and evaluation as steps preceding the development of a SETA program considering the rate of technical control failures across the country.

Whenever both internal and external controls are implemented lackadaisically, there is always a huge financial loss in an organization. Risks occur when management does not understand the technical controls they have put in place or adequate staff maintenance of these controls.

Cases of internal fraud occurs when poor trading mistakes are made by investors who could not admit their mistakes on bad business decisions. Over 90 Nigerian banks with state government's participation and privately owned banks failed in the 1990s as a result of excessive operating expenses, inadequate credit administration, interest rate speculation, asset mismatching, weak controls, fraud and forgeries an overtly aggressive growth policy abandonment of prudent banking, persisted in those banks (Ugoani, Amu, & Emenike, 2014). According to Dhillon & Moores, (2001), Toshihide Iguchi, a bond trader of Japan's Daiwa Bank for the New York office made trading mistakes that lead to over $1.1 billion in accumulated losses from 1984 through 1995, which he felt he could not admit. As the losses mounted, so did his cover-ups and exploitation of Daiwa's poor information security and accounting controls. Eventually, the Federal Reserve and U.S. Attorney's Office got involved once the scandal broke in the news, and Daiwa Bank lost its charter to do business in the U.S.

2 Examples of some

3 Summary

In summary, the lessons derived from the lapses from the above-mentioned banks is that technical controls need to be manned and reviewed by humans, automation alone cannot be relied on. Furthermore, since money is involved, formal accounting controls systems should be instituted and followed. Informal controls which are the third sets of controls are less expensive than both technical and formal controls. These controls center around increasing employee awareness, ongoing education, training, and management development programs that grow a subculture. Informal controls foster awareness of what is going on, but not be so punishing as to cause employees to refrain from admitting when they make mistakes.

Businesses can do a few other things to reduce insider threats, this can be done by (i) hardening the financial systems; (ii) increase logging and reduce anonymity; (iii) reduce stress and frustrations (iv) assist and implement compliance; and (v) dismantle peerpressure to prevent cover-ups in the workplace. (Willison, 2006). Ironically, while some humans make mistakes, others can also catch some of these mistakes better than some forms of automation. Nevertheless, the insider threat is always present and likely will be with us for quite some time. However, when designing and deploying security solutions for organizations, it is important to take the user into consideration. To protect company assets, it is important to secure hiring practices, roles, policies, standards, guidelines, procedures, risk management, awareness training, and management planning must all contribute to protecting assets. The use of these security structures provides some protection from the threat humans present against your security solutions.

Iterating from Furman, Theofanos, Choong, and Stanton's (2012) article, participants were already acquainted with the security symbols and trust marks although Kirlappos and Sasse (2012) expressed that security training on phishing offers little assurance to clients who survey a possibly pernicious site in this attitude. Security instruction needs to consider the drivers of customer conduct, in this circumstance the prompts consumers search for and how they decipher them. Successful security awareness, education, and preparing must accomplish more than caution clients of perils they should focus on the confusions that underlie consumer activities. Even though we concentrate on phishing, a leap of change could help security scientists and specialists grow more robust security training, instruction, and preparation in different ranges of computer security. Instructive campaigns should first comprehend clients' impression of computer and online security for it to be compelling (Furman et al., 2012). Current instruction and preparation endeavors do not make impacts because they expect that clients are quick to stay away from risk and hence prone to embrace practices that may secure them. Cybercriminals just post their website with malevolent substance on the web, and then utilize site design improvement procedures to have it ascend to the top when you look at the invented organization. More robust training must be carried out to supplement any specific anti-phishing measures to enhance clients' capacity to recognize phishing locales. Compelling security training needs to test clients' presumptions about trust signals and their choice procedures and supplant them with trust signs and systems for surveying risk in an online situation (Kirlappos et al., 2012).

The initial move toward viable client instruction is to perceive that awareness, training, and preparation is the three particular strides procedure to enhance client ability. Clients should be pulled to considerations and to help them understand that there are issues that may influence them. Training is an important step to make clients responsive to instruction and preparation measures. The use of solid visual components or silliness should be utilized to catch clients attention to enable security awareness (Kirlappos et al., 2012). Having a workforce taught and more attentive of security regions resemble growing the Information Security division into the entire organization. It gives the Security Director or Chief Information Security Officer (CISO) a more extensive base of mental aptitude in which they can tap if necessary. Completing a security education training and awareness (SETA) programme can be seen as a piece of risk administration. By incorporating security and risk management into the organization and its continuous procedures, these vital capacities will turn into a method for working together. By having uneducated workers, an organization is going out on a limb inputting the security of the whole association under the control of not very many security experts that can't ultimately secure the data with just the assistance of innovation. This risk can significantly minimize through the execution of an effective SETA program (Hight, 2005).

Users should receive training when they first enter an organization, and they should receive periodic refresher training, even if it's just an email from the administrator reminding them of the threats. The human side of information security is significant, though in spite of the implied focus upon technology, achieving IT security is more than just a technical problem, there is a need to increasingly involve the active participation of human to design, deploy, configure and maintain systems securely. (Furnell & Clarke, 2012).Fundamental controls are significant to our networks, but they are not complete without the human side of information security. Since the devices and infrastructure, we use to share and retrieve information has changed the way we protect this information and the users who depend on them should also change (Thompson, 2013). Fundamental controls like antivirus, firewalls, and online security are not enough and as important and sufficient as human controls. Both hackers and other information security criminals have exploited the human side of information security and so should be protected or guarded. The people who use, administer, and operate accounts in computer systems are the weakest link in the security chain.

Several organizations data have been compromised as a result of mere users bad choice of decision making as they click the email which may have links that send the user to a dangerous site in the internet or page. Sometimes using an infected USB stick, using a personal device to connect to public sites that may be difficult for organization's security detection and receiving physical mail may also be very dangerous to the organizations' data. There is always a warning on not clicking on links in emails, links are dangerous. It has been observed that humans are more at the edge while intruder and attackers are the closest to you and know you more than you think. Attackers have begun to personalizing their attacks, so we should also personalize our defense. The human element of information security should be embraced and not ignored (Thompson 2013).Furman, Theofanos, Choong, & Stanton (2012), stated that more than 9 Million US residents become victims of identity theft costing the US economy an estimate of $8 Billion a year. Humans are often unaware of the risks and therefore not equipped to use available tools to manage them. The use of protection updates, security sets, and installation of firewalls, spyware, and antivirus must be well understood and managed properly by uses of networks should be used to mitigate risks. Users need to be educated to be aware and to employ sound practices routinely. To do this and change user's perception of security, Furman et al., (2012) suggested three ways to change user's behavior. **??**010), when their users have prior exposure to phishing education, they will be less susceptibility to phishing, this means that there will be less clicking on legitimate websites and reduce giving out information that may be used by attackers. Sheng et al. iterated that gender and age are the two key demographics that predict phishing susceptibility, especially women clicking on links in phishing emails more easily than men. Women have less technical training and less technical knowledge than men; also, users at the age between 18 and 25 are much more likely to fall for phishing than the others. As participants in this age group have lower education level, and younger on the Internet so have less exposure to training materials and more susceptible to risks as stated by other researchers in Sheng et al.,'s (2010) study. The introduction of the SETA programs to provide anti-phishing education and training to high school and college students can mitigate risk.

According to the Flynn (n.d), organizations may not be able to protect the integrity availability and confidentiality of information in this present day highly networked systems environment without ensuring that its employees are involved in understanding their roles and responsibilities and are adequately trained to perform these responsibilities. Stallings and Brown (2012, 2 nd Ed.) stated that there should be an emphasis on the importance of security awareness policy document provided to all employee. This policy should be established to employees that participate in the awareness program is compulsory, and that sufficient fine will be given to all employee who does not participate in the awareness activities. The SETA program is for all users in an organization with a specific program for their jobs and level of technical expertise while the responsibility to organize this program is on the Chief Information Officer (CIO) **??**Flynn n.d). Failures in information security technical controls can be avoided or mitigated with strong Security Education, Training and Awareness (SETA) programs. The UK Office of Fair Trading launches a campaign aiming at increased consumer consciousness to make shopping websites by launching successful security awareness in websites and newsletters. The security education, training, and awareness program will do more than just warning users of dangers. These awareness programs also target the misconceptions that underline the user's action. (Kirlappos and Sasse, 2012). Organizations should also keep in mind, not to overload users with too many details and information but to help users understand their role in information securely and how they can mitigate risks, providing information early and making the programs formal. **??**Flynn, n.d).Researchers and practitioners recognize the need for business leaders to establish adequate internal control frameworks. Small and Medium Enterprises (SME) leaders lack strategies for improving internal control systems. The purpose of this case study was to explore the strategy leaders of SMEs in Nigeria use effective controls to improve internal control practices. Building on the internal control theory and transactional leadership theory, semistructured face-to-face, and phone interviews were conducted with eight purposively-selected leaders of SMEs in Nigeria who successfully implemented internal control practices. Themes that emerged from the thematic analysis of the interview data include segregation of duty; processes adherences, policies, and procedures; staffing, training, and experience; information technology; and staff empowerment and management commitment. (Aladejebi, 2017) The result of this study shows that leaders of companies in Nigeria use similar strategies for the improvement of their internal control practices.

The participants used segregation of duty and adherence to processes, policies, and procedures as strategies for improving internal control practices. Findings of this study could contribute to positive social change by providing organizations with knowledge on strategies to improve internal control practices which will minimize loss of assets and boost profitability and business sustainability. Increase in business profitability, stakeholders will increase the firms' corporate social responsibility (CSR) through payment of more taxes, and provision of employment opportunities and social amenities to the local community (Aladejebi, 2017). a) Purpose of the SETA Program 1) Improve organization security 2) Holds employees for their actions by communicating the policy to their users. 3) Encourage security feedback 4) To change employee security culture 5) Help in developing security skills and knowledge so that users can perform their jobs using IT system security 6) More awareness of the need to protect system resources. 7) To enable the employee to focus on security. b) Benefits of SETA programs 1) Improve Employee behavior.

2) Increase ability to hold employees accountable for their actions.

4 Future Consideration

Future examination ought to recognize the attituded that will help clients in building the proper cybersecurity mental models. A complete mental model would empower users to comprehend with the viability of the ways of dealing with stress and precisely assess analogies that they convey from the physical world to the virtual world (Furman et al., 2012) IV.

5 Conclusion

In conclusion, the paper discusses the technical side of Information Technology and the worry researchers, administrators, and managers have concerning insider attackers where people with legitimate access behave badly and put organization's data at risk with unwelcome consequences. A lesson was learned from the example of the Hard Disk: Naive User and Absent Policy shows that sometimes security can be threatened by well-intended insiders indicating that security education, training, and awareness program is meant for all users in an organization with a specific program for their jobs and level of technical expertise. Technical controls are only part of a total security awareness program. When information security professionals only focus on technology, the human side can often be overlooked, with potentially devastating consequences. Hackers and other information security criminals have exploited this human side at least as often as they have breached technical controls. The cost of this exploitation to organizations and individuals has been staggering. One reformed hacker, Kevin Mitnick said that companies spend millions of dollars on firewalls, encryption, and secure access devices and it's money wasted because none of these measures address the weakest link in the security chain: the people who use, administer, operate and account for computer systems **??**Cyber Attack, 2000). [1]

[1] © 2019 Global JournalsThe Human Side of Information Security when Technical Controls Fail

[Dahunsi and Olumuyiwaariyo] , Stephen Dahunsi , Olumuyiwaariyo .

[Auxier et al. ()] 'Aligning Technology, Policy and Culture to Enhance Nuclear Security: A Comparative Analysis of Nigeria and the'. John D Auxier , Ii; , Joseph Stainback , I V Ruric , Howard Hall , Lewis . http://trace.tennessee.edu/ijns/ *International Journal of Nuclear Security* 2017. 3 (1) .

[Furman et al. ()] 'Basing cyber security training on user perceptions'. S M Furman , M F Theofanos , Y.-Y Choong , B Stanton . *IEEE Security & Privacy* 2012. 10 (2) p. . (Retrieved from Walden Library Database)

[Dhillon and moores ()] 'Computer crimes: theorizing about the enemy within'. G Dhillon , S &moores . 10.1016/S0167-4048(01. *Computers & Security* 2001. 20 (8) p. .

[Stallings and Brown ()] *Computer security: Principles and practice. 2 nd Ed*, W Stallings , L Brown . 2012. Pearson.

[Flynn] *Implementing Security Education, Training, and Awareness Programs*, J Flynn . fromhttp://slideplayer.com/slide/10501090/

[Ugoani ()] 'Poor Management and Failed Banks: A Study of Banks with State Governments Participation in Nigeria'. J N N Ugoani . *International Journal of Economics, Commerce and Management United Kingdom* 2014. 2 (2) .

[Furnell and Clarke ()] 'Power to the people? The evolving recognition of human aspects of security'. S Furnell , N Clarke . *Computers & Security* 2012. 31 (8) p. . (Retrieved from the Walden Library databases)

[Kirlappos and sasse ()] 'Security education against phishing: A modest proposal for a major rethink'. I Kirlappos , M A &sasse . *IEEE Security & Privacy* 2012. 10 (2) p. . (Retrieved from the Walden Library databases)

[Olufemi ()] *Strategies for Improving Internal Control in Small and Medium Enterprises in*, A Olufemi . 2017.

[Aladejebi ()] *Strategies for Improving Internal Controls in Small and Medium Enterprises in Nigeria. Walden Dissertations and Doctoral Studies*, A O Aladejebi . Http//scholarworks.walden.edu/dissertations/4708 2017.

[Thompson ()] 'The human element of information security'. H Thompson . *IEEE Security & Privacy* 2013. 11 (1) p. . (Retrieved from the Walden Library databases)

[Hight (2005)] 'The importance of security, education, training, and awareness program'. S Hight . http://www.infosecwriters.com/text_resources/pdf/SETA_SHight.pdf *City of Raleigh*, 2005. November 2005. p. .

[Willison ()] *Understanding the perpetration of employee computer crime in the organizational context. Information and organization*, R Willison . 10.1016/j.infoandorg.2006.08.001. 2006. 16 p. .

[Nigeria and Walden] *University Dissertation and Doctoral study*, Nigeria , Walden .

[Dhillon ()] 'Violation of safeguards by trusted personnel and understanding related information security concerns'. G Dhillon . *Computers & Security* 2001. 20 (2) p. .

[Sheng et al. ()] 'Who falls for phish? A demographic analysis of phishing susceptibility and the effectiveness of interventions'. S Sheng , M Holbrook , P Kumaraguru , L F Cranor , J Downs . *CHI '10 -Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2010. p. .

[Sheng et al. ()] 'Who falls for phish? A demographic analysis of phishing susceptibility and the effectiveness of interventions'. S Sheng , M Holbrook , P Kumaraguru , L F Cranor , J Downs . *CHI '10 -Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2010. p. . (Retrieved from the Walden Library databases)