International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 7 Issue: 6 16 - 19

The Effectiveness of Cybersecurity Compliance in a Corporate Organization in Nigeria

Dr. Yakubu Ajiji Makeri
Kampala International University Uganda
School of Computing and Information Technology
Yakubu.makeri@kiu.ac.ug

Abstract: The complexity and growth also create asymmetries between attackers and their targets, and incentives that drive underinvestment in cybersecurity The Digital technologies have transformed how people socialize, shop, interact with government and do business. The World Wide Web is of made amounts of information instantly available. The smartphones have put our fingertips everywhere we go it an improvement on effectiveness cybersecurity training for end users of systems and offers suggestions about and how topManagement leaders can improve on trainingto effectively combat cybersecurity threats at the organizations. Is imperative to achieve higher end-user cybersecurity compliance; practice is accepted, as a means to increase compliance behavior in any organization. The Training can influence compliance by one or more of three causal pathways: by increasing cybersecurity awareness, by increasing cybersecurity proficiency (i.e., improve cybersecurity skills) and by raising cybersecurity self-efficacy. This includes an extensive review of the cybersecurity policies and competencies that are the basis for training needs analysis, setting learning goals, and practical training. This paper discusses opportunities for human resource (HR) practitioners and industrial and organizational (I-O) psychologists, and informationtechnology (IT) specialists, and to integrate their skills and enhance the capabilities of organizations to counteract cybersecurity threats. AnyOrganizations cannot achieve their cybersecurity goalson workers alone, so all employees who use computer networks must be trained on the skill and policies related to cybersecurity.

*****

Introduction

The idea of end-user is many scholars have repeated the weakest link in the security chain, and practitioners of Cybersecurity, Operations involve core technologies, processes, and practices designed to protect networks, computers, programs, people and data from attack, damage. Or unauthorized access to the systems.Some object to this perspective, arguing that it is used as a cover for the failure to design useful and usable safeguards. The cyber threat to any organizationis the most effective systems must also involve employee end users of computer systems,in fact, nearly all employees with access to the computers or networks play a role in cybersecurity. Theposition in their organizations whether they know it or not,for instance, a SANS Institute report suggests that “A Security Awareness program is probably the most important weapon in the Information Security professional’s arsenal.” (SANS Institute, 2001).Both cybersecurity professionals and hackers have long to know that end users are the weakest link in organization cybersecurity (West, 2008). Although much of the responsibility for cybersecurity professional rests with employees.Developing savvy computer and mobile device users are essential to cybersecurity defense.

This paper focuses on training end users with or no professional cybersecurity training for they have the greatest need to improve in the organization. The article reviews what we know about practical approaches to cybersecurity training for end users. Awareness programs provide guidelines such as using strong passwords, use a different password for each account, do not post the password on the computer screen and so on, but fail to educate the user on other issues, such as interpreting warning messages and responding appropriately. Savitz (2011) remarks, “We’re all familiar with the obscure “certificate warnings” that our Web browsers occasionally grace us with – these warnings are entirely indecipherable, un-actionable, and thus routinely ignored.” This suggests that cybersecurity training programs may need to go beyond simple awareness education.

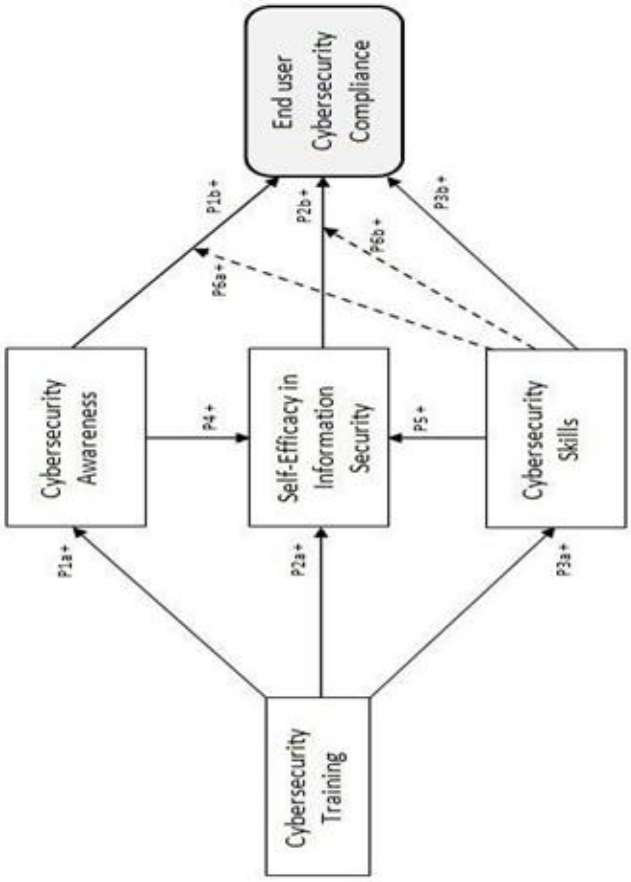

Figure-1 Research model

Cybersecurity Training (CT)

In business environments, the need for the implementation of security countermeasures such as CT has been emphasized and recommended to reduce computer abuse (Straub and Welke 1998). Security policies form the basis for security education training and awareness (SETA). CT sessions, in general, are aimed at informing the users about unacceptable system use and penalties for noncompliance (Straub 1990). CT is defined as those activities that impart specific cyber skills such as safe internet browsing, encryption, decryption and system manipulation (Torkzadeh and Van Dyke 2002), to make security decisions (Furman et al. 2011). The ultimate goal of CT is to impart knowledge and skills such as vulnerability analysis and mitigation, intrusion detection, and incident response, to be less susceptible to social engineering.

Human always has weakest element in the cybersecurity program Training developers to code securely, training operations staff to prioritize a healthy security posture, training end users to spot phishing emails and social engineering attacks, and the cybersecurity begins with awareness withall the companies with experience some kind of cyber attack even if they have robust controls in place. Likewise, an enterprise mustimplement the essential elements of cybersecurity for such care and maintaining secureauthentication practices and storing sensitive data where it is openly accessible to the end user.

The End-user training is recognized as an essential component of the steps necessary to improve cybersecurity compliance, and consequently, cybersecurity posture. Antecedents of cybersecurity compliance in both the home and organizational context have been studied. Among the individual factors that have been examined are cybersecurity awareness, self-efficacy in information security and, to a lesser extent, cybersecurity skills. Each of these variables is potentially a mediator between cybersecurity training and compliance. Research has not examined either the mediating role of these three factors, nor has it reviewed the relative effectiveness of these measures in achieving compliance. Hence the research questions that will be pursued in our research are:

1. What factors mediate the relationship between cybersecurity training and compliance?
2. What is the relative effectiveness of each factor in improving compliance?
3. How does the nature of training affect each of the mediating variables?

A good cybersecurity strategy is to go beyond these basics devices,The Sophisticated hackers can circumvent most defenses, and the attack surface the number of ways or “vectors” an attacker can gain entry to a system is to companies. The It was expected that with these technology advances and the criminals and nation-state spies now threaten most the ICA cyber-physical systems such that most cars, power plants, and the medical devices andhardware and software devices. Similarly, the trends toward hardware and software devices cloud computing, bring your device (BYOD) policies and the burgeoning internet of things (IoT) creates new challenges. Defending these systems has never been more effective.

Cybersecurity Awareness (CA)

We can define as the state of being cognizant of performing secure tasks on a computer (Bulgurcu et al. 2010). Studies have focused on different aspects of awareness. For instance, some have examined knowledge of computer usage policies (e.g., Cronan et al. 2006), others have examined security countermeasures (e.g., D’Arcy et al. 2009) and so on. The multiple aspects collectively include comprehensive information about general guidelines of information security, education on security risks and its consequences on cybersecurity threats, and tracking internet usage for abnormal activities (Choi et al. 2013). All awareness aspects listed in table-3 can be categorized into three dimensions.

Types of cybersecurity

The scope of cybersecurity is too broad core areas to described; any good cybersecurity strategy should take them all into account. If you've not trained your staff, is now is an excellent time for the organization to gain the educated he end user needs to help keep the internet safe. In our increasingly connected world, with our household appliances are connected to the internet, there are also more opportunities than ever before for cybercriminals to wreak havoc on businesses.

The approaches to information security include both technical, non-technical solutionsas they Cyber attackscome a long way from the email viruses well, as Passwords are the most commonly used method of authenticating users to information systemscriminals adapt to changing, The IT security experts whose job it is to keep our data safe in any organization

Infrastructure and Cybersecurity

The Critical infrastructure includes the cyber-physical systems that society relies on, including the electricity grid, water purification, traffic lights, and hospitals with the Although the aim of having security policies is good, and with Plugging a power plant into the internet, Usable security, for example, makes vulnerable to cyber attacks. However, the solution for organizations responsible for critical infrastructure is to perform due diligence to protect organization vulnerabilities and protect against them

SecurityNetwork

Then security network guards against unauthorized intrusion as well as malicious insiders. Ensuring security network often trade-offs requires. Example, This makes passwords more subject to different kinds of attacks.To access passport such as extra logins might be necessary but slow down productivity tools used to monitor network security generate a lot of data so much that end users often miss valid alerts. To help manage network security monitoring and security teams are increasingly using machine learning to flag unusual traffic and alertto threats in real time.

Security onDevice

The era of Bring Your Device (BYOD), more and more mobile devices are entering the workplace, connecting the corporate network, and accessing data in the organization,however, this creates even more entry points for threats to come through; it's crucial for employees to ensure their mobile devices are not connected to the corporate network .

The same threats that lurk over laptop and desktops apply to mobile devices. Smartphonesand tabletsTo this end, we explore could be seen as less secure because they lack pre-installed endpoint protection. The end Users should always be mindful of which websites they're visiting, which apps they' installing.

Physical Security

The Physical security and Cyber threats aren't the only ones employees need to look out for. They Also play a role in keeping sensitive information of the organization protected and leaving a mobile device, or its most risk end users end up committing. If someone were to wipe thephone of an employee's and log into their computer, all of there data and information would be accessible in their device.

Below are the few best practices to help the end user to increase their physical security within the organization

- **Lock your device before and after you leave your desk.** In Windows users, press and hold the Windows key, then press the "L" key. For Mac users, press Control + Shift + Eject (or the Power key) at the same time.
- **Documents should be locked at the cabinet(Store).**Should avoid having sensitive information floating around on their desk (Employees). The before or end of the day, they leave their office unattended; it's always a good idea to stow company documents and the like into a lockable safe or cabinet.
- **Properly discard the information.** When it comes to getting rid of those documents or files, be sure properly shred and discard them.

Cybersecurity Compliance

The End user is a specific case of cybersecurity behavior in which end users conformity with the safe and secure rules and policies, and comply with a recommended of action (Johnston and Warkentin 2010, Herath and Rao 2009).The training programs are designed to achieve goals that meet instructional needs. It is counterproductive to launch training without a thorough assessment of role-relevant tasks, behaviors, and environment (Goldstein & Ford, 2001). Table-1 provides a summary of a sample of studies in which CC is the dependent variable. Several points can be seen in the table. First, cybersecurity compliance has been studied both in organizational and home context. In an organizational context, the studies have been conducted at both corporate and individual level of analysis. In the home context, studies have been at adifferent level of analysis. The model that is being developed in our research is for the different level of analysis and should be applied in both the home and organizational context. Fortunately, there are already a number of organizations that have identified the need for continental coordination and increased cybersecurity awareness While the rest of the world is increasing its focus on cybersecurity through relevant policies, strategies, infrastructure, technology development,

and awareness campaigns, only a few African countries have cybersecurity policies and appropriate security response structures or agencies such as CERTs.

The full responsibility to engender organizational support and convene of SMEs whose collective competencies match the complex challenges posed by a need for the specific training.Organizations must systematically train employees an army of cybersecurity; not all employees will become cyber experts, employers can hold trained end-users accountable for cyber defense performance apropos of the roles they perform.This will teach the user that they are a target, on how to look out for and phishing, password, social engineering, handling of any sensitive data and device.

The most effective way to deliver practical Cybersecurity awareness should reach all levels and inform all users of the internet – from vulnerable, school-going children to families, industry, critical national infrastructures, governments, and the African continent with its unique needs. This will enhance resilience against cyber crimes and attacks and inform African policy development but also prompt the establishment of appropriate organizations such as CSIRTs and collaboration mechanisms to secure the continent and join the efforts of the global community of responsible and secure internet users. Since security awareness has shown to be a barrier to securing information systems in a variety of organizations, it is essential to know that higher institutions like FSU have a role to play in ensuring that user awareness is promoted and appropriately implemented.

REFERENCES

[1]. MOSTI, 2009. National Cyber Security, the way forward, available online from http://www.mosti.gov.my/mosti/images/pdf/national_cyber_security.pdf, Accessed on [01 March 2011].

[2]. Cabinet Office, 2009. Cyber Security Strategy of the United Kingdom, available online from http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf, Accessed on [20 February 2011].

[3]. Cyberspace Policy Review, Assuring a Trusted and Resilient Information, Accessed on [12 February 2011] and Communications Infrastructure http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

[4]. Ministry of Defence-Estonia, 2008. Cabinet Office, 2009. Cyber Security Strategy- Cyber Security Strategy Committee, available online from http://www.kmin.ee/files/kmin/img/files/Kuberjulgeoleku_strategia_2008-2013_ENG.pdf, Accessed on [23 February 2011].

[5]. Obama, B.H., 2009. Remarks By The President On Securing Our Nation's Cyber Infrastructure, BH Obama, President of the United States of America; The White House, Office of the Press Secretary, available online from

[6]. http://www.whitehouse.gov/the_press_office/Remarks-by-thePresident-on-Securing-Our-Nations-Cyber-Infrastructure/, Accessed on [21 February 2011]. [23] Osrin.net, 2011. Estonia's Cyber Security Policy, available online from http://osrin.net/2008/10/estonias-cyber-security-policy/, Accessed on [28 February 2011].

[7]. T. Peltier, "Implementing an Information Security Awareness Program." Information Systems Security 14.Vol. 2, pp. 37–49, 2005. [25] Y. Rezgui and A. Marks, "Information security awareness in higher education: An exploratory study," Journal Computers & Security, vol. 4, pp. 12-25, 2005. Vol 27, pp 241-253, 2008.

[8]. B.D. Cone, C.E. Irvine, M.F. Thompson, and T.D. Nguyen, "A video game for cybersecurity training and awareness," Journal Computers & Security, vol. 16, pp. 63-72, 2007.Vol 27, pp 241-253, 2008.

[9]. UK CERT, 2011. United Kingdom Computer Emergency Response Teams, available online from http://www.ukcert.org.uk/, Accessed on [24 February 2011].

[10]. Compeau, D., Higgins, C. A., & Huff, S. (1999). Social cognitive theory and individual reactions to computing technology: A longitudinal study. *MIS Quarterly*, 145-158.

[11]. Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. (2007). A video game for cybersecurity training and awareness.*computers& security*, *26*(1), 63-72.

[12]. Cronan, T. P., Foltz, C. B., & Jones, T. W. (2006). Piracy, computer crime, and IS misuse at the university. *Communications of the ACM*, *49*(6), 84-90.

[13] D'Arcy, J., Hovav, A., &Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse a deterrence approach. *Information Systems Research*, *20*(1), 79-98.

[14] Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward PIT. *Journal of the Association for Information Systems*, *8*(7), 23.

[15] Dworkin, J. B., Larson, R., & Hansen, D. (2003). Adolescents' accounts of growth experiences in youth activities. *Journal of youth and adolescence*, 32(1), 17-26.

[16] Eminagaoglu, M., Ucar, E., and Eren, S. (2009). The positive outcomes of information security awareness training in companies – *A case study*, *InformationSecurity Technical Report*, 14, 223-229.

[17] Eric Savitz. (2011) (http://www.forbes.com/sites/ciocentral/2011/11/03/humans-the-weakest-link-in-information-security/#7e48cb2d31fd, last visited May 4, 2016)

[18] Fischer, K. W., (1980). A theory of cognitive development: The control and construction of hierarchies of skills. *Psychological Review*, *87*(6), 477.

[19] Foltz, C. B., Paul Cronan, T., & Jones, T. W. (2005). Have you met your organization's computer usage policy?.*Industrial Management & Data Systems*, *105*(2), 137-146.

[20] Frayne, C. A., & Latham, G. P., (1987). Application of social learning theory to employee self-management of attendance. *Journal of applied psychology*, *72*(3), 387.

[21] Furman, S. M., Theofanos, M. F., Choong, Y. Y. & Stanton, B. (2011). Basing cybersecurity training on user perceptions. *IEEE Security & Privacy*, (2), 40-49.

[22] Gist, M. E., Schwoerer, C., & Rosen, B. (1989). Effects of alternative training methods on self-efficacy and performance in computer software training. *Journal ofapplied psychology*, *74*(6), 884.