A Dynamic Decision-Model for Re-thinking Information Security in Higher Institution of Learning

Bukhari, B., Longe, O.B., Jean-Paul, C. & Auwal, A.T.
School of IT & Computing
Information Systems Programme
American University of Nigeria
Yola, Adamawa State, Nigeria
E-mails: bukhari.badamasi@aun.edu.ng, olumide.longe@aun.edu.ng, Jeanpaul.cleron@aun.edu.ng, auwal.tata@aun.edu.ng
Phones: +2348036992294, +2348160900893, +2348034532760; +2348034532760

ABSTRACT

Model thinking is explore as a great tool in which information security officers "actors" can use and think critically, at the same time, design a better model that can help higher institutions to manage and protect their network from intrusion. Similarly, a decision model is employed to allow for the choice of the appropriate security protocols/mechanisms. On the other hand, actors can also deploy technical or administrative mechanisms as the security protocols on the network or on the entire organizational information system. In this paper, a multi-dimensional approach to cyber security was suggested in which the interaction of different variables within institutions can be mapped to minimize the level of cybercrime incidents when measures are fully implemented, hence cybercrime incidents. The approach is system dynamics models based on system theory. A system dynamics model for the cybercrime incidents in higher institutions can be used, where the core structure (or the main causal loop) of the model is based on the dynamic interactions between the actions of the attackers and the target organization, and the perceive ease of attack (Behara et al., 2007). This target (higher institutions) is selected because it is one of the major targets by cybercriminals (Lagazio, Sherif, & Cushman, 2014).

Keywords: System Dynamics, Decision Model, Information Security, Higher Institution

23rd iSTEAMS Conference Proceedings Reference Format

Bukhari, B., Longe, O.B., Jean-Paul Cleron & Auwal, A.T. (2020): A Dynamic Decision-Model for Re-thinking Information Security in Higher Institution of Learning. Proceedings of the 23rd iSTEAMS Conference, American University of Nigeria, Yola. April, 2020. Pp 109-116 www.isteams.net/yola2020

1. INTRODUCTION

To analyze information security in any organization, several actors have to think in different ways in which the deployment of security measures can be done effectively. Information security is a key to every organization whether IT organizations, the financial sector, or higher institutions. The incidents in which usually caused by non-compliance with security measures are on the increase. Although, security measures adopted by most organizations is purely technical, while very few organizations believe in using both technical and administrative security measures in curtailing security breaches (Alarifi, 2019). Information security officers in organizations are challenged with different varieties of securing organizational data such as risk mitigation, security planning, security technology selection, threat assessment, performance monitoring, and policy formation (Whitman & Mattord, 2011). Imposing security on organizational network cannot just be by setting-up rules alone, rather it should be a combination of the social and technical interplay (Inglesant & Sasse, 2011).

Therefore, this realizes the challenge of re-thinking information security in organizations, specifically academic institutions, in a form of providing policies and procedures followed with the endorsement of those policies by senior management. The security policies otherwise known as administrative security is necessary. Understanding the role and interplay of technical security and administrative security of academic institutions are quite acceptable to users and at one hand meet the need and help organizations to effectively secure its information system resources.

2. LITERATURE REVIEW

Higher institutions continue to experience different kinds of cybercrime incidents that change with time and materialization due to advancements in technology. It is a known fact that cybercriminals emerge from the training and systematized approach to the acts by cybercriminals. Over the last decades, owing to technological advancement, global dynamics have completely changed in socio-technical alignments, and international security. Hitherto, cybercriminals take advantage of the advanced technology and adopt new methods in carrying-out their illicit acts (McCarthy, 2011). Yar and Steinmetz (2019) stated that the world is now more interconnected even though societies are increasingly facing serious threats. Cybercriminals are taking advantage of the situation to extort vital information that they can use for the furtherance of other attacks within institutions. It is also noteworthy that, cybercriminals have changed from traditional acts of crimes such as robbery with the violence to the virtual world in line with the advancement in technology (Alarifi, 2019).

Similarly, Asghari, van Eeten, and Bauer (2016); and Kesharwani and Tripathy (2012) re-iterated that fraud through virtual environments has been on the increase thus hurting businesses. A study conducted by McAfee (2018) reported that a firm estimated the global economy is losing 445 billion dollars due to cybercrime incidents annually. Moreover, Hong Kong authorities reported lost of HK$2.3 billion in 2016. In another cybercrime incident where hackers locked the personal data claiming to be given bitcoin as ransom in which the technology crime team helped to unlocked data; hence safeguarding the privacy of the individual. Cybercrime incidents are on the rise where cheating and deception increases exponentially as perpetrators utilize email and phone frauds to lure victims (Alarifi, 2019).

Denial of Service (DoS) attack, Distributed Denial of Service (DDoS) attack, phishing email, ransomware are most of the security challenges being faced by higher institutions. In a study conducted by Verizon Enterprises Solutions in 2015, 292 cases of data breach was experienced by higher institutions in the developed countries (Solutions, 2015). The consequence of breaching the institutional network is that, sensitive students' information was exposed that comprises medical history, altering students' grades, jeopardizing university payroll system. In another study conducted by Mistry (2019), it was reported that 54 percent (54%) of the cybercrime activities are usually caused by insiders. Similarly, Infoblox (2018) reported 48 percent (48%) of security risks come from within the affected institutions.

Furthermore, most of the cybersecurity of the frustrating institutions are difficult to secure. Sometimes, many of the security measures provided at higher institutions are not as effective as they should be. Wright (2020) stated that "because of the way schools are designed with open networks so students and teachers can connect". Wright (2020) further added that "everyone having laptops, tablets, or smartphones, and the ability for all those devices to get to social media websites, the malware and scams in a school environment are more likely to be spread".

In another study conducted by Colin Wood (2020) reported that St. Louis Community College with four campuses announced phishing attacked by cybercriminals and compromised the records of 5,000 staff and students at the College. Some of the records compromised include cell phone numbers, student ID numbers, dates of birth, address, names, and email addresses.

In this paper, model thinking is explore as a great tool in which information security officers “actors” can use and think critically, at the same time, design a better model that can help higher institutions to manage their information resources on the network. Similarly, a decision model is employed to allow for the choice of the appropriate security protocols/mechanisms by people concern. On the other hand, actors can also deploy all the available mechanisms as the security controls on their network or on the entire information systems. Furthermore, this paper suggests a multi-dimensional approach in which the interaction of different variables within institutions can be mapped to minimize cybercrime incidents when measures are fully implemented. A model called system dynamics which is used to analyzed information security based on system theory in higher institution. The target (higher institutions) is selected because it is one of the major targets by cybercriminals (Lagazio et al., 2014).

3. INFORMATION SECURITY MODEL

Information security has been called different things raging from IT security, data security, and computer security. But, since information is the key and always considered in organizations to be worth more than the networks or computers it runs on, therefore the term is "Information Security”. According to Von Solms and Van Niekerk (2013), information security is aim to achieve three main characteristics namely confidentiality which refers to the protection of unauthorized access to organizational data. Integrity relates to the protection against undesired changes of organizational records. While availability concern with the expected use of resources within the desired time frame. The information security model is a computer model which used to identify and impose security mechanism (Behara, Huang, & Hu, 2007). It is also a framework in which security mechanism is developed, and describes how security should be laid out and governed within the organization.

Higher institutions suffer a lot of setbacks to security breaches which lead to compromising students and staff records. The information security model as depicted in Figure 1, shows “information” as un-secure since it has not full-fill any of the three characteristics of information security. For the three characteristics (confidentiality, integrity, and availability) to be full-filled, higher institution must either decide to choose technical security, administrative security or use both. Technical security further subdivided into IT security and physical. Similarly, administrative security could either be formal or informal. Therefore, for an institution to have its information secured, it must satisfy all the four conditions. These conditions include providing computer security, implementing communication security, deploying physical security and imposing administrative security. Once these security measures are deployed, the institution will be fully secured including all the information systems resources.

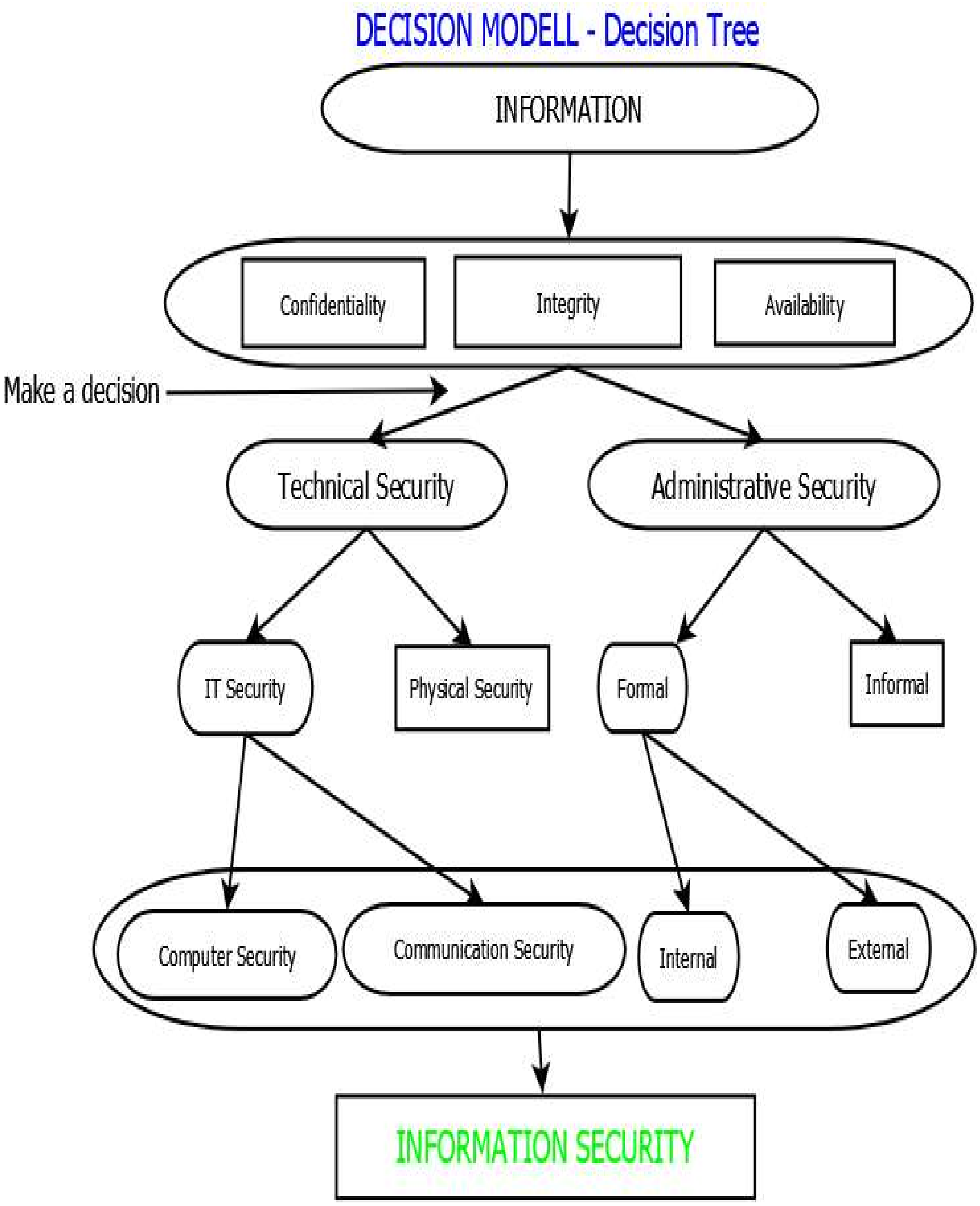

Figure 1: Proposed Information Security Model

Similarly, for full security to be achieved in higher institutions, it is necessary to have maximum computer security (CS), maximum communication security (TTS), maximum physical security (PS) and maximum administrative security (AS) indicated mathematical on the next page.

Security = S; Technical security = TS; Administrative security = AS; Communication security=TTS; and Physical security = PS

So,

$$S = TS + AS$$

But, $TS = ITS + PS$

Also $ITS = CS + TTS$

Now $S = CS + TTS + PS + AS$

Therefore; Full Security will be achieved by:

$$\lim_{\mathrm{s}\to\mathrm{FS}} (S) = [\mathbf{CS}\mathrm{max} + \mathbf{TTS}\mathrm{max} + \mathbf{PS}\mathrm{max} + \mathbf{AS}\mathrm{max}]$$

Decision-models for information security provide guidelines for the development of information security, any attempts to manage higher institutions' resources to improve information security must understand the dynamic nature of security threats, countermeasures, and effort to prevent and recover from an incident of cybercrime.Consequently, an institution can experience cybercrime incidents if security mechanisms are not fully deployed. System dynamic is particularly silent for the analysis of information security. Previous studies has used system dynamics to model areas of information security such as insider threats (Andersen et al., 2004; Gonzalez, Qian, Sveen, & Rich, 2005; Melara, Sarriegui, Gonzalez, Sawicka, & Cooke, 2003), the dynamic interaction of threats and counter-measures (Saunders, 2003), and human factors in risk-dependent compliance (Gonzalez & Sawicka, 2002).

The focus of this section is on the effect of non-deployment of cybersecurity on the network of higher institution of learning and the risk associated with it, with the help of decision-model and a system dynamics. Figure 2 indicates a system dynamics model for cybercrime incidents and the loops associated with the each variable.

4. SYSTEM DYNAMICS MODEL

Figure 2 shows a system dynamics model for the cybercrime incidents in the higher institutions of learning. The core structure (or the main causal loop) of the model is based on the dynamic interactions between the actions of the attackers and the target organization, and perceive ease of attack. Typically, causal loops in system dynamics comes in two types: a reinforcing loop, where the variables involved reinforce one another, and a balancing loop, where the variables interact with one another in an oscillatory behavior (Behara et al., 2007).

It is argue that the main causal loop in the cybercrime incident phase is largely one of reinforcement; that is, the successes of cybercrime incidents lead to more incidents, and reducing attack frequency leads to still fewer cybercrime incidents. Although such incident dynamics is plausible, the implied result of zero or infinite number of incidents from this reinforcement is unrealistic.

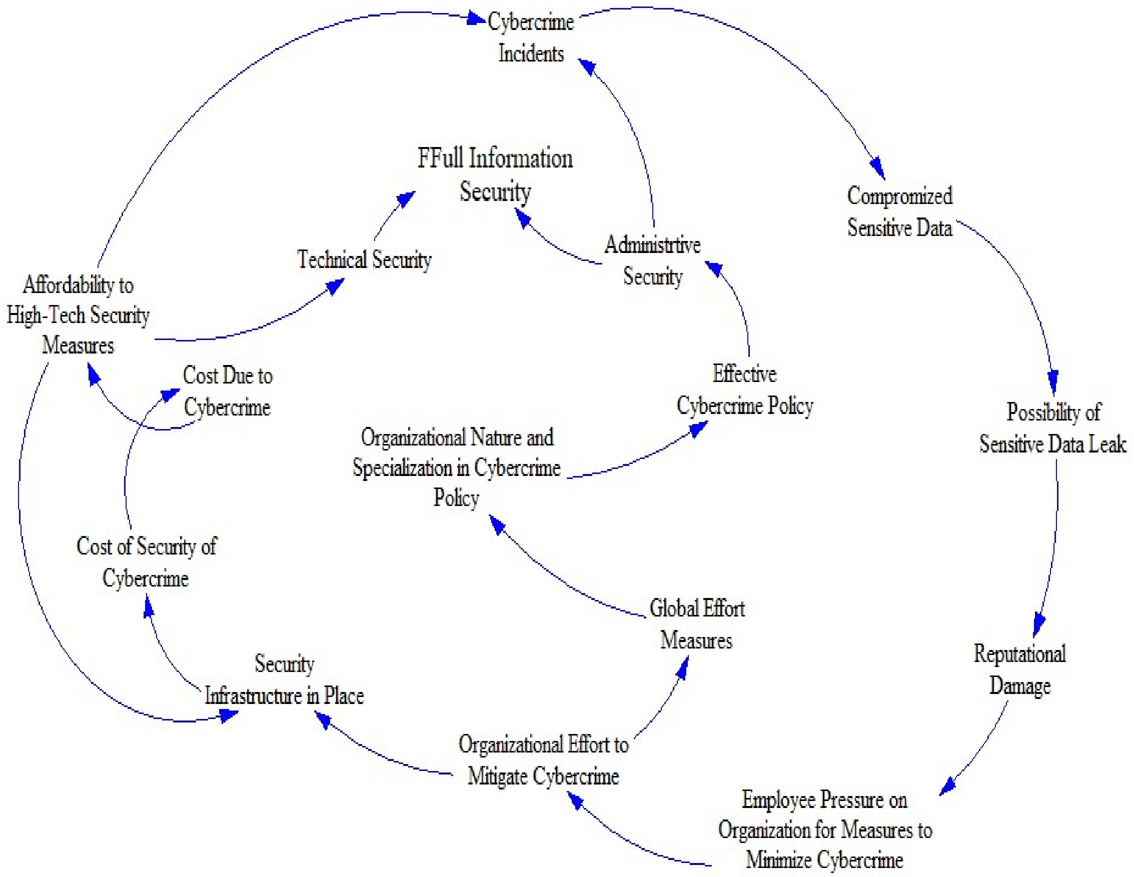
Cybercrime Incidents
FFull Information Security
Compromized Sensitive Data
Technical Security
Administrtive Security
Affordability to High-Tech Security Measures
Cost Due to Cybercrime
Effective Cybercrime Policy
Possibility of Sensitive Data Leak
Organizational Nature and Specialization in Cybercrime Policy
Cost of Security of Cybercrime
Global Effort Measures
Reputational Damage
Security Infrastructure in Place
Organizational Effort to Mitigate Cybercrime
Employee Pressure on Organization for Measures to Minimize Cybercrime

Figure 2: System dynamic for cybercrime incidents

Figure 2 explains why it is important for higher institutions to deploy and maintain full security on their networks. The figure shows that once the security mechanisms are not fully provided, “cybercrime incidents” will be high, and that will increase the probability of those incidents relate to “compromise sensitive data”, which in turn increase the “possibility of sensitive information leak” and therefore propaganda campaigns against higher institutions, eventually leading to “reputational damage” for the institution. However, the “reputational damage” may raise the awareness of cybercrime activities and lead to more “employee pressure on the organization for measures to minimize cybercrime", which could work in the favour of increasing organizational effort and strategies for tackling cybercrime. Therefore, sensitive information leaks, possibly triggered by cybercriminals could have an initial negative impact on higher institution. It also describes the organizational exposure of vulnerabilities and that will trigger ways in dealing with cybercrime incidents, prompting the design of more collaborative and effective measures to address those vulnerabilities and mitigate cybercrime incidents.

The figure further indicated that better security infrastructure and global enforcement measures are mostly the result of consideration related to enhancing strategic organization position. Moreover, these measures also rely not only to maintain and prevent cybercrime incidents from occurring rather to focus on the effective and affordable high-tech security measures and effective cybercrime policy deploy within higher institutions which will yield greater and effective security “Full Information Security”.

Moreover, the feedback loop in figure 2 indicates, if institution does not afford to provide high-tech security measures on the network, ordinary security infrastructure need to be at least deployed for the institution to be secured and prevent cybercrime incident.

5. CONCLUSION

Providing security to every organizational information systems is necessary since employee information should be protected from any wrongful access or tempering of data, as well as been available to the right persons at the right time. However, since higher institutions ultimately focus more on students' records, information must be secured, but also possible to transfer information between different sections of the institutions such as bursary departments, academic affairs divisions, faculties, departments, as such a decision model for re-thinking information security is provided to achieve optimal security in higher institutions. The information security model is necessary for higher institutions because students and employee records need to be protected from any wrongful access or tampering by unauthorized person. This can be achieved through using models, thinking of how to overcome security challenges within academia. Failure to effective deploy and manage security measures by the institutions, will lead to cybercrime incidents as depicted in figure 2 where a system dynamics a model analyzed information security in the higher institutions.

REFERENCES

1. Alarifi, A. (2019). Strengthen of Cybersecurity in the Organizations: Challenges and Solutions. International Journal of Computer Applications, 975, 8887.
2. Andersen, D. F., Cappelli, D., Gonzalez, J. J., Mojtahedzadeh, M., Moore, A., Rich, E., . . . Weaver, E. (2004). Preliminary system dynamics maps of the insider cyber-threat problem. Paper presented at the Proceedings of the 22nd International Conference of the System dynamics Society.
3. Asghari, H., van Eeten, M., & Bauer, J. M. (2016). Economics of cybersecurity Handbook on the Economics of the Internet: Edward Elgar Publishing.
4. Behara, R., Huang, C. D., & Hu, Q. (2007). A system dynamics model of information security investments.
5. Gonzalez, J. J., Qian, Y., Sveen, F. O., & Rich, E. (2005). Helping prevent information security risks in the transition to integrated operations. Telektronikk, 101(1), 29.
6. Gonzalez, J. J., & Sawicka, A. (2002). A framework for human factors in information security. Paper presented at the Wseas international conference on information security, Rio de Janeiro.
7. Inglesant, P., & Sasse, M. A. (2011). Information security as organizational power: A framework for re-thinking security policies. Paper presented at the 2011 1st Workshop on Socio-Technical Aspects in Security and Trust (STAST).
8. Kesharwani, A., & Tripathy, T. (2012). Dimensionality of perceived risk and its impact on Internet banking adoption: An empirical investigation. Services Marketing Quarterly, 33(2), 177-193.
9. Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cyber crime on the financial sector. Computers & Security, 45, 58-74.
10. McAfee, C. (2018). Net losses: Estimating the global cost of cybercrime. Retrieved from
11. McCarthy, D. M. (2011). An economic history of organized crime: a national and transnational approach: Routledge.
12. Melara, C., Sarriegui, J. M., Gonzalez, J. J., Sawicka, A., & Cooke, D. L. (2003). A system dynamics model of an insider attack on an information system. Paper presented at the Proceedings of the 21st International Conference of the System dynamics Society.
13. Mistry, E. B. (2019). Erudio EdTech Consulting Business Plan: An Organization Development-influenced Plan. The College of St. Scholastica.
14. Saunders, J. H. (2003). A dynamic risk model for information technology security in a critical infrastructure environment Risk-Based Decisionmaking in Water Resources X (pp. 23-39).
15. Solutions, V. E. (2015). Data breach investigations report. Verizon, Report.
16. Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97-102.
17. Whitman, M. E., & Mattord, H. J. (2011). Principles of information security: Cengage Learning.
18. Yar, M., & Steinmetz, K. F. (2019). Cybercrime and society: SAGE Publications Limited.