Analyzing the Effect of IT Decision-Making on Cybersecurity Breaches in Higher Education

Lawrence J. Awuah, PhD

Abstract: The recent and current data breaches and cyberattacks continue to spike at an alarming rate, which in most cases can be consequential if proactive measures are not taken. Unfortunately, taking a closer look at most of those breaches and/or cyberattacks indicates that risk-based and event-based decision-making could have intended or unintended impacts on potential threats and the level of mitigated effort implemented. In this view, the lack of centralized IT governance, particularly in Higher Ed institutions, over the years, has witnessed frequent breaches associated with rising security incidents. It has therefore become critically important that IT and cybersecurity executives do well to balance IT uptime with data protection requirements while adhering to security policy enforcement.

Liu, C. W., Huang, P., & Lucas Jr, H. C. (2020). Centralized IT decision making and cybersecurity breaches: Evidence from US higher education institutions. *Journal of Management Information Systems*, *37*(3), 758-787. DOI: https://doi.org/10.1080/07421222.2020.1790190

Summary: "Despite the consensus that information security should become an important consideration in information technology (IT) governance rather than the sole responsibility of the IT department, important IT governance decisions are often made on the basis of fulfilling business needs with a minimal amount of attention paid to their implications for information security. We study how an important IT governance mechanism—the degree of centralized decision making—affects the likelihood of cybersecurity breaches. Examining a sample of 504 U.S. higher-education institutions over a four-year period, we find that a university with centralized IT governance is associated with fewer breaches. Interestingly, the effect of centralized IT governance is contingent on the heterogeneity of a university's computing environment: Universities with more heterogeneous IT infrastructure benefit more from centralized IT decision making. In addition, we find the relationship between centralized governance and cybersecurity breaches is most pronounced in public universities and those with more intensive research activities. Collectively, these findings highlight the tradeoff between granting autonomy and flexibility in the use of information systems and enforcing standardized, organization-wide security protocols."

Keywords*: Risk management, risk assessment, IT security; IT governance; cybersecurity breach; centralized decision making; cybersecurity analytics; security operations*

Recent high-profile security breaches, notably those involving much-publicized and large-scale breaches and ransomware attacks on Colonial Pipeline, Facebook data breach, Kaseya Ransomware attack, and Sony Pictures have attracted scrutiny as to how the seemingly flawed decisions of employees or IT leadership can have major cybersecurity implications. Additionally, the recent and current data breaches and cyberattacks continue to spike at an alarming rate with associated consequential impacts. A closer examination of most of those breaches indicates that risk-based and event-based decision-making could have intended or unintended impacts on potential threats and the level of mitigated effort implemented. With cyberattacks becoming more widespread and more sophisticated than ever before, due care and due diligence should consistently be the focal point of IT executives. By the third quarter of 2022, [8] indicated a total of 112 publicly disclosed security incidents were identified, resulting in over 97 million compromised records. This finding represents an increase of approximately 11% in security incidents

compared to the previous year. In their study, Liu et al. [1] found that academic institutions with centralized IT governance record fewer security breaches. This claim was in part attributed to the fact that those institutions with distributed IT infrastructure benefit more from centralized IT decision-making than those who do not. This assertion suggests that lack of centralized IT governance, whether in the corporate establishments or in Higher Ed institutions, can lead to frequent breaches associated as a result of rising security incidents. As well, several studies have examined financial loss, legal implications, and moral obligations involving data breaches and their impact on organizations, data owners, and victims [1]-[6], [8]. It is therefore incumbent on IT and cybersecurity leadership to do more to balance IT functionality and uptime with data protection needs while instituting security policy enforcement. This practice can make cybersecurity a business enabler to minimize risks while maximizing revenue for continued business growth.

On the other side of the spectrum, IT governance and decision-making are contingent on human factors. Human error has been known to be the main cause of most cyber security breaches; indeed, humans are the weakest link in the security chain [12]. For this reason, cybersecurity leadership cannot ignore security awareness training programs. The executives should be mindful of the fact that humans form a significant factor contributing to data breaches. This awareness can augment the centralized IT decision-making in confronting cybersecurity breaches in Higher Ed institutions in particular and the industry in general. According to [11], security awareness training programs are educational in nature that equip employees with tools to identify, mitigate, and report such attacks crafted by social engineering techniques. One of the biggest risks to an organization's IT security is often not a weakness in the technology control environment per se; rather it is the action or inaction by employees and other personnel that can lead to security incidents. For example, employee noncompliance related to IT security policies continues to raise eyebrows for most organizations today. In other words, considering the variety of IS security policy compliance strategies in place, security awareness training [9], [10]-[11] forms a crucial part of the war on cyber threats. Evidently, despite widespread awareness of risks, significant investments in cybersecurity protection, and substantial economic incentives to avoid security breaches, organizations remain vulnerable to phishing attacks [2].

Furthermore, several studies [4]-[6] suggest that while cybersecurity is usually treated as a technology problem, most data breaches are the result of human error. By identifying the social behavior indicators, along with the rationales behind the decision-making process, the development of cybersecurity architecture can be improved. This aligns with the assertion by Liu et al. [1] that that adopting a centralized IT unit with a better understanding of the overall IT architecture can better equip the executives in managing risks even in a sophisticated IT environment. This is particularly important to the average cybersecurity team who could possibly make reactive decisions in addressing reported breaches. In any case, the human factor needs to be an integral part of every IT implementation when reducing and protecting against information security risks accompanying the development, architecture, and maintenance of an IT system [5]. In other words, discussing IT security problems must factor in policies, behavior, and user compliance requirements [6].

Over the past few years, [1] noted that the management of information security has gained significant research interests in the research community, as well as expert interests in the field. Typically, risk-based decision-making is reflective of strategic investments by virtue of the desire for detection, prevention, and response plans. These three parameters need to be balanced for optimum gains. Additionally, the importance of good management practices in protecting organizational assets and enforcement policies in checking employee security behaviors in organizations has also been recognized [5]-[6], [9]-[10]. One typical example is law enforcement, which can play a key role in this effort. Hui et al. estimated the impact of enforcing the Convention on Cybercrime (COC) on the desire to deter and reduce distributed denial of

service (DDOS) attacks, for example [7]. The authors noted that directly observing attacker behavior can impact deterrence to complement law enforcement and leadership actions. Overall, making well-informed decisions regarding the value and benefits of secure IT implementations in the organization is great if cybersecurity is considered a business enabler. For instance, proactive investment strategies should be adopted to help minimize risks to the organization and maximize return on investment (ROI) from the perspective of understanding cybersecurity as a business enabler.

Moreover, there are other factors that make the role of IT and information security leadership an important ingredient in ensuring a substantial security posture. In some literature, there have been constant calls for IT executives to improve security operations capabilities with the aim of identifying and confronting cyberattacks using applicable incident response techniques as presented by [3]. For example, by automating security controls and policies, the security operations teams can operationalize cyber response best practices with the right guidance. In another study, strict security policies surrounding Bring Your Own Device (BYOD) computing environment in organizations were studied. Thus, complying with BYOD security policies is necessary within organizations to address the factors that lead to the desired security behavior [4]. As mentioned earlier, [1], [5] examined the implications of IT decision-making on the effect of information security management on the protection of assets and critical data. In their justification, the authors developed and tested hypotheses considering how centralized and strategic IT decision-making affect the value of information security over a certain period.

Key Takeaways

IT/Cybersecurity executives in academic institutions must consider doing the following:

1. Endeavor to put safeguards in place including security controls, policies, security awareness programs, disaster recovery plans (DRP)/ business continuity plans (BCP) and others.
2. Focus on embracing strategic goals in line with cybersecurity as a business enabler in terms of risk reduction, cost-effectiveness, and resource optimization targeted at high ROI.
3. Understand the threat landscape, assess cybersecurity maturity, improve cybersecurity program, and document short- and long-term cybersecurity strategy.
4. Balanced prevention techniques, response strategies, and detection capabilities with actionable intelligence.

In a nutshell, the theoretical development and empirical analyses yielded two important findings about the adoption of centralized IT governance in the enterprise. The main goal is that this practice tends to minimize cybersecurity breaches, especially when an academic institution has a heterogeneous IT environment in place. In these days of escalating attempts to breach information systems everywhere at any time, it is imperative that senior executives—including CISO, CIO, CFO, CRO, and CEO—consider the impact of IT governance decisions on their cybersecurity maturity and the value it brings to the organization. Therefore, the quest for reinventing cybersecurity solutions must be a continuous focus to bolsters cybersecurity infrastructure with appreciable visibility and the need to gravitate toward broader security strategies for added benefits to the organization.

References:

[1] Liu, C., Huang, P., & Lucas, H., C. (2020). Centralized Information Technology Decision Making and Cybersecurity Breaches: Evidence from U.S. Higher Education Institutions. *Journal Of Management Information Systems, 37*(3), 758–787. https://doi.org/10.1080/07421222.2020.1790190

[2] Wright, R., Johnson, S. L., & Kitchens, B. (2022). Phishing Susceptibility in Context: A Multi-level Information Processing Perspective on Deception Detection. *Wright, RT, Johnson, SL, Kitchens, B." Phishing Susceptibility in Context: A Multi-level Information Processing Perspective on Deception Detection" MIS Quarterly*.

[3] Kinyua, J. & Awuah, L. (2021). AI/ML in Security Orchestration, Automation and Response: Future Research Directions. *Intelligent Automation & Soft Computing, 28*(2), 527–545. DOI:10.32604/iasc.2021.016240

[4] Palanisamy, R., Norman, A. A., & Kiah, M. L. M. (2020). Compliance with Bring Your Own Device security policies in organizations: A systematic literature review. *Computers & Security*, *98*, 101998.

[5] Bhaharin, S., H., Sulaiman, R., Mokhtar, U., A., & Yusof, M., M., (2019). Issues and Trends in Information Security Policy Compliance. *2019 6th International Conference on Research and Innovation in Information Systems (ICRIIS)*. DOI: 10.1109/ICRIIS48246.2019.9073645

[6] Angraini, A., & Okfalisa, R. Y. (2019). Information security policy compliance: Systematic literature review. *Procedia Computer Science*, *161*, 1216-1224.

[7] Hui, K. L., Kim, S. H., & Wang, Q. H. (2017). Cybercrime deterrence and international legislation: Evidence from distributed denial of service attacks. *Mis Quarterly*, *41*(2), 497.

[8] Irwin, L. (2022, September 1). List of Data Breaches and Cyber Attacks in August 2022–97 Million Records Breached. *IT Governance*. https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-august-2022-97-million-records-breached

[9] Puhakainen, P., & Siponen, M. (2010). Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. *MIS Quarterly 34*(4), 757-778.

[10] Richet, J. L. (2012). How to Become a Black Hat Hacker? An Exploratory Study of Barriers to Entry Into Cybercrime. In *AIM*.

[11] Solomon, A., Michaelshvili, M., Bitton, R., Shapira, B., Rokach, L., Puzis, R., & Shabtai, A. (2022). Contextual security awareness: A context-based approach for assessing the security awareness of users. *Knowledge-Based Systems*, *246*, 108709.

[12] Richet, J. L. (2022). How cybercriminal communities grow and change: An investigation of ad-fraud communities. *Technological Forecasting and Social Change*, 174, 121282.