Information Security Management

Kyle D. Reinert

Old Dominion University

Author Note

This paper was prepared for Cybersecurity as a Social Science (CYSE 201S), taught by Professor Armistead.

**Information Security Management**

The security threats to any organization's information have become more sophisticated and will continue to as time goes on. In our new era of technology, Industry 4.0, machines and other technologies are now connected with the Internet of Things (IoT) and the cloud. Combining the weakest link, humans, with the advancing technologies of this era makes it more challenging to secure and protect organizational information (Bhaharin et al., 2019). Information security management ensures that an organization's information and information systems are protected from unauthorized access, disturbance, disclosure, and destruction while maintaining confidentiality, integrity, and availability (CIA) (Bhaharin et al., 2019). Due to this position, information security management plays a vital role in protecting an organization's information, requiring social science to perform its job adequately.

In the history books of the future, Industry 4.0 should be found as our fourth industrial revolution that came with many pros and cons that the others had before it. Sony & Naik (2019) call it "the present trend in automation and data exchange in organizations" that can also entirely change how an organization operates. It consists of IoT, artificial intelligence, robots, an internal connected network, digitization, programmable logic controller (PLC), communication protocols, Supervisory Control and Data Acquisition (SCADA), and cybersecurity (Javaid & Haleem, 2019). Creating technological solutions for current and future problems depends on an organization's strategies and information security policy. Soomro et al. (2016) also claim that information security management requires a holistic approach to technical, human, and organizational factors.

The human factor in information security is the weakest link and the primary source of information leakage to an organization. However, technology factors alone cannot guarantee a secure environment; therefore, amplifying the weakest link is the best option (Bhaharin et al., 2019). This is why policies and procedures are instilled in a workplace to complete day-to-day tasks, as most of an organization's attack surface "lies within unintentional insider threats," who can be employees who are not correctly complying with security policies and procedures (Posey & Canham, 2018). However, information security management cannot just create a policy and call it a day. There has to be a healthy balance between employee productivity and the policies created because the policy can hinder employee performance (Posey & Canham, 2018).

Attempts to control internal user security behaviors must be looked at through social science perspectives relating to psychology, sociology, and economics because they are all connected in an organization. For example, employees may face certain decisions to perform their duties, either believing that they can perform some tasks in complete accordance with policy or complete all tasks deviating a bit from the policy (Posey & Canham, 2018). Bulgurcu et al. (2010) drew on the theory of planned behavior, claiming that internal control, perceived behavioral control, and attitude toward compliance influence an employee's intent to comply with the organization's information security policies. However, Posey & Canham (2018) have stated that prior cybersecurity policy compliance research "are limited to individual-level compliance only and fail to show how, and when, micro-level compliance activities influence aggregate structures" and require a more computational social science approach. According to the Dual-Process Theory of decision-making, humans depend upon an automatic system and a 'rational' system. An automatic system can seem instinctive and effortless but can also be inclined to mistakes. The 'rational' system is processed much slower and consciously handled deliberative approach that feels more effortful. Human factors research shows that individuals become more reliant upon automatic processing when stressed or fatigued; therefore, employees may tend to depend on habituation over deliberative decision-making when under these circumstances. (Posey & Canham, 2018).

Over time, technology will continue to advance along with risks, threats, and weaknesses. In order to protect an organization's information, information security management requires social science expertise. Policies created should be able to balance employee productivity with the policies they create since policies can negatively impact employee performance. Research and theories involving social science are extremely beneficial for the development of information security policies as it does not only affect how secure an organization is but also affect the production and overall quality of work-life for employees.

Bibliography

Bhaharin, S. H., Mokhtar, U. A., Sulaiman, R., & Yusof, M. M. (2019). Issues and trends in information security policy compliance. *2019 6th International Conference on Research and Innovation in Information Systems (ICRIIS)*. https://doi.org/10.1109/icriis48246.2019.9073645

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523–548. https://doi.org/10.2307/25750690

Javaid, M., & Haleem, A. (2019). Industry 4.0 applications in medical field: A brief review. *Current Medicine Research and Practice*, *9*(3), 102–109. https://doi.org/10.1016/j.cmrp.2019.04.001

Posey, C., & Canham, M. (2018). A computational social science approach to examine the duality between productivity and cybersecurity policy compliance within organizations. *International Conference on Social Computing, Behavioralcultural Modeling & Prediction and Behavior Representation in Modeling and Simulation (SBP-BRiMS)*.

Sony, M., & Naik, S. (2019). Key ingredients for evaluating industry 4.0 readiness for organizations: A literature review. *Benchmarking: An International Journal*, *27*(7), 2213–2232. https://doi.org/10.1108/bij-09-2018-0284

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009