American Journal of Operations Management and Information Systems
2020; 5(2): 25-28
http://www.sciencepublishinggroup.com/j/ajomis
doi: 10.11648/j.ajomis.20200502.12
ISSN: 2578-8302 (Print); ISSN: 2578-8310 (Online)

Case Report

Challenges in Addressing Information Security Compliance in Healthcare Research: The Human Factor

Sweden De Matas*, Brendan Keegan

Office of Research Oversight, Department of Veterans Affairs, Washington DC, United States

Email address:

Sweden.dematas@va.gov (S. De Matas), Brendan.keegan@va.gov (B. Keegan)

*Corresponding author

To cite this article:

Sweden De Matas, Brendan Keegan. Challenges in Addressing Information Security Compliance in Healthcare Research: The Human Factor. *American Journal of Operations Management and Information Systems*. Vol. 5, No. 2, 2020, pp. 25-28. doi: 10.11648/j.ajomis.20200502.12

Received: June 24, 2020; **Accepted**: July 8, 2020; **Published**: July 28, 2020

Abstract: This retrospective case report aimed to evaluate the impact of information security compliance in research programs across a large federal healthcare organization. The authors sought to discern whether the methodologies employed for promoting and ensuring compliance delivered the expected benefits and produced a more informed basis for employee decision-making. Data collected from compliance report assessments conducted at 103 federal research programs were reviewed and analyzed by clustering into three primary groupings (procedural, technological and behavioral). While noncompliance related to technological strategies was rare, moderate levels of procedural noncompliance was observed across most areas of analysis, and the highest rates of non-compliance identified in the behavioral category and observed across all areas of analysis, signifying the need for a more comprehensive approach to information security oversight and compliance strategies with specific consideration to those factors that impact human behavior.

Keywords: Information Security, Research, Behavior, Compliance, Risk, Policy, Oversight

1. Introduction

The security of information and information systems have become a priority to many organizations as dependence on those systems is often paramount to organizational operations, and its use inherently fraught with risk [1]. As a result, oversight of information and information systems is important and when managed effectively can help reduce loss, protect resources, and enable operational continuity [2].

In today's complex environment, the need for ongoing and multifaceted approaches to information security are not only necessary, but prudent, and significant financial and human capital placed into relevant oversight and compliance programs [3]. Despite this, and without regard to increased federal scrutiny, information security incidents continue to increase with data losses occurring each year [4]. Amid these dynamics however, information security oversight and compliance strategies remain rather basic, and largely unevolved [5].

Common strategies for detecting and mitigating information security risk routinely involve technological and procedural resources, and while necessary, informatics researchers [6] stress that by themselves, these strategies alone are not good determinants of risk [7]. Rather, leaderships' involvement, effective information security policies [8], employee awareness, and human behavior [9], are all necessary factors in decreasing risk as well as promoting and motivating compliance. Human behavior in particular, is often considered the utmost, if not the primary determinant of risk [10] and as a result, the role that employees play in information security compliance cannot be understated.

This case report aimed to evaluate the impact of information security compliance strategies in research programs across a large federal healthcare organization. The authors sought to discern whether the methodologies employed for promoting and ensuring compliance delivered the expected benefits and produced a more informed basis for employee decision-making. In addition, the authors hoped to expand the literature regarding information security compliance through the lens of employee decision-making and organizational performance.

2. Literature Review

To understand an employee's motivation to comply with organizational requirements (i.e., information security policies and procedures), it's first important to recognize those primary influences and determinants of human behavior that impact decision-making and as a result, organizational performance, but within this context there are numerous theoretical and conceptual frameworks. For this case report however, the primary focus will be on the theory of planned behavior (TPB), the rational choice theory (RCT), and the dual processing theory (DPT).

The TPB is a concept that associates individual (i.e., employee) beliefs with behaviors and founded on those behaviors where employees can exert self-control with behavioral intent a key component. Principally, an employee's aim to implement a specific behavior is predicated on their attitude towards that behavior, the subjective norms as well as the observed behavioral controls [11], thus, an employee's motivation to perform a specific behavior is based on a favorable attitude towards that behavior, a favorable perception of whether the behavior is socially accepted, and a favorable perception of the ability to control the behavior. Therefore, organizations that are overly focused on procedural resources (e.g., policies) will be less effective in promoting and motivating employee compliance, if those resources are viewed as excessively complicated and burdensome.

Similarly, the RCT postulates that employees' behaviors are not dissimilar from economic exchanges where available options and potential outcomes are weighed, in other words, a perceived cost-benefit analysis [12], and depending upon the desired level of satisfaction, the employee chooses the most rational option that maximizes their (i.e., personal or individualized) advantages and gains. Consequently, oversight and compliance strategies that are not individually meaningful will likely not motivate compliant behavior and as a result, the need to impart meaningful values that are congruent with employees' beliefs, while at the same time distilling self-interest and promoting voluntary compliance is crucial to advancing organizational performance.

Last, the DPT suggests that employee decision-making is as a result of two different thought pathways, unconscious and conscious. Both pathways are used to learn and process information as well as to decide ethical behavior [13]. Using this theory, the first pathway of processing information is fast, automatic, and involuntary, typically unconscious, emotional and lacking self-control; information is intuitive, non-specific and without context. The second pathway however is slower, deliberate, and voluntary with information serial, explicit and detailed, therefore conscious. Given this framework, conscious attitudes and actions change over time with persuasion and training, while unconscious attitudes and intentions are less likely to change [14]. As a result, the ability to promote and motivate compliant employee behavior is presumably limited as unconscious attitudes which may negatively impact organizational performance and affect behavioral intention. Regardless, meaningful and effective resources (e.g., information security training) may influence conscious attitudes, and as a result positively impact employee decision-making.

There are intricate thought processes that impact human behavior and contrary to conventional thinking, the process for decision-making is not always logical; rather, it is often influenced by external factors that significantly impact employees' intentions. While information security oversight and compliance strategies cannot comprehensively address every potential behavioral eventuality, consideration of those factors that impact human behavior along with leaderships' involvement, effective procedural and technological strategies [15, 16] and deterrence campaigns [17] will garner significant influence and advance employee compliance in research information security through informed decision-making and as a result, organizational performance.

3. Methodology

Detailed information regarding the sample size, participant descriptors, data collection processes, measures, data analysis, and results are outlined in the data article, *[a]n exploration of research information security data affecting organizational compliance* (De Matas, Keegan, 2018) [18]. In brief, 103 compliance reports from site reviews conducted at research programs across a large federal healthcare organization that assessed compliance with information security policies and regulations were reviewed. Data obtained from those reviews were derived from in-depth interviews, document reviews, and physical evaluations of the research space. Analyses were conducted on compliance data aggregated in categories related to the resources primarily relied on for mitigating information security risk (i.e., behavioral, procedural, and technical).

4. Discussion

Based on this retrospective review of information security compliance assessment reports and associated data, the authors made several determinations. First the Veterans Health Administration (VHA) should be commended for developing and implementing information security oversight and compliance programs that contained technological (e.g., network monitoring, intrusion detection) and procedural (e.g., information security policies and procedures) strategies for detecting and mitigating research information security risk, and for its leadership's support and involvement in those programs. Second, employee awareness of information security requirements was prioritized by VHA and promulgated through mandatory new employee and annual training programs. These strategies undoubtedly limited unwarranted exposure to VHA research information and information systems but despite that, instances of noncompliance remained common.

While noncompliance related to technological strategies was rare, moderate levels of procedural noncompliance was observed across most areas of analysis including the

unauthorized use of external (non-VHA) information systems, inadequate management of research information (e.g., data security), inadequate reviews of research projects by subject matter experts for information security implications, unauthorized use and/or disclosure of sensitive information (i.e., privacy-related), noncompliant information security training requirements, and noncompliant reporting of research-related information security incidents. Consistent with that outcome, qualitative analyses revealed that despite the presence of detailed information security policies and procedures, those resources were often described as overly complicated and burdensome, leading to confusion, miscommunications, and implementation errors. To complicate matters further, information security subject matter experts were commonly viewed as lacking the requisite information security knowledge and abilities required to review and analyze complex scientific research material for information security implications. Thus, the ability to promote and motivate research information security compliance using procedural strategies was limited, as perceptions of available resources, including subject matter expertise, was less than favorable.

Not surprising, the highest levels of noncompliance observed across all areas of analysis was in the behavioral category. Employees attitudes towards information security requirements indicated that those requirements lacked individual meaning, and as a result, the completion of related tasks, perceived unfavorably. For example, while information security trainings were mandatory, and intended to convey basic information security requirements, those trainings were often viewed as tedious and unengaging, thus, they were less likely to distill individual behavior (e.g., value and emotional perceptions) or impart meaningful information security values that promoted and motivated compliant behavior [19].

Accordingly, while technological strategies for promoting and motivating information security compliance across VHA Research programs were mostly successful, procedural and behavioral strategies fell short of delivering the expected benefits, signifying the need for a more comprehensive approach to information security oversight and compliance strategies. Clearly consideration must be given to those factors that impact human behavior in order to encourage and advance voluntary compliance in research information security, and as a result employee decision-making and organizational performance.

5. Limitations

Although this case report involved a retrospective review of programmatic assessment data that positively contributed to existing information security literature regarding compliance and oversight, employee decision-making and organizational performance, it is important to acknowledge its limitations. Data were derived from onsite evaluation reports focused on VHA research programs only; therefore, results are based solely on those evaluations. In addition, qualitative assessments were made based on reviewer notes, and not on data derived directly from individual employees (e.g., through surveys).

6. Conclusion

The adoption of information security practices in research programs across a large federal healthcare organization was examined. Using onsite reports, the findings of noncompliance were clustered into three categories (i.e., procedural, technological and behavioral) with behavioral noncompliance at its highest levels across all areas of analysis. Additionally, the data demonstrated that the methodologies employed by VHA for promoting and ensuring compliance did not deliver the expected benefits, signifying the need for a more comprehensive approach to research information security compliance and oversight within VHA.

Acknowledgements

The authors wish to thank the Department of Veterans Affairs for its support in this project; however, it should be noted that the views presented in this paper are those of the authors and do not necessarily represent the views of the Department of Veterans Affairs.

References

[1] Ransbotham, S., Mitra, S. (2009). Choice and Chance: A conceptual model of paths to information security compromise. *Information Systems Research,* 20: 1: 121-139.

[2] Guest, G. Compliance cannot compel ethical behavior (2016). https://phys.org/news/2016-02-compliance-compel-ethical-behavior.html (accessed July 2017).

[3] Griffith, S. J. Corporate governance in an era of compliance (2016). *William & Mary Law Review,* 57 (6).

[4] Pahnila, S., Siponen, M., Mahmood, A. (2007). Employees' Behavior towards IS Security Policy Compliance. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.106.7038&rep=rep1&type=pdf (accessed November 2017).

[5] Haugh, T. (2017). The trouble with corporate compliance programs. *MIT Sloan Management Fall Review*.

[6] Kayworth, T., Whitten D. (2010). Effective information security requires a balance of social and technology factors. *MIS Quarterly Executive,* 9: 163–75.

[7] 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: 523-548.

[8] Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems,* 18: 151-164.

[9] Werlinger, R., Hawkey, K., Beznosov, K. (2008). Human, organizational and technological challenges of implementing

IT security in organizations, in *Proceedings of the Second International Symposium on Human Aspects of Information Security & Assurance (HAISA)*, Plymouth, UK, 35-47.

[10] Durgin, M. U. (2007). Understanding the Importance of and Implementing Internal Security Measures.

[11] Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes,* 50 (2): 179-211.

[12] Paternoster, R., Pogarsky, G. (2009). Rational choice, agency and thoughtfully reflective decision making: The short and long-term consequences of making good choices. *Journal of Quantitative Criminology,* 25 (2): 103-127.

[13] Kahneman, D. (2003). Maps of bounded rationality: psychology for behavioral economics. *American Economics Review,* 93 (5): 1449-1450.

[14] Haidt, J. (2013). The righteous mind: Why good people are divided by politics and religion. New York University, New York.

[15] Puhakainen, P. (2006). A design theory for information security awareness (working paper). Faculty of Science, University of Oulu, Finland.

[16] Willison, R. (2006). Understanding the perpetration of employee computer crime in the organizational context, *Information and Organization,* 16 (4): 304.

[17] 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).

[18] De Matas, S. S., & Keegan, B. P. (2018). An exploration of research information security data affecting organizational compliance. *Data in Brief*, *21*.

[19] Peterson, K. and McCleery, E. (2014). Evidence Brief: The effectiveness of mandatory computer-based trainings on government ethics, workplace harassment, or privacy and information security related topics. VA ESP Project #09-199.