ICRMAT 2020 Proceedings of the International Conference on Research in Management & Technovation pp. 137–142
DOI: 10.15439/2020KM1
ISSN 2300-5963 ACSIS, Vol. 24

A Perspective On The Intersection Of Information Security Policies And IA Awareness, Factoring In End-User Behavior

S. Raschid Muller, Ph.D., MBA
Assistant Professor of Cybersecurity
Capitol Technology University Laurel, MD, USA
Email - srmuller@captechu.edu
https://orcid.org/0000-0002-1742-7575

***Abstract*—In 2017 Executive Order 13800 was enacted for all federal entities to use the NIST Cybersecurity Framework to report on FISMA compliance. According to GAO-19-545 report sixteen agencies were identified as failing to successfully implement FISMA regulations rooted in information security policies (ISPs). This paper will introduce the link between information assurance awareness with the prescribed actions and its direct influence on information security policies. While organizations are conscious of the federal rules and regulations, most continue to fail to successfully implement and comply with the guidelines due to a sincere lack of information assurance and awareness, which ties directly into human behavior. A discussion on the intersection of information security awareness and behavior will be presented. The UTAUT theory measures and informs the researcher on factors that influence the end-user. Conclusively, recommendations will be offered on why organizations need to invest in a mechanism that measures these factors, which increases information awareness to change behavior, thus achieving better compliance with their organizational ISPs.**

***Index Terms*—ISPs, IA awareness, IT Governance, UTAUT, Behavior**

I. Introduction

IN 2002 as part of the E-Government Act, Congress enacted FISMA legislation to ensure that federal agencies begin to strengthen policies and practices. According to the GAO-19-545 Report [1] to Congress, sixteen agencies were identified as failing to implement FISMA regulations following the law successfully. The NIST Cybersecurity Framework was enacted in 2017 under Presidential Executive Order 13800 to report on FISMA compliance. The NIST Cybersecurity Framework has five core security functions: identify, protect, detect, respond, and recover. NIST requires these five functions to run concurrently to provide the necessary protections for federal agencies to manage their respective security measures continually.

This paper will focus on the information awareness aspect of the first core security function of Identify. Within this category, to comply, the agency must "develop and understand the organization's ability to manage Cybersecurity risks to systems, people, assets, data, and capabilities" [1]. As denoted in Figure 1 below from the 2019 report, 15/16 agencies failed to implement the first step of the five core security functions, which draws the question: If 93% of the audited agencies can't effectively implement the first of five core steps of NIST Cybersecurity Framework, then how effective will the agencies be in implementing the remaining four steps? Also, what conclusions can be drawn about the simple adoption of a policy that can be made about accepting the regulation as a whole? Is there a general sense in the federal space that Cybersecurity is not that important? Why aren't the agencies taking the mandatory regulations seriously and implementing the security controls required by the law? If employees are paid to implement security controls according to the law and aren't effective, why? The FISMA mandate is the foundation on which federal agencies need to focus on its information security governance. The general purpose is to develop the importance of understanding how human behavior contributes to organizational security policies' noncompliance.

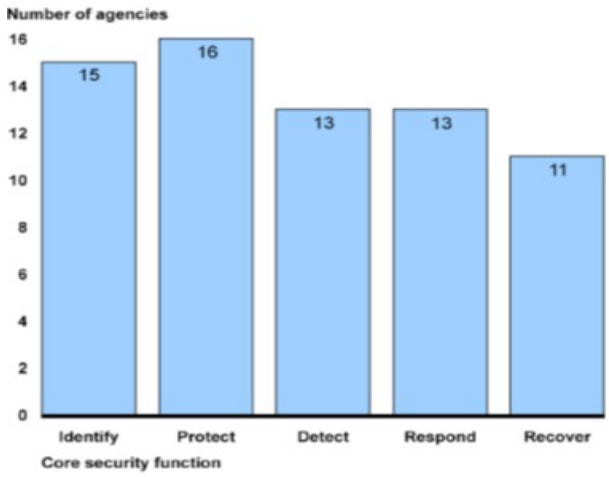

Fig 1. A graphic depicting how the sixteen agencies within the report were NOT in compliance with the five core security functions with the NIST framework [1]

There are several recognized academic theories in the information technology sector that address the behavior. The

paper will review peer-reviewed literature in the information security policy area. First, it must be understood those ISPs are the backbone of a solid security governance structure within any organization. Consistent adherence to the ISPs ensures the security and functionality of an organization are IT assets used for business and communication mediums. ISPs must also be continually reviewed, changed, adjusted, and adopted to address cyber threats' evolving nature.

These evolving cyber threats contribute to another significant part of information security governance within an organization: awareness. The concept of information assurance awareness plays a significant role in maintaining a security posture from the human perspective. NIST [2] often cites that humans pose the most considerable vulnerability to information system security. NIST SP 800-39 [2] offers a federal perspective and set of recommendations for information security leaders to be aware of the various threats to IT systems. NIST suggests that organizations develop, train, and maintain information security governance through continual monitoring and vigilant awareness.

Conclusively, the manuscript will seek to offer background on the chosen theory of behavior in the latest case studies. This research looks to extend the Unified Theory of Acceptance and Use of Technology (UTAUT) [3] to the federal sector. The UTAUT seeks to explain human behavior with the intent of using information systems by the end-user. Summarily the article will identify the importance of organizations studying and identifying end-user behavior in shaping future security policies that can be followed to provide better informational security governance.

II. Literature Review

A. GAO report - Highlights

The 2019 GAO report takes a detailed look at the several areas where the sixteen agencies are measured for effectiveness against the NIST Cybersecurity Framework for implementation following the information security program required by FISMA. The eight elements of the information security program are periodic risk assessments, cost-effective policies and procedures, subordinate plans for providing security, security training, periodic testing and evaluations of controls, remedial actions process, incident responses, and continuity of operations.

In Figure 2, 11/16 agencies failed to implement cost-effective policies and procedures, and 13/16 were unable to implement adequate security training, which is of great concern to the research conducted. Effective and iterative information security governance seems to allude to the various agencies at significantly high rates, which is unacceptable according to the GAO reports. The policies are required by law to be implemented as a baseline security standard.

As the baseline is often stress-tested with adversarial attacks from internal and externals threats, the information security policies must always be flexible and adaptive to the

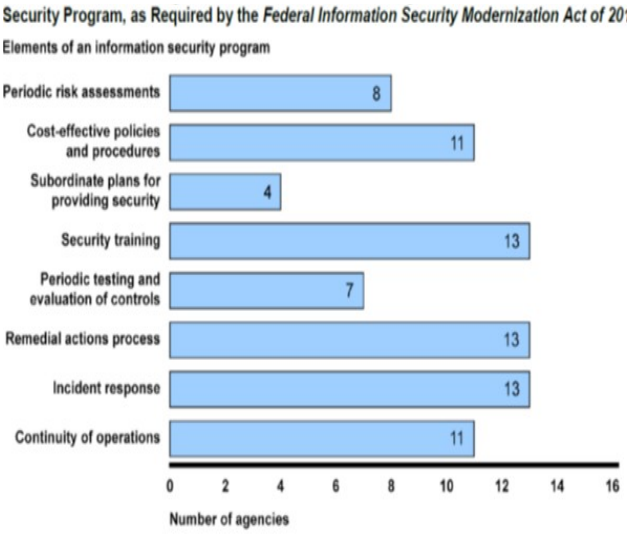

Fig 2. A graphic depicting how the sixteen agencies within the report were NOT in compliance with a FISMA information security program's eight elements [1].

environment when new vulnerabilities are introduced. In the same fashion where the Microsoft software platform provides continuous updates to vulnerabilities found that can compromise an operating system, the information security policies must have the same elasticity level for adaptation. Figure 3 below reflects report security incidents to US-CERT from 2009 – 2018. Note that the significant decrease in Cyber incidences in 2016 was reflective of a policy change, i.e., a shift in dollars invested in minor cyber incidences that could be adjudicated with the new concept of mandatory "continuous monitoring" that reflected low-level incidents like sniffing or probing networks that produced false positives on enterprise network defense commercial programs.

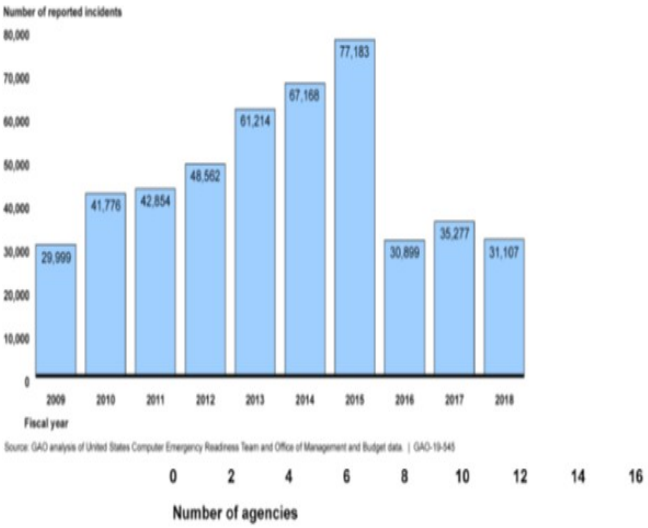

Fig 3. A graphic depicts federal agency reporting Cyber incidences from 2009 – 2018 [1].

B. Information Security Policies

The research literature on ISP compliance indicates that a general problem exists among employees who do not comply with prescribed information security policies [4]. It is also known that employees can be the most significant security threat to company information when they participate in risky behaviors such as accidentally installing viruses on company computers or using specific programs without prior knowledge [5]. Finally, Miller and Gregory [6] assert that consideration should be given to human behavior when authoring organizational policy. However, it is not known what human factors predict employees to not comply with existing corporate policies [7].

Employees are the major obstacle to the inadequate implementation of ISPs. In many cases, employees' security behaviors result in inadequately designed security policies [8]. Frequently, ISP methods focus on changing employees' behaviors because employers consider those behaviors unreasonable or erroneous, but compliance problems can result from inaccurate or inflexible ISPs. A few studies have shown that ISPs that do not reflect current work practices can also contribute to non-compliant security behaviors [9]. Kostadinov [10] asserts that information security policies (ISP) with an organization as a set of standards should be implemented for all end-users to gather compliance for information systems. Improved organizational, informational security factors are identified by research on ISP compliance conducted by various researchers and practitioners who seek explanations for the expected outcome [11]. Organizational information assets gain significant protections from the strict adherence to these ISPs in the form of complied governance.

Peltier [12] states that for organizations to achieve full compliance, the development, and delivery of effective policies must follow a sound and investigative strategy. However, Etsebeth [13] states that ISPs and security infrastructures are ineffective if the employees tasked with maintaining security do not understand data security expectations and demands. Developing structurally sound ISPs might be the most cost-effective action that organizations need to prevent information security breaches and incidents while not heavily relying upon its IT security staff when networks and information systems are being compromised [15].

This mandate can be achieved when every employee within the organization takes the fundamental responsibility or complying with ISPs and takes an active role in protecting data within the information system. Summarily, ISPs are needed in organizations so that researchers and practitioners can understand the expected outcomes of an awareness initiative and why this occurs [16].

C. Information Security Awareness

Ahlan, Lubis, and Lubis [17] define IT awareness as "a mental state where end-users recognize, comply, practices, and embed the prescribed organizational security policies into their work routine regularly." Consistent information security awareness is achieved when the organization's culture adopts the security policies achieving a higher rating in compliance and governance.

Research has shown that information security awareness can significantly impact security compliance behavior [18]. Haeussinger and Kranz [18] conducted a study examining the mediating effect of awareness on security behavioral compliance. The researchers also studied the institutional, individual, and environmental antecedents of information security awareness. Haeussinger and Kranz collected survey data from 475 employees and used the data to test their empirical model. Their model explained a substantial proportion of the variance of information security awareness (.50) and behavioral intention to comply (.41).

The results of Haeussinger and Kranz's study indicated that an organization's use of an ISP and employees' knowledge of information systems were the most influential antecedents of information security awareness. Haeussinger and Kranz also found that an employee's information security awareness alters the relationship between the antecedents of information security awareness and its behavioral intentions. Haeussinger and Kranz noted that the findings support the use of ISPs to encourage employees to engage in compliant behavior. Although information security managers often have limited resources to handle security demands, awareness and training programs can help managers and information assurance professionals to do their jobs more effectively [19].

Information systems database breaches that make the news are usually external threats versus internal [20]. While those breaches can be too costly, outsider threats are generally addressed using traditional security measures. Some organizations attempt to avert information security issues by focusing on technical solutions. Still, Yildirim [19] acknowledged that the effective management of information security requires an organization to address human factors. Yildirim recommended that managers take several security countermeasures that combine technical and social interventions using an integrated, systematic process.

The research on information security is extensive, yet while most concepts regarding information security have been reviewed and discussed in the existing literature, some critical areas remain unaddressed [21]. For example, few studies examined information security awareness training [17]. Conclusive empirical evidence showing the effectiveness of security awareness training or awareness campaigns is not available [22]. Pahnila et al. [22] noted that evidence does exist to support the effectiveness of training activities and informational campaigns in other fields. As a result, there is scholarly interest in assessing the value of information security awareness training and ISP compliance.

Because of the difficulty in teaching general users about complex security issues and users' tendency to be inattentive to security concerns, users may not always apply what they know about their organizations' security standards [23]. Figure 4 contains an illustration of how security

awareness training translates into actual security behavior. In Step 1 of the security awareness process, users undergo security awareness training. Users are exposed to information security materials showing correct and incorrect actions. These security behaviors are referred to as explicit behaviors.

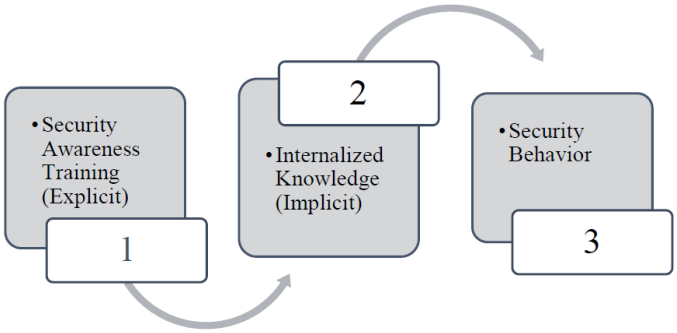

Fig. 4 A theoretical model of how security awareness training affects behavior [23]

In Step 2, after being presented with the information security awareness material, users must complete a short test measuring the extent of the internalized message. The internalized knowledge is referred to as implicit behavior. Finally, in Step 3, employees' actual behavior is measured to test whether information security behaviors changed due to awareness training and whether appropriate behaviors require internalized understanding [23]

Employees can be the most significant security threat to company information when they participate in risky behaviors [24]. An abundance of recent research has focused on employees' risky behaviors [25]. Examples of those behaviors include accidentally installing viruses on company computers and using questionable software programs without permission or prior knowledge. IT systems are dependent on employees' behavioral compliance with security requirements [23]. Without information security awareness training and a commitment to compliance, people's intentional and unintentional actions cause adverse consequences that negatively impact organizations [26].

Deepa [27] states that many organizations utilize information security awareness training to support information assurance professionals' use of advanced information security technology. Organizations do not always offer information security awareness training to regular users, and the lack of focused training makes employees the weakest link in any organization [27]. While many organizations recognize people as their primary asset and risk, some organizations do not adequately address insider threats and vulnerabilities, nor do they assess the security practices of third-party partners and supply chains [28]. Training is often needed to maximize the benefits of human assets and minimize risks. In addition to training, another way to maximize human assets and reduce information security risk is to implement ISPs that provide employees with guidelines and structure when dealing with information security.

D. UTAUT2 and Behavior

Scholars have proposed many theories and frameworks to understand and predict users' behaviors regarding technology acceptance, adoption, and use [7]. The many different frameworks represent evolving perceptions of the drivers of users' attitudes toward technology. One of the more recent models proposed to explain technology-related behavior is the UTAUT2 [14].

Venkatesh et al.'s [14] UTAUT2 was an extension of the original UTAUT. The UTAUT2 framework was designed to explain the interaction between seven intrinsic and extrinsic variables and users' behavioral intentions regarding technology [14]. The present study examined four intrinsic factors included in the UTAUT2 as predictor variables: performance expectancy, effort expectancy, hedonic motivation, and habit. The present study examined three additional extrinsic factors included in the UTAUT2 as predictor variables: social influence, facilitating conditions, and price value. Researchers have used UTAUT2 as a predictive framework [7]. As such, the UTAUT2 was deemed an appropriate tool to examine factors that might predict end-users' behavioral intentions to comply with ISPs. Figure 2 presents the relationships between the variables in the UTAUT2 model.

Figure 5 illustrates Venkatesh et al.'s [14] addition of hedonic motivation, price value, and habit as predictors of behavioral intentions and user behavior. The causal networks of the influence matrix in the UTAUT2 are based on dimensions and criteria that demonstrate the perceived usefulness, complexity, social factors, perceived behavioral control, interest, quality, past behavior, service quality, and usage time on behavioral intention [14]. Perceived behavioral control "reflects perceptions of internal and external constraints on behavior and encompasses self-efficacy, resource facilitating conditions, and technology facilitating conditions" [3]. In Venkatesh et al.'s [3] research, performance expectancy, effort expectancy, social influence, facilitating conditions, hedonic motivation, price value, and habit had the highest impact as predictors of behavioral intentions to accept and use technology.

Venkatesh et al. [14] stated that facilitating conditions depends on the users' perception of technical support when using technology. Subsequent research has shown that hedonic motivation also remains a significant factor in the acceptance and use of new technology [29]. Hedonic motivation has not been thoroughly explored in the context of ISP compliance, highlighting a need for the present study. Additionally, Arenas-Gaitán, Peral-Peral, and Ramon-Jeronimo [30] noted that price value creates doubt about an end-user's role in adopting technologies when making financial decisions. Arenas-Gaitán et al. [30] also argued that habit, one of the UTAUT2 factors, directly and indirectly, affects end-user's behavioral intention to comply with ISPs in organizations.

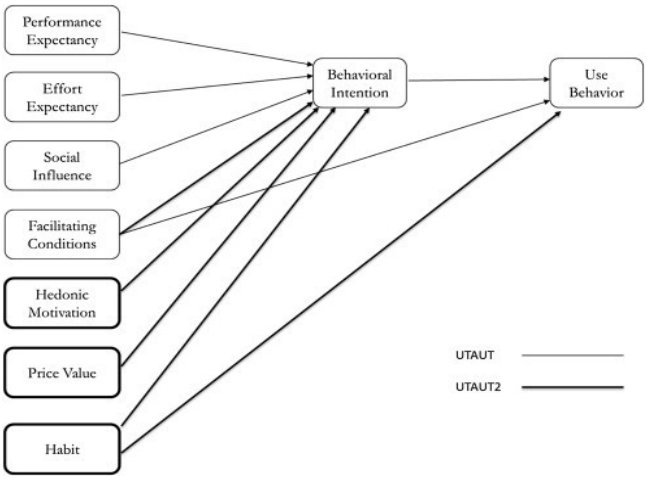

Fig 5. UTAUT and UTAUT2 factors [14].

Thus, the use of the UTAUT2 in the present study addressed a gap in the research literature and contributed to knowledge about end-users' behavioral intentions to comply with ISPs [31].

Lebek et al. [11] suggested that a theory of ISP awareness is needed for researchers and practitioners to understand awareness initiatives' expected outcomes. The UTAUT2 [14] theoretical framework can help scholars and practitioners understand how and why information security awareness initiatives influence end-users' behavioral intentions [23].

III. Conclusion and Recommendations

Scholars have acknowledged that employees' noncompliance with ISPs could result in inadequate information security [9]. Furthermore, the information security threats' scope requires information security and information assurance professionals to focus on protocols and processes that can offer protection against those threats to develop effective ISPs [32]. Developing a better understanding of the behavioral factors that influence ISP compliance among employees might improve organizational data security [33]. Continual training programs and policy guidelines explicitly designed for end-users may be more effective if structure and routine are emphasized rather than benefits associated with performance benefits, ease of use, technical support systems, social expectations, or cost considerations. Such an approach would work to highlight the importance of developing compliance habits.

Studies frequently focus on behavioral intentions to comply instead of observed ISP compliance behaviors [34]. The use of the behavioral intention construct means that the link between technology adoption factors and observed compliance behaviors has not been thoroughly investigated. By designing a study that allowed employers to tracked compliance behaviors, the need to make assumptions about some variable relationships would be reduced. Studies could also be conducted that determine the importance of information security awareness by measuring employees' attitudes and behaviors both before and after information security awareness training. Such research would necessitate a quasi-experimental approach, as multiple measures would be administered [17]. Studies investigating the effectiveness of security awareness training or awareness campaigns are not readily available. As a result, researchers must make assumptions about awareness factors that influence employee attitudes and self-efficacy beliefs about information security.

Summarily, in reflecting upon the theories and research to address the lapses reported by the 2019 GAO report, it is recommended that outside of the routine federal OMB directives with Congressional oversight, that the federal government take an approach of offering assistance in bringing the agencies up to speed with a corrective plan of action. This plan would take an in-depth analysis of the process and the employees entrusted with the security of the information systems and associated processes. Stricter laws and regulations in accountability that require the forfeiture of fines and criminal/civil penalties could be implemented. Conclusively, after the Office of Personnel Management records breach in April of 2014, the federal agencies are still not correctly performing the necessary steps to safeguard information systems directly tied to national security and the intelligence apparatus. Hopefully it won't take the losses of livelihoods from an economic perspective or, more importantly, American lives from a national defense perspective before agencies align with following the directives set forth by OMB.

References:

[1] Government Accountability Office (GAO) Report # 19-545. Federal Information Security: Agencies and OMB Need to Strengthen Policies and Practices, 2019. https://www.gao.gov/assets/710/700588.pdf [Accessed October 10, 2020]

[2] National Institute of Standards and Technology (2011) Managing Information Security Risk: Organization, Mission, and Information System View, Special Publications (SP PUBS) 800-39, 2011. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf. [Accessed October 9, 2020]

[3] V. Venkatesh, M. Morris, G. Davis, and F. Davis. User acceptance of information technology: Toward a unified view, 2003. MIS Quarterly, 27, 425-478. doi:10.2307/30036540. [Accessed October 9, 2020]

[4] K. Quigley, C. Burns, and K. Stallard, K. Cyber gurus: A rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection, 2015. Government Information Quarterly. Retrieved from http://doi.org/10.1016/j.giq.2015.02.001 [Accessed October 21, 2020]

[5] S. Lupin, H. Tun, A. Thike, and M. Puschin. Hybrid modeling as a tool for analysis of information systems security. In Proceedings of the 2016 IEEE North West Russia Young Researchers in Electrical and Electronic Engineering Conference (EIConRusNW), 2016 (pp. 259-261). Piscataway, NJ: IEEE. [Accessed October 3, 2020]

[6] L. Miller, and H. Gregory. CISSP and information security education, training, and awareness, 2016. Retrieved from http://www.dummies.com/programming/certification/cissp-information-security-education-training-awareness/. [Accessed October 3, 2020]

[7] C. Huang, and Y. Kao. UTAUT2 based predictions of factors influencing the technology acceptance of phablets by DNP. Mathematical Problems in Engineering, 2015, 1-23. doi:10.1155/2015/603747 [Accessed October 3, 2020]

[8] B. Stahl, N. Doherty, and M. Shaw. Information security policies in the UK healthcare sector: A critical evaluation. Information Systems Journal, 22, 77-94, 2012. doi:10.1111/j.1365-2575.2011.00378.x. [Accessed October 1, 2020]

[9] E. Kolkowska, F. Karlsson, and K. Hedström. Towards analyzing the rationale of information security noncompliance: Devising a value-based compliance analysis method. The Journal of Strategic Information Systems, 26, 39-57, 2017. doi:10.1016/j.jsis.2016.08.005 [Accessed October 10, 2020]

[10] D. Kostadinov. Key elements of an information security policy, 2014. Retrieved from https://resources.infosecinstitute.com/key-elements-information-security-policy/#gref [Accessed October 5, 2020]

[11] B. Lebek, J. Uffen, M. Neumann, B. Hohler, and M. Breitner. Information security awareness and behavior: A theory-based literature review. Management Research Review, 37, 1049-1092, 2014). doi:10.1108/MRR-04-2013-0085 [Accessed October 5, 2020]

[12] T. Peltier. Information security policies, procedures, standards: Guidelines for effective information security management, 2016. Boca Raton, FL: CRC Press. [Accessed October 6, 2020]

[13] V. Etsebeth. Information security policies: The legal risk of uninformed personnel. Paper presented at the ISSA 2006 From Insight to Foresight Conference, Sandton, South Africa, 2006. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.145.1602&rep=rep1&type=pdf [Accessed October 6, 2020]

[14] V. Venkatesh, J. Thong, and X. Xu. Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology, 2012. MIS Quarterly, 36, 157-178. doi:10.2307/41410412. [Accessed October 5, 2020]

[15] S. Fourtané. How 'defense in depth' gets data protection right, 2018. Retrieved from https://www.securitynow.com/author.asp?section_id=613&doc_id=741221 [Accessed October 5, 2020]

[16] J. Hammarstrand, and T. Fu. Information security awareness and behavior: Of trained and untrained home users in Sweden, 2015. Retrieved from http://www.diva-portal.se/smash/get/diva2:950568/FULLTEXT01.pdf. [Accessed October 5, 2020]

[17] A. Ahlan, M. Lubis, and A. Lubis Information security awareness at the knowledge-based institution: Its antecedents and measures. Procedia Computer Science, 72, 361-373, 2015. doi:10.1016/j.procs.2015.12.151 [Accessed October 5, 2020]

[18] F. Haeussinger, and J. Kranz. Information security awareness: Its antecedents and mediating effects on security compliant behavior. Paper presented at the Thirty-fourth International Conference on Information Systems, Milan, Germany, 2013. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.669.8230&rep=rep1&type=pdf [Accessed October 15, 2020]

[19] E. Yildirim. The importance of information security awareness for the success of business enterprises. In D. Nicholson (Ed.), Advances in human factors in cybersecurity: Advances in intelligent systems and computing (Vol. 501, pp. 211-212), 2016. Cham, Switzerland: Springer. [Accessed October 15, 2020]

[20] N. Giandomenico, and J. de Groot. Insider vs. outsider data security threats: What's the greater risk, 2018. Retrieved from https://digitalguardian.com/blog/insider-outsider-data-security-threats. [Accessed October 15, 2020]

[21] M. Heckman, and R. Schell. Using proven reference monitor patterns for security evaluation. Information, 7(2), 23-32, 2016. doi:10.3390/info7020023 [Accessed October 15, 2020]

[22] S. Pahnila, M. Siponen, and A. Mahmood. Employees' behavior towards IS security policy compliance. In R. H. Srague, Jr. (Ed.), Proceedings of the 40th annual Hawaii International Conference on System Sciences (pp. 156-165), 2007. Piscataway, NJ: IEEE. [Accessed October 15, 2020]

[23] A. Stephanou, and R. Dagada. The impact of information security awareness training on information. Security behavior: The case for further research. In H. Venter, M. Eloff, J. Eloff, & L. Labuschagne (Eds.), Information security for South Africa: Proceedings of the ISSA 2008 Innovative Minds Conference (pp. 311-330), 2008. Pretoria, South Africa: Information Security South Africa [Accessed October 15, 2020]

[24] J. Andress. The basics of information security: Understanding the fundamentals of infosec in theory and practice, 2015. Rockland, MA: Syngress. [Accessed October 5, 2020]

[25] A. Shameli-Sendi, R. Aghababaei-Barzegar, and M. Cheriet, M. Taxonomy of information security risk assessment (ISRA). Computers & Security, 57, 14-30, 2016. doi:10.1016/j.cose.2015.11.001/ [Accessed October 5, 2020]

[26] F. Aloul. The need for effective information security awareness. Journal of Advances in Information Technology, 3, 176-183, 2012. doi:10.4304/jait.3.3.176-183. [Accessed October 15, 2020]

[27] T. Deepa. Survey on need for cyber security in India. Unpublished manuscript, Acharya Institute of Technology, Bangalore, Karnataka, India, 2014. doi:10.10.13140/2.1.4555.7768 [Accessed October 15, 2020]

[28] D. Shackleford. Combating cyber risks in the supply chain. SANS Institute, 2015. Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/combatting-cyber-risks-supply-chain-36252. [Accessed October 15, 2020]

[29] H. Kyriakou, J. Nickerson, and G. Sabnis. Knowledge reuse for customization: Metamodels in an open design community for 3D printing. MIS Quarterly, 41, 315-332, 2017. doi:10.25300/MISQ/2017/41.1/17. [Accessed October 15, 2020]

[30] J. Arenas-Gaitán, B. Peral-Peral, and M. Ramon-Jeronimo. Elderly and internet banking: An application of UTAUT2. Journal of Internet Banking and Commerce, 20(1), 1-23, 2015. Retrieved from http://www.icommercecentral.com [Accessed October 15, 2020]

[31] S. Muller, and M. Lind. Factors in information assurance professionals' intentions to adhere to information security policies. International Journal of Systems and Software Security and Protection, 11(1), 2020. Hershey, PA: IGI Global [Accessed October 15, 2020]

[32] F. Alqahtani. Developing an information security policy: A case study approach. Procedia Computer Science, 124, 691-697, 2017. doi:10.1016/j.procs.2017.12.206. [Accessed October 5, 2020]

[33] N. Lord. Data security experts reveal the biggest mistakes companies make with data and information security, 2018. Retrieved from https://digitalguardian.com/blog/data-security-experts-reveal-biggest-mistakes-companies-make-data-information-security [Accessed October 5, 2020]

[34] N. Humaidi, and V. Balakrishnan. Leadership styles and information security compliance behavior: The mediator effect of information security awareness. International Journal of Information and Education Technology, 5, 311-318, 2015. doi:10.7763/IJIET.2015.V5.522

Dr. S. Raschid Muller is a Senior Cybersecurity SME with the Department of Defense (DoD) at Fort Meade, Maryland. He teaches Cybersecurity at the undergraduate and graduate levels at Arizona State University, University of Maryland Global Campus, and Capitol Technology University. Dr. Muller is a 2020 Brookings Institute Fellow (LEGIS) currently serving on the House Committee for Homeland Security assigned to the Cybersecurity, Infrastructure Protection, and Innovation subcommittee in the United States Congress. He will attend U.C. Berkeley's Executive Leadership Academy in 2021 as a Fellow in the Goldman School of Public Policy. He is a member of IEEE, ISACA, NDIA, and AFCEA.