CYBERSECURITY PERSPECTIVES

EMPLOYEE CYBER SECURITY AWARENESS TRAINING MATTERS

Frederick L. Hicks

Paper 2 | September 2019

Suggested Citation:

Hicks, F.L. (2019). Employee Cyber Security Awareness Training Matters. *AICL Cybersecurity Perspectives*, Paper 2, accessed on September 29, 2019, https://www.americascyber.org/cyberperspectives.

ABSTRACT

Ransomware attacks and data breaches are here to stay. Successful attacks stem from human errors within organizations. Chief Information Security Officers (CISOs) must garner the support of everyone, especially leadership to counter the attacks. Arsenal for organizations starts with cybersecurity awareness training and the existence of cyber security policies. Board of Director and Executive level cybersecurity awareness are pivotal toward organization-wide awareness of the severity and impact of cyber-attacks. Organization resources are scarce, nevertheless, any organization investments in cybersecurity awareness training garners definite returns. Organization cybersecurity is a continuous activity. Everyone in the organization must share this critical function to mitigate information security attacks. Human capital in organizations can become effective tools to reduce vulnerabilities.

1. INTRODUCTION

Headlines continue to report successful ransomware attacks and data breaches. These occurrences result in heavy monetary costs from legal fees and victim payouts. These attacks are here to stay. Information security professionals deploy a plethora of technology solutions and policies to defend against attacks; however, humans remain the largest threat to information security. Researchers emphasize hackers target people not computers (Safa et al 2016). Further, Shultz (2005) reminds us information security is primarily a people problem because people make technology and people run technology; this provides room for human errors. Ten years ago, researchers demonstrated between 50%-75% of security incidents originate from within an organization (D'arcy et al 2009).

These statistics continue to prevail according to a recent 2018 Insider Threat report where researchers found 53% of the attacks against companies were insider attacks (Schulze, 2018). Security professionals need to focus on the human aspects of information security. Therefore, to address these present issues to organizations' information security programs, we explore: *(1) the area to which Chief Information Security Officers (CISOs) should focus on to improve information security, and (2) how this approach can complement (or improve) security policy compliance.* CISOs must focus on information security awareness to maximize the human assets. To reduce the number of human errors, employees must grow more aware of the information security threats and equivalent protections.

2. EMPLOYEE AWARENESS FOCUS

The majority of the CISO's focus must be the proper development of an organization wide implementation of an *employee information security awareness and training program*. An organization's information security resources are scarce. As a result, The CISO must carefully allocate resources while ensuring the effective manner in which they address the security challenges of the organization. She should invest the limited resources on awareness and training to increase

cybersecurity policy compliance. When users are knowledgeable regarding information security risks, they may help improve the organization's information security practices (Spears and Barki 2010).

Users who are more aware may act proactively by taking steps to secure the organizations information assets. To align information security efforts for the organization, the CISO must start at the top. With direct support from executive management, employees actualize "value" of the information assets. This approach posits that user awareness of security countermeasures directly influences the punitive measures implemented by organizations to resolve information systems misuse associated with human errors. Creditable research results suggest three practices deter information security misuse: (a) user awareness of security policies; (b) security education, training, and awareness (SETA) programs; and (c) computer monitoring (D'Arcy et al 2009). Factors (a) and (b) above depend on human behavior to be aware and comply with information security policies.

3. MORE AWARENESS EQUALS COMPLIANCE

The CISO can improve compliance with information security policy through several approaches. One goal of a tailored C-level security awareness training is the CISO's ability to garner support from executive management to emphasize to organization's staff that information security is everyone's responsibility. Traditionally end users perceive information security is the sole responsibility of the Information Technology (IT) department. Once knowledge spreads that it is a shared task, individuals may decide to defend an organization's information assets. Research finds that information security knowledge sharing, collaboration, and other factors have a significant effect on employees' attitude towards compliance with organizational information security policies (Safa et al 2016). Further, alignment of information security with the organization's outcomes helps to ensure employee's ability to see how their compliance affects the organizations overall performance. Conversely, employees also discover how their non-compliance may lead to unwanted circumstances such as sanctions or fines. This is extremely important for

banking institutions or hospitals who must comply with regulations such as Health Insurance Portability and Accountability Act of 1996.

Second, the information security goals and objectives established by the CISO must be very clear to the staff who must comply. Clarification occurs during the Security Education Training and Awareness program. Compliance increases when end users understand what non-compliance is. Further, when end users understand how noncompliance hurts the organization's bottom line, they may be more prone to comply. For example, if a banking institution faces legal penalties for violating information security policies, which affect their customers, the bank may have to pay heavy legal fees, fines, and members may face other harsh penalties. Wells Fargo faced heavy fines for internal data breaches (Stempel, 2019).

Third, organizations often use a checkbox approach to evaluate their information security program implementation. Unfortunately, information security is an on-going effort. Employees must continuously comply with the information security policies. SETA programs must occur throughout the year. Because employees come and go, the organization maintain information security training for new arrivals. Finally, the CISO must invest resources to ensure the user awareness-training program is successful to improve information security compliance. Resources for a successful SETA initiative must ensure include qualified information security trainers, evaluations of employees, leadership commitment, and sustainability. Successful programs measure effectiveness and is tailored to the needs of each audience. Successful security training programs are also hands-on and accountable. CISOs must ensure the security awareness training is mandatory for all staff.

4. CONCLUSION

The majority of organizations rely on technology alone to solve the information security threats. Technology controls cannot solely guarantee a secure environment for information systems. Organizations must consider the human aspects of information security. Cyber

security threats will continue to target humans who operate the technology and data systems. With the proper security awareness training, humans can become the key to ensure an organization's information system confidentiality, integrity, and availability are intact.

REFERENCES

D'Arcy, J., Hovav, A., and Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*(1), 79-98.

"Health Information Privacy." *HHS.gov*, 4 Jan. 2019, www.hhs.gov/hipaa/index.html.

Safa, N., Solms, R., and Furnell, S. (2016). Information Security Policy Compliance Model in Organizations. *Computers and Security*, 56, 1-13.

Schultz, E. (2005). The human factor in security. *Computers & Security*, 24, 425-6.

Schulze, K. (2018). *Insider Threat Report. Insider Threat Report.* CA. Retrieved from https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf

Spears, J., and Barki, H (2010). User participation in information systems security risk management. *MIS Quarterly,* 503-522.

Stempel, J. (2019, March 1). Wells Fargo officials enter $240 million settlement over bogus accounts. Retrieved October 27, 2019, from https://www.reuters.com/article/us-wells-fargo-settlement/wells-fargo-officials-enter-240-million-settlement-over-bogus-accounts-idUSKCN1QI4P3.

Whitman, M., and Mattord, H. (2004). Principles of Information Security, 2nd Edition. Cengage Learning.

AUTHOR BIOGRAPHY

Frederick L. Hicks has over 30-years of Information Technology C-level management experience in not-for-profit agencies in south Florida. Hicks holds a Master's in Management from St. Thomas University. Currently, he is the CIO at the Early Learning Coalition of Miami-Dade and Monroe. He is also a 2nd year Executive Doctoral student in the School of Business at St. Thomas University for Information Security. Hicks is the recipient of the 2016 Technology Leader Award from the Miami Chamber of Commerce. Hicks is an America Institute for Cyber Leadership (AICL) fellow.