6-2017

The policy-practice gap: Describing discordances between regulation on paper and organizational practices

David Sikolia
Illinois State University, dsikoli@ilstu.edu

David Biros
Oklahoma State University, david.biros@okstate.edu

The policy-practice gap: Describing discordances between regulation on paper and organizational practices

David Sikolia
Illinois State University
dsikoli@ilstu.edu

David Biros
Oklahoma State University
David.Biros@okstate.edu

EXTENDED ABSTRACT

Lack of employee training and awareness of information security issues is a leading cause of breaches and incidents. A 2015 security survey by Ernst and Young suggests that careless or unaware employees are the leading security vulnerability. A 2016 survey by Price Waterhouse Coopers (PWC)(2017a) found that 47 percent of the respondent companies did not have an employee security and awareness program. For the 53 percent of the organizations that do conduct training, there is little information on the form (i.e. instructor lead, computer/web based interactive, or a simple PowerPoint presentation sent to employees), the length, the appropriateness, and the frequency of recurrence. Further, a 2016 survey by the Information Systems Audit and Control Association (ISACA)(2017b) of nearly 3000 information security professionals found that social engineering and insider threat (both malicious and accidental) were two of the top three security concerns. These issues could be addressed with proper information security and awareness training.

Interestingly, in the past 10-15 years, a number of laws were passed that require organization to perform employee security and awareness training. The Federal Information Security and Modernization Act (FISMA) requires government agencies and those companies that conduct business with the Federal government to conduct security awareness training. The Health Insurance Portability and Accountability Act (HIPAA) requires that hospital, clinics, and doctors' offices must "implement a security awareness and training program for all members of its workforce." Not only does the law apply to medical offices, but also to dental offices, optometry offices, and any organization or company that handles patient data. The Family Educational Rights and Privacy Act (FERPA) requires the same type of training for employees in government and private educational institutions that handle student educational records and data. It also applies to companies and organizations that handle student records. Other laws and standards such as the Gramm-Leach-Bliley Act and the Payment Cared Industry Data Security Standard (PCI-DSS) require organizations to conduct employee information security and awareness training as well.

There are a number of laws that require security awareness training for organizations to be in compliance, yet it appears not all organizations conduct any of the required training. The purpose of this study is to understand the level of compliance with the laws by organizations from various industries. Furthermore, we seek to understand why organizations fail to comply with the training requirements. We will begin by enumerating the various laws, regulations, standards and guidelines. Then we will develop a survey instrument (questionnaire) tailored to the various industries, in accordance with the applicable regulations. Then the questionnaire will be send to the relevant authorities (Chief information officers, Chief technology officers etc.) in each organization that would be willing to participate. The feedback will be analyzed to determine the policy-practice gap. Furthermore, we will seek to understand from the data why there is a policy-practice gap. The results will be shared with the practitioners, in addition to providing us with guidance on further, future research.

Keywords

Information security, security awareness training

References

2017a. "The Global State of Information Security® Survey 2017." Retrieved 02/22/2017, 2017, from http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/assets/gsiss-report-cybersecurity-privacy-possibilities.pdf

2017b. "State of Cyber Security 2017." Retrieved 2/22/2017, 2017, from http://www.isaca.org/cyber/pages/state-of-cyber-security-2017.aspx