Editorial: Time to move away from compliance – cybersecurity in the context of needs and investments of organizations

Cybersecurity this far has been considered a compliance issue where employees are expected to obey the security policies, and organizations need to follow the legislation. Much of the research has focused on the compliance behavior of individuals and organizations as well. Most of the security in large organizations is assessed by consultants who use standard checklists to evaluate compliance with legislation and standards with little regard to return on investment or other business objectives. While we teach our students nuances of assessing organizational cybersecurity through a lens of classic risk analysis where assets, vulnerabilities and threats are used to compute the potential exposure to the firms, then controls are determined by rigorous cost-benefit analysis. In reality, a lack of data and the complexity of analysis drive security assessments for compliance via checklists. While security needs are driven by specific contexts (industry, size, threats and resources), most companies follow the same standards and guidelines for security to simplify the process. As technology advances and the impact of cyber breaches magnify, we need to consider cybersecurity in the context of the needs and investments specific to organizations.

Return on investment (ROI) is a key metric for organizations; however, it is not commonly used for cybersecurity. One of the reasons is that cybersecurity is not a profit-making enterprise but rather a service for the organization. We need to find an alternative standard for measuring the value of cybersecurity, perhaps as savings in terms of expected losses if security were not implemented. The challenge lies in the difficulty to accurately compute the expected losses given the high complexity of the problem, constantly shifting environments (legislative, technology and threat landscape) and variability in the organizational context. Even the financial markets are not able to assess the impact of cybersecurity breaches accurately and have largely ignored breaches unless they are massive. Companies, thus, increasingly resort to purchasing cyber insurance (GAO Report) [1]. However, insurance companies struggle with the uncertainty as their premiums continue to escalate.

How can academic researchers help corral the problem to make it more tractable? While we advocate moving away from a one size fits all checklist approach, we should perhaps relax the notion of calculating a precise ROI for security due to its impracticality. It might be pertinent to find a middle ground where we define organizations across multiple dimensions to assess the value of security. Much research is needed in the field to make cybersecurity risk management more efficient and cost-effective. The papers appearing in this second issue

Organizational Cybersecurity Journal: Practice, Process and People
Vol. 2 No. 1, 2022
pp. 1-2
Emerald Publishing Limited
e-ISSN: 2635-0289
p-ISSN: 2635-0270
DOI 10.1108/OCJ-05-2022-018

challenge our current understanding of cyber risks and the role of organizational factors in varying contexts from Sweden's nuclear power industry to German family-owned businesses.

Gyllensten and Torner focus on how the work organization and psychosocial working conditions influence the employees' ability and motivation to contribute to information security. The authors draw attention to inherent value conflicts emanating from the misalignment of organizational values with security values. Based on data from the nuclear power industry, this study establishes the critical role of well-adapted rules, supportive organizational culture and individual responsibility for employees' participative and rule-compliant security behavior.

Ulrich, Timmermann and Frank study the impact of family (owned) business characteristics on the approach to cyber risk defense. The authors make an interesting finding that even though family businesses see employees as a greater risk, they do not invest adequately in cybersecurity as compared with nonfamily businesses. The omission of organizational aspects and routines may be to maintain their position in the family network.

Mohammed emphasizes the importance of developing effective strategies in the event of a data breach to mitigate their impact on functional areas and affected stakeholders. The author relies on the service failure literature to propose concentrating organizational efforts on customer recovery, employee recovery, process recovery and regulatory recovery. These recovery areas are critical when resolving data breaches and may have a severe impact on an organization.

The next big frontier for information technology is emerging to be cyber-physical systems. The pervasive use of sensors and associated automatic actuators in physical systems raises the criticality for security where life and property are at stake. The cybersecurity needs are going to be dramatically different for such systems. It is thus crucial to move away from universal standards for cybersecurity to more nuanced implementation of security using classic risk management and pragmatic means to compute the value for security investments while taking cognizance of organizational contextual factors.

Gurvirender Tejay and Sanjay Goel

Note

1. https://www.gao.gov/products/gao-21-477