Developing a cybersecurity culture to influence employee behavior

Jean-Loup Richet

In our increasingly connected world, cybersecurity has become a critical concern for individuals, businesses, and governments alike. With the ever-growing threat of cyberattacks, it is more important than ever to raise awareness of cybersecurity risks and best practices. By promoting cybersecurity awareness, we can help protect ourselves and our data from malicious actors (Richet, 2021). Cybersecurity awareness helps to educate individuals about the dangers of cybercrime and the importance of taking steps to protect themselves online... But also to comply with organizational rules and deter them from deviant behaviors!

When it comes to deterring employee deviant behavior in information security, sanctions are one of the most commonly used methods. Organizations have long used sanctions as a way to deter employees from committing fraud. Sanctions can range from financial penalties to termination of employment.

However, research on this topic has been mixed, with some studies showing that sanctions are effective and others indicating that they are not. Trang & Brendel (2019) take a closer look at the role of sanctions in deterring employee deviant behavior and explore how contextual and methodological moderators can impact this deterrence approach. Their findings suggest that while sanctions have an overall effect on deviant behavior, their effectiveness depends on the context in which they are implemented and the methodology used to study them. In particular, they find that deterrence theory is more likely to predict deviant behavior in malicious contexts, cultures with a high degree of power distance, and cultures with high uncertainty avoidance. By understanding the moderating effect of these contextual and methodological factors, organizations can better design sanction mechanisms that are tailored to their specific needs and objectives.

There is a growing body of evidence that suggests organizations with strong cybersecurity cultures are better equipped to manage cyber risks, to protect their data and systems, but also to manage employee deviant behaviors. Practitioner research (IBM, 2021) found that organizations with a security-conscious culture are three times more likely to have comprehensive security programs in place and four times less likely to experience a data breach originating from an insider.

While the benefits of a strong cybersecurity culture are clear, developing such a culture is no easy task. Alshaikh (2020) identify and explain five key initiatives that three Australian organizations have implemented to improve their respective cyber security cultures. The five key initiatives are: identifying key cyber security behaviors, establishing a 'cyber security champion' network, developing a brand for the cyber team, building a cyber security hub, and aligning security awareness activities with internal and external campaigns. These key initiatives have helped organizations exceed minimal standards-compliance to create functional cyber security cultures. Organizations looking to improve their cybersecurity culture should consider implementing some or all of these five key initiatives. By doing so, they will be better positioned to manage cyber risks and protect their data and systems. It will also help them to create a culture of security within organizations, making it more likely that employees will report suspicious activity, take precautions to prevent attacks, and comply with information security policy. In addition, raising awareness of cybersecurity issues can help to better inform policymakers as they work to enact laws and regulations to promote cybersecurity and protect our interconnected world.

References:

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, *98*, 102003.

IBM. (2021). Cyber Resilient Organization Study 2021. Retrieved from: https://www.ibm.com/resources/guides/cyber-resilient-organization-study/

Richet, J.L. (2021). Trends in Cybercrime: Cases the Banking Sector. *BPI France*, Jun 2021, Paris, France. 2021.

Trang, S., & Brendel, B. (2019). A meta-analysis of deterrence theory in information security policy compliance research. *Information Systems Frontiers*, *21*(6), 1265-1284.