Is There a Need for Increased Cybersecurity Awareness Within the Workplace?

Aidan T. Sidwell

Old Dominion University

IDS 300W: Interdisciplinary Theory and Concepts

Patricia Oliver

November 17, 2025

Abstract

As technology becomes further integrated into the workplace, the level of cyber threats rises. Are current employees aware of these threats? Do they need to be? Is there a need for increased cybersecurity awareness within the workplace? Through my research, I have found answers to these questions, and throughout the course of this paper, I will share my findings. My research consisted of viewpoints from several disciplines, such as cybersecurity, ethics, education, and psychology. It is through the findings of these disciplines that not only does cybersecurity awareness within the workplace need to increase, but the manner in which it is taught and portrayed needs to evolve within the current digital landscape.

Keywords: Cybersecurity, Cyberawareness, Surveillance, Education, Frameworks

Is There a Need for Increased Cybersecurity Awareness Within the Workplace?

The human factor is generally considered the weakest factor in the realm of cybersecurity. Despite ever-increasing technological advances and the increased sophistication of systems designed to protect sensitive data, human error still remains one of the leading causes of cyber incidents. Through my research, the two primary ways to mitigate this issue are through surveillance and cybersecurity awareness. As this paper aims to determine the necessity of increased cybersecurity awareness, I will first discuss surveillance. If surveillance is enough of a solution on its own, there would be no need for increased cybersecurity awareness. While certain types of surveillance can make employees feel safer, such as gates, security cameras, and security guards, others can be perceived as invasive. For example, surveillance techniques such as screen and email monitoring, which are designed to detect and prevent internal breaches, often come with negative connotations among employees. The more invasive types of surveillance are effective tools for ensuring greater security within the workplace, but could hamper the productivity, morale, and mental health of employees. In fact, research has shown that constant exposure to invasive surveillance methodologies can lead to varying psychological consequences, including anxiety, fatigue, depression, and other health issues, which can ultimately impair an employee's effectiveness and well-being in the workplace. "...some psychological studies have documented the link between monitoring and fatigue, anxiety, depression and nervous disorders, and adverse impacts on health and productivity"(West & Bowman, 2014). Surveillance, while a strong tool for security, is not enough of a solution to prevent the need for increased cybersecurity awareness among employees.

Cybersecurity awareness, or CSA, is defined by Sunil Chaudhary as follows: “CSA encompasses an understanding of cyber risks that could potentially lead to cyber incidents and other cyber threats, their preventive and mitigation strategies, and, more crucially, the attitude and ability to translate the acquired knowledge into the right action or behaviour”(Chaudhary, 2024). Chaudhardy argues that cybersecurity awareness is often misdefined as simply knowing information regarding cybersecurity. When in reality, a true understanding of cyber concepts and an understanding of why they are important is necessary as well. Employees need more than knowledge; they need to be invested in security and develop good routines, practices, and cyber hygiene. In other words, cybersecurity awareness is not only the development of knowledge, but also the development of behaviors. This distinction between definitions of cybersecurity awareness is critical when analyzing the current employee attitude towards cybersecurity. Employees may know of concepts, but they don’t always think it's their job to care about them. It is a common mindset to believe that cybersecurity is only the responsibility of those in the information technology field or those who are cybersecurity professionals. Additionally, Chaudhary asserts that thinking with security in mind is not an intuitive thing to do. Consequently, employees are predisposed to thinking that cybersecurity awareness training is a nuisance that takes away time from what they deem to be more productive tasks. With all this in mind, perhaps the issue at hand is not entirely the level of cybersecurity awareness but the manner in which it is taught and represented to employees as well.

In the world of cybersecurity, cybersecurity frameworks are created to organize an organization's plan for combating cyber threats, thereby protecting sensitive information and data. "This approach can cover a wide range of topics, such as the best practices for password management, spotting and avoiding phishing scams, safeguarding sensitive information, and handling security incidents. This method offers a consistent approach to training and assists firms in making sure that all employees, regardless of job function or level of technical skill, receive the same training. Additionally, by utilizing frameworks for cybersecurity awareness, businesses can gauge the success of their training initiatives using indicators like employee feed-back, the frequency of security awareness training, and the volume of security incidents reported"(Taherdoost, 2024). By implementing a framework for cybersecurity awareness, companies can clearly illustrate to their employees the expectations regarding cybersecurity. Additionally, a cybersecurity framework functions as a means of teaching employees how to be security-minded and ensuring best practices are used within the workplace. "These programs are designed not only to equip individuals with the necessary knowledge and skills to recognize and respond to potential threats but also to foster a cybersecurity-conscious culture within the organization"(Abrahams et al., 2024).

Conclusion

In summation, cybersecurity awareness is more than just knowing cybersecurity-related concepts; it is understanding their importance and consciously integrating them into daily routines and behaviors. For cybersecurity awareness to be truly effective, it must go beyond theoretical training to foster a security-conscious mindset and culture. In order to properly portray cybersecurity awareness to employees within the workplace, the implementation of a

cybersecurity framework is necessary. These frameworks set clear goals, guidelines, and expectations for employees. Only when employees are properly educated on and understand the importance of cybersecurity can human error be properly mitigated.

Citations

Chaudhary, S. (2024). Driving behaviour change with cybersecurity awareness. Computers & Security, 142, 103858. https://doi.org/10.1016/j.cose.2024.103858

Dursun, F. (2025). Digital Age Workplace Security: Cyber Hygiene Approach in Remote Work. İşletme Bilimi Dergisi, 13(1), 138-157. https://doi.org/10.22139/jobs.1623655

Taherdoost, H. (2024). A Critical Review on Cybersecurity Awareness Frameworks and Training Models. Procedia Computer Science, 235, 1649-1663. https://doi.org/10.1016/j.procs.2024.04.156

Temitayo Oluwaseun Abrahams, Oluwatoyin Ajoke Farayola, Simon Kaggwa, Prisca Ugomma Uwaoma, Azeez Olanipekun Hassan, & Samuel Onimisi Dawodu. (2024). Cybersecurity awareness and education programs: A review of employee engagement and Accountability. Computer Science & IT Research Journal, 5(1), 100–119. https://doi.org/10.51594/csitrj.v5i1.708

West, J. P., & Bowman, J. S. (2016). Electronic Surveillance at Work. Administration & Society. https://doi.org/10.1177/0095399714556502