Mackenzie Cooke
03/29/2025
CYSE 200T 25962
Mr. Kirkpatrick

The Human Factor within Cybersecurity

Managing information systems (and their budgets) can be a painstaking task that requires understanding the discipline. It requires balancing protection against outside threats and insiders. Understanding what is at risk is important when evaluating the most critical resources to implement. Cybercrime and white-collar crime pose unique and complex challenges, requiring clear definitions and prevention strategies.

What are cybercrimes and white-collar crimes?

Cybercrime is malicious digital activity that damages individuals and/or companies (Payne & Hadzhidimova, n.d., p. 1). While anyone can do it, younger people are most likely to commit cybercrimes (Payne, 2018, p. 19). At the same time, older people are likelier to commit a white-collar crime (Payne, 2018, p. 19). Actions like hacking sensitive data, unauthorized access to private systems, and cyberbullying fall under the definition of cybercrime (Payne, 2018, p. 19). While unauthorized access to private information can fall under white-collar crimes, hacking and cyberbullying only meet the cybercrime definition (Payne, 2018, p. 19).

What is White-Collar Cybercrime?

White-collar cybercrime is a specific type of cybercrime. While it does meet the original definition of cybercrime, the term holds a more narrowed definition. While it is digital malicious intent, it has the white-collar name due to who is perpetrating the crime. Businesses or people (or people pretending to be a businesses) wreak havoc on a company, consumers, or the general public (Payne, 2018, p. 22). White-collar cybercrimes include damaging company digital assets, gathering sensitive information under false pretences, and taking advantage of consumers or people related to the business (Payne, 2018, p. 21). These crimes are specifically white-collar

because trusted professionals commit them (or people pretending to be professionals) (Payne, 2018, p. 21).

Employee Training Program

If I were to protect my company's information assets (and allocate the limited budget), I would prioritize placing every employee through an extensive training program. Ensure that employees are given up-to-date and relevant information from their first day on board throughout their time with the company. While our budget may be limited, I think proper time and resources should be allocated to training individuals since employees can be the first line of defense regarding cyber threats. So my first order of business would be a training-packed employee orientation and a fantastic annual training refresher for maximum employee readiness in the company. Training can be the most effective form of cybercrime prevention if updated regularly and adequately taught.

Insider Threat Prevention

Insider threat prevention can benefit any company. Employees found to be insider threats will have consequences, which will be publicly posted to prevent similar actions in the future. Deterrance is a tool that will be used to make public displays condemning acts of insider threats (Payne, 2018, p. 30). Knowing the company and legal ramifications will likely deter other employees from committing the same crimes. Emphasizing insider threat prevention can be a valuable tool.

Cyber Protection from Outside Threats

One large component of my plan will be implementing software and hardware protections on the company's digital assets. Physical security is just as important as a firewall. Again, with appropriate employee training, everyone within the company should be doing their

part in protecting information systems. Another important task will be to hire qualified cybersecurity professionals to keep our systems safe. Another important part will be to ensure systems run as efficiently as possible for cost-effectiveness.

Conclusion

Cybersecurity faces real threats, including cybercrime and, more specifically, white-collar cybercrime in some instances. With a low budget, the most important things to implement would be allocating resources to training employees and improving physical and network security. Insider threats can also harm the company, so proper training and deterrence measures will be equally important. Cybercrime is a common issue within the workplace. We can protect the network within a reasonable budget with adequate training and smart resource usage.

Mackenzie Cooke
03/29/2025

CYSE 200T 25962
Mr. Kirkpatrick

References

Payne, B. K. (2018). White-Collar Cybercrime: White-Collar Crime, Cybercrime, or Both? *Criminology, Criminal Justice, Law & Society*, *19*(3), 16-32.

Payne, B. K., & Hadzhidimova, L. (n.d.). Cybersecurity and Criminal Justice: Exploring the Intersections. *INPRESS at International Journal of Criminal Justice Sciences*, 1-18.