1-2 Journal: Prioritizing Cybersecurity Risk

Joshua Merren

Southern New Hampshire University

CYB-410-13417-M01 Security Risk Management

Professor Christopher Molstad

5 September 2024

Prioritizing cybersecurity risks is crucial to keeping sensitive information safe, building trust with the people we work with, and avoiding losing money or harming our reputation. It involves identifying the most significant threats and addressing them first. This approach is critical because it requires everyone in the company to cooperate. One example of this in action is the risk management framework suggested by NIST, which stresses identifying, assessing, and responding to risks based on their impact and likelihood (Barrett, 2020). By teaching every employee about their role in keeping our systems safe, we help everyone stay alert and ready. It also helps when everyone agrees on how much risk is acceptable, making our strategies stronger and more effective. These strategies help create a strong feeling in the community that supports our security efforts. When everyone works together like this, we can react to threats faster and more effectively, strengthening our defenses. This teamwork does not just help us now but also keeps us secure in the long run.

Proactively managing risks is a big part of keeping our digital spaces safe. Regular checks to find and fix weak spots before they cause problems can reduce the chances of a successful attack. According to the "Cost of a Data Breach Report 2024" by IBM, the global average cost of a data breach has reached a record high of USD 4.88 million, a 10% increase over the previous year. Importantly, the report highlights that organizations employing security AI and automation considerably saved an average of USD 2.22 million in breach costs compared to those that did not (IBM, 2024). Leveraging advanced technologies in cybersecurity efforts offers significant financial benefits. Additionally, one in three breaches involved shadow data, emphasizing the growing challenge of managing and securing proliferating data. Keeping track of these checks helps us see what is working and what is not. This ongoing attention stops problems before they start and keeps our online environments reliable. Making these activities a

routine ensures that our security is always current. This preparedness is crucial for stopping immediate threats and planning to stay safe from future risks. Such efforts make our digital areas more robust and trustworthy, letting our company operate smoothly and maintain a good reputation. We build a secure foundation for our digital activities by focusing on these priorities.

References

Barrett, M. P. (2020, January 27). *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*. NIST. https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11

IBM. (2024). *Cost of a Data Breach Report 2024*. https://table.media/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf