**Unit 7.1****: Cybersecurity and Data Breaches: Understanding Risks and Mitigation Strategies**

Anicet Hermann Zie

Post University, School of Arts & Science

CIS311 - Technical Writing in CIS

Dr. Matt Zullo

October 12, 2025

**Executive Summary**

This research report explores the growing issue of cybersecurity and data breaches that continue to threaten both private and public sectors worldwide. Drawing on ten scholarly and industry sources, this paper examines the major causes, financial and operational impacts, and strategies organizations can adopt to mitigate risks. The report highlights how human error, weak infrastructure, and sophisticated attacks contribute to breaches and emphasizes the need for robust frameworks, employee training, and continuous monitoring. The research also references the National Institute of Standards and Technology (NIST) and the Center for Internet Security (CIS) as key frameworks that support cybersecurity resilience. Findings suggest that organizations investing in proactive defense mechanisms and awareness programs experience fewer breaches and reduced financial losses. The report concludes by advocating for a multi-layered security approach combining technology, policy, and human awareness to protect sensitive data effectively.

**Introduction**

In the digital age, data has become one of the most valuable organizational assets, making cybersecurity a critical priority across industries. As businesses increasingly rely on digital platforms and cloud infrastructure, cyberattacks and data breaches have grown both in frequency and sophistication. IBM Security (2023) reports that the average global cost of a data breach reached $4.45 million, marking a 15% increase over three years. Such financial losses are accompanied by reputational damage, loss of customer trust, and potential regulatory penalties. The purpose of this research report is to analyze the root causes of cybersecurity breaches, examine their organizational impact, and present strategies for risk mitigation using industry best practices and frameworks. Understanding and addressing these threats is essential for maintaining operational integrity and ensuring compliance with data protection standards.

**Methodology**

The research for this report was conducted using authoritative databases such as EBSCOhost, ProQuest, and JSTOR. Keywords including “cybersecurity,” “data breaches,” “risk management,” “information security,” and “mitigation strategies” were used to locate relevant materials. The sources selected for this study include academic journals, government publications, and industry reports from recognized institutions such as the Centers for Internet Security (CIS), the European Union Agency for Cybersecurity (ENISA), and IBM Security. Selection criteria focused on credibility, publication date (2017–2023), and relevance to cybersecurity management practices. The analysis synthesized qualitative findings across ten authoritative references to identify common trends, causes, and best practices in mitigating cybersecurity risks.

**Findings**

**Causes of Data Breaches**

Data breaches often originate from a combination of human error, system vulnerabilities, and targeted attacks. Cheng et al. (2017) found that inadequate authentication, unpatched software, and insider threats are among the most common causes of corporate data loss. Bada, Sasse, and Nurse (2019) emphasized that employee negligence such as falling for phishing scams or weak password practices remains a dominant cause of security incidents. The Ponemon Institute (2021) highlighted that remote work environments have further increased risk exposure, as employees access company systems through unsecured networks and personal devices**.**

**Impacts on Organizations**

The consequences of cybersecurity incidents extend beyond immediate financial loss. According to Castillo (2021), organizations experience long-term effects such as reputational harm, customer attrition, and loss of intellectual property. IBM Security (2023) confirmed that compromised companies spend an average of 277 days identifying and containing a breach. Additionally, regulatory frameworks such as the General Data Protection Regulation (GDPR) impose severe penalties for non-compliance, further emphasizing the importance of robust data protection measures.

**Prevention and Mitigation Strategies**

Organizations must adopt proactive defense mechanisms to reduce the likelihood of breaches. The Centers for Internet Security (2022) recommend implementing a layered security model with critical controls, including access management, incident response planning, and continuous monitoring. Employee awareness and regular cybersecurity training play a vital role, as users are often in the first line of defense (Bada et al., 2019). Technological solutions such as encryption, multi-factor authentication, and intrusion detection systems further enhance data protection (Cheng et al., 2017).

**Role of Frameworks and Awareness**

Adopting standardized frameworks such as the NIST Cybersecurity Framework (2018) and ENISA’s threat landscape guidelines (2022) enable organizations to assess and manage their cybersecurity maturity. These frameworks help institutions identify critical assets, evaluate vulnerabilities, and implement preventive controls aligned with best practices. Gordon, Loeb, and Zhou (2020) emphasized the economic importance of strategic cybersecurity investments, noting that prevention yields higher returns than post-breach recovery. Combining governance policies with technical safeguards and regular training ensures that both human and technological components work together to secure information assets.

**Conclusion**

Cybersecurity and data breaches continue to present complex challenges requiring a multifaceted response. This report has demonstrated that breaches typically stem from human error, technical vulnerabilities, and insufficient organizational controls. The findings support the argument that preventive strategies such as employee education, adherence to security frameworks, and consistent investment in cybersecurity infrastructure are critical to minimizing risk. Future efforts should focus on enhancing global collaboration, integrating artificial intelligence in threat detection, and maintaining adaptive policies that evolve with emerging threats. Ultimately, securing organizational data requires not only advanced technology but also a culture of awareness and accountability**.**

**References**

Alsmadi, I., & Xu, S. (2019). Security of data in the cloud: A survey of issues, challenges, and future directions. \*Journal of Information Security and Applications, 48\*, 102–112. https://doi.org/10.1016/j.jisa.2019.102419

Bada, A., Sasse, M. A., & Nurse, J. R. C. (2019). Cybersecurity awareness campaigns: Why do they fail to change behavior? \*Communications of the ACM, 62\*(3), 61–65. https://doi.org/10.1145/3303862

Castillo, M. (2021, July 28). Data breach costs rise to $4.24 million, highest in 17 years. \*CNBC News.\* https://www.cnbc.com/2021/07/28/ibm-report-data-breach-costs-rise-to-4point24-million-highest-in-17-years.html

Centers for Internet Security. (2022). \*CIS critical security controls for effective cyber defense.\* Retrieved October 5, 2025, from https://www.cisecurity.org/controls

Cheng, L., Liu, F., & Yao, D. (2017). Enterprise data breach: Causes, challenges, prevention, and future directions. \*Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 7\*(5), e1211. https://doi.org/10.1002/widm.1211

European Union Agency for Cybersecurity. (2022). \*ENISA threat landscape 2022.\* Retrieved October 5, 2025, from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Gordon, L. A., Loeb, M. P., & Zhou, L. (2020). Investing in cybersecurity: Insights from the Gordon-Loeb model. \*Journal of Information Security, 11\*(2), 94–104. https://doi.org/10.4236/jis.2020.112007

IBM Security. (2023). \*Cost of a data breach report 2023.\* IBM. Retrieved October 5, 2025, from https://www.ibm.com/reports/data-breach

National Institute of Standards and Technology. (2018). \*Framework for improving critical infrastructure cybersecurity.\* https://doi.org/10.6028/NIST.CSWP.04162018

Ponemon Institute. (2021). \*Cybersecurity in the remote work era.\* Ponemon Research. Retrieved October 5, 2025, from https://www.ponemon.org