Data Protection Policy, Workforce Culture, and the Implications of Generative AI

Kayla Thompson

Old Dominion University

CYSE 425W

Professor Shideh Yavary Mehr

November 27, 2025

Abstract

Data protection policies are foundational to modern cybersecurity, shaping organizational culture. This paper examines the DPP's influence on employee behavior, accountability, and trust within organizations. It argues that a well-implemented data protection policy strengthens cybersecurity culture. Furthermore, the examination of how Generative AI (Gen AI) can amplify support opportunities for automation, training, and governance. Through analysis and justification, the paper demonstrates that Data Protection Policies, supported by Gen AI, create a resilient and security-based organizational culture.

Introduction

Cybersecurity strategies aren't limited to firewalls and encryption, but encompass a significant amount of influence on how organizations perceive and manage risk. Data Protection Policies (DPPs) establish fundamentals for handling sensitive data, influencing employee behavior, and organizational values. A strong cybersecurity culture is curated when employees digest these fundamentals, treating it as a shared priority. As technology advances, so does the intelligence of cyber threats; organizations must adopt policies that reinforce accountability, compliance, and ethics. With the inclusion of Generative AI offer tools to enhance policies and awareness.

Data Protection Policy

Everyone has data and sensitive information that should not be exposed to the general public like social security numbers, credit cards numbers, addresses, etc. Policies that shape the safekeep of sensitive information outlines how an organization collects, stores, and processes, and secures personal and sensitive data. One element includes compliance with regulations like GDPR, HIPPA, and CCPA; these are all data protection policies in different workplace fields. HIPAA is a Patient to Medical Doctor confidentiality agreement, where doctors can not release confidential information to anyone unauthorized personnel.

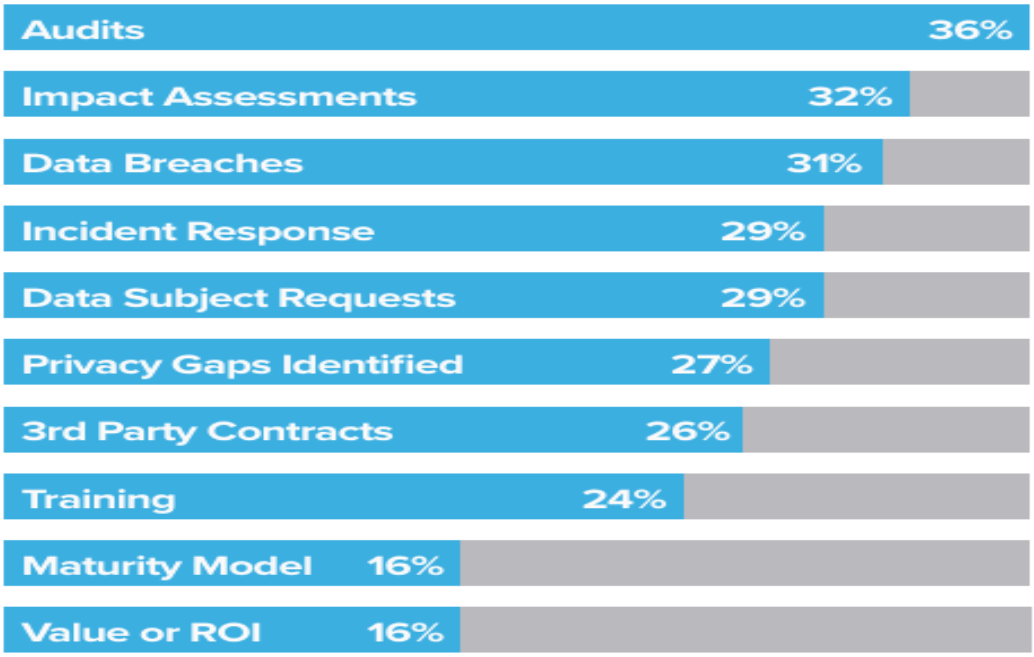
Data protection policy also outlines access controls to limit data exposure and encryption to safeguard sensitive information. All banking platforms have access controls to prevent black hat hackers from potential threats and accessing unauthorized sensitive information to credit cards, debit cards, routing numbers, and more. To mitigate these risks, preventive measures and employee training are important to retention and the reduction of data breaches.

Analysis

With numerous data protection policies being implemented in workplaces, it strengthens organizational culture in many ways. The workplace starts with the people who make it happen, the employees. Employees recognize the importance of safeguarding personal data, which is evident in the training employees receive to identify, mitigate, and resolve data threats from unauthorized personnel. It's not just the responsibility of the IT departments of an organization to mitigate breaches, but a shared responsibility for everyone involved in the company. The training employees receive is evident, which creates trust between consumers and stakeholders, gaining confidence in the organization's commitment to privacy. As Gstrein and Beaulieu (2022) note, “No one is an island in a ‘datafied’ society. Sharing the same time, space and cultural dimension makes it difficult for an individual to stand apart”.

To make sure organizations are keeping up with these expectations, goals, and metrics are evaluated to measure and improve systems. We can evaluate this by the reduction of data beaches during a specific period of time, creating compliance audit scores to maintain the integrity of the organization's values, employee training completions in a timely manners that are frequently updated, and consumer surveys of their experience with the organization. The Oxford Academic stated, “The success of any regulation, however good, ultimately depends on how well it is executed”. Metrics like compliance audit scores and breach reduction rates are essential for evaluating execution quality.

Figure 1. Shows Privacy Metrics Reported to the Board of Directors.



Note. Adapted from *Privacy Metrics Report* by O. Tene & M. Culnan, Future of Privacy Forum, September 2021. The diagram illustrates common privacy metrics reported to boards of directors, including audits, impact assessments, data breaches, incident response, and training. These metrics demonstrate how organizations measure compliance, accountability, and cultural maturity in data protection programs.

Generative AI

Generative AI has made a disruptive impact on the technological industry with algorithmic programs to assist with reading large files of data. Generative AI can amplify the effectiveness of Data protection policies in numerous ways. One way Gen AI can improve efficiency is by automating compliance checks. AI can scan systems for policy violations in real time. AI is a handy tool in creating immersive experiences to educate employees on data protection while being interactive. According to Oxford Academic, “Access to AI assistance

increases worker productivity, as measured by issues resolved per hour, by 15% on average, with substantial heterogeneity across workers". This helps employees retain information to perform better in their quality of work. To even implement or have these policies, leadership needs to create them, which may take days, weeks, months, or even years. To reduce this, Gen AI can help organizations update policies to better reflect evolving regulations. Though these new tools can help move the company along quickly, Gen AI may introduce risks like generating synthetic data that can be misused or create vulnerabilities if not properly monitored. With Generative AI as an amazing tool to organizations and having risks, it is important to require strong monitoring to ensure its support rather than undermine data protection.

Conclusion

Data protection policies shape organizational culture by embedding values of privacy, accountability, and trust. Organizations should implement preventative measures and a compliant environment where employees view data protection as a shared responsibility. Generative AI amplifies this by offering tools for automation, training, and governance. However, its integration requires monitoring the system to avoid new risks. Data protection policies supported by Gen AI represent a powerful model for strengthening cybersecurity culture in the new era of technology.

References

Buckley, G., Caulfield, T., & Becker, I. (2024). GDPR and the indefinable effectiveness of privacy regulators: Can performance assessment be improved? *Journal of Cybersecurity, 10*(1), tyae017. Oxford Academic. https://academic.oup.com/cybersecurity/article/10/1/tyae017/7754590

Finck, M., & Pallas, F. (2024). Generative AI and data protection. *International Data Privacy Law, 14*(1), 1–20. Cambridge University Press. https://www.cambridge.org/core/services/aop-cambridge-core/content/view/201F37EBCB407697A4249D74CF9F1204/S3033373324000024a.pdf/generative_ai_and_data_protection.pdf

Finck, M., & Pallas, F. (2024). Generative AI and data protection. *ResearchGate*. https://www.researchgate.net/publication/387747423_Generative_AI_and_data_protection

Gstrein, O. J., & Beaulieu, A. (2022). How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches. *Philosophy & Technology, 35*(1), 3. National Center for Biotechnology Information (NCBI). https://pmc.ncbi.nlm.nih.gov/articles/PMC8800549/

International Association of Privacy Professionals (IAPP). (2022, March 14). *Measuring privacy programs: The role of metrics*. IAPP News. https://iapp.org/news/a/measuring-privacy-programs-the-role-of-metrics

Tene, O., & Culnan, M. J. (2021). *Privacy Metrics Report*. Future of Privacy Forum. https://fpf.org/wp-content/uploads/2022/03/FPF-PrivacyMetricsReport-R9-Digital.pdf