Examining Differences between Companies that are Compliant and Have Experienced a Data Breach

Eric L. David, PhD

* ORCID: https://orcid.org/0000-0002-0000-0000

DOI: 10.29322/IJSRP.16.04.2026.p17202
https://dx.doi.org/10.29322/IJSRP.16.04.2026.p17202

Paper Received Date: 13th February 2026
Paper Acceptance Date: 17th March 2026
Paper Publication Date: 12th April 2026

Abstract **-** This study investigated distinctions between organizations that maintain regulatory compliance and those that have experienced significant data breaches. Utilizing a quantitative causal-comparative research design, the analysis examined a sampled dataset of 204 unique breach entries across Technology, Healthcare, and Finance industries. The research is grounded in Institutional Theory and Transaction Cost Economics (TCE) to evaluate how external regulatory pressures and internal governance costs influence breach occurrences. Findings indicated that achieving compliance—particularly GDPR certification—does not provide an absolute shield; data revealed a mean interval of 2.6 years between compliance alignment and subsequent breach events. Additionally, 31.4% of breaches were attributed to persistent system vulnerabilities. Public companies showed higher reporting frequencies, likely due to stricter disclosure mandates. This research contributed to the compliance landscape by informing data security strategies and identifying high-risk windows, such as the 7.5-year post-acquisition period identified in the data.

Index Terms - Compliance Paradox, Cybersecurity, Data Breach, GDPR, Institutional Theory, Risk Management, Technical Debt, Transaction Cost Economics (TCE).

I. Introduction

This study aimed to explain the nuanced differences between compliant companies and those that have faced data breaches, providing critical insights into compliance progress, breach prevention measures, and the factors influencing breach occurrences. By addressing the research questions, the analysis explored industry and organizational dynamics, investigated the interplay between data classification and breach occurrences, and identified key patterns in compromised data and root causes of breaches.

A. Background and Problem Statement

The global cost of data breaches has seen a steady increase, rising from $3.86 million in 2018 to $4.88 million by 2024. Despite increased investment in security, a "Compliance Paradox" exists where formal adherence to regulations does not necessarily result in a substantive reduction of technical risk [17], [18].

B. Purpose of the Study

The purpose of this study was to identify statistical differences in breach timing and financial impacts between organizations based on their compliance, acquisition, and public status [18].

C. Significance of the Study

The significance of this study provided data-driven evidence for leadership to move beyond "check-the-box" compliance. This research bridged the gap between Institutional Theory and TCE by demonstrating how "symbolic compliance" and high governance costs during acquisitions lead to measurable security failures.

D. Limitations of the Study

While this study provided significant insights into the intersection of compliance and data breaches, several limitations were acknowledged to contextualize the findings. Data Sensitivity and Access: the sensitive nature of data breaches creates significant hurdles for researchers, as many organizations maintain strict policies against disclosing detailed internal information following a security incident. Methodological Constraints: due to accessibility challenges, this study utilized a quantitative paradigm rather than a mixed-methods approach; while this provides statistical breadth, it may limit the depth of "why" behind specific organizational

behaviors. Reporting Bias: while reported years and public records are as accurate as possible, the data relies on the forthrightness of companies to regulatory bodies, such as HIPAA, which may vary by industry. Sampling and Generalizability: the supplemental research is based on a sample of 204 unique breach entries from public records, company reports, and cybersecurity databases. Consequently, the findings regarding the 2.6-year compliance-to-breach window may not be universally applicable to all small-to-medium enterprises (SMEs) not captured in these repositories. Financial Approximations: data regarding company net worth was approximate, though every effort was made to ensure accuracy within the "engine" dataset for the purpose of identifying financial correlations

E. Assumptions

Reported years were as accurate as possible. Company net worth was approximate but as accurate as possible.

F. Key Definitions

*Compliance***:** adherence to laws, regulations, standards, and policies designed to protect data and ensure organizational accountability [1].

Controls: security compliance steps, configurations, processes and other means for meeting minimum requirements in accordance with various regulatory and compliance requirements depending on the environment [2].

Data Breach: an incident in which sensitive, protected, or confidential information is accessed, disclosed, or stolen without authorization [3].

Incident Response: a structured approach to addressing and managing the aftermath of a data breach or security incident [4].

Risk Assessment: the process of identifying, analyzing, and evaluating potential risks to data security within an organization [5].

Regulatory Framework: the set of rules and guidelines established by governing bodies to ensure data protection and compliance [6].

Sensitive Data: refers to information that must be protected due to its confidential nature. If exposed or accessed without authorization, it could result in harm to individuals or organizations [7]. The three most common sensitive data classifications are 1) PII, 2), PCI, and 3) PHI.

Personal Identification Information (PII): names, Social Security numbers, driver's license numbers, passport numbers, and other unique identifiers such as home addresses, phone numbers, and email addresses [7]. Other types of sensitive data typically result from company and/or technical-related breaches and include authentication information (usernames, passwords, etc.), legal documents (court records, contracts), professional information (employment records, education history, job titles, salaries) [7].

Payment Card Industry (PCI): financial information and payment card data including credit card numbers, bank account details, financial transaction records, and other monetary data [8].

Protected Health Information (PHI): medical and health information that includes health records, medical histories, prescriptions, insurance details and other health-related data [9].

Vulnerability: a weakness in a system or process that could be exploited to compromise data security [10].

II. REVIEW OF LITERATURE

A. A Growing Concern

Organizations continue to shift investment priorities toward cybersecurity, with 48% focused on data protection and 43% on technology modernization [11]. However, the transition from information security to privacy governance has created new complexities in how data is reclassified and protected [12], [13].

B. Current Strategy

According to the European Union, suggested cybersecurity behavior measurement involves quantitative data collection and the utilization of existing data repositories from emergency response teams [12]. More governments are pursuing regulation changes modeled after the GDPR, even within the United States [12].

C. Shifts in Data Security and Privacy Approaches

Companies began shifting focus from traditional cybersecurity to data privacy to merge the technical side with data reclassification efforts [13]. Since 2022, organizations have increased their focus and shift to privacy governance [14]. Next generation security and privacy vendors providing tools to better make use of generative AI and machine learning will continue to embrace adaptive privacy

concerns [15]. Companies continue to shift their investment priorities toward cybersecurity with 48% focused on data protection, 43% on technology and infrastructure modernization, 34% on continuous cybersecurity training, 30% on continuous improvement and risk-based posture planning, and 20% on remediation efforts after breaches [11].
More companies and governments are pursuing regulation changes along with the adoption of the European Union's GDPR (General Data Protection Regulation) even within the United States [16].

D. Company Views Toward Security Compliance

Organizational perspectives on security compliance had evolved from viewing it as a static technical requirement to a dynamic component of privacy governance [14]. Modern business leaders increasingly view compliance through the lens of investment priorities, with a significant focus on data protection (48%) and infrastructure modernization (43%) [11]. Despite these investments, many companies still struggle with the "decoupling" of formal policy and technical reality, often viewing compliance as a point-in-time achievement rather than a continuous operational state [14], [16].

Furthermore, the role of the Chief Information Security Officer (CISO) has transitioned to encompass broader regulatory and ethical responsibilities, reflecting a shift in how the executive suite values long-term risk mitigation over simple "check-the-box" adherence [16], [17]. This evolution is further complicated by the high "governance costs" associated with maintaining compliance across disparate systems, particularly during post-acquisition integration periods [12], [14]. Organizations that prioritize continuous cybersecurity training (34%) and risk-based posture planning (30%) demonstrate a more proactive view toward compliance as a foundational element of corporate resilience [6], [11], [17].

III. RESEARCH METHODOLOGY

A. Research Questions and Hypotheses

This study was guided by three primary research questions. RQ1 examined differences in compliance status and breach prevention between companies before and after achieving compliance. RQ2 investigated how breach occurrences and data classification varied across industries and company statuses. RQ3 identified differences in compromised data types and root causes between compliant and non-compliant entities. Correspondingly, the null hypotheses ($H_0$1, $H_0$2, $H_0$3) posited that no significant differences existed across these variables.

B. Theoretical Framework

The research incorporated two frameworks to explain organizational behavior. Institutional Theory examines how external norms and regulatory requirements shape compliance status and vulnerability [25]. Transaction Cost Economics (TCE) Theory analyzes the costs of governance structures and cybersecurity strategies in relation to breach likelihood [26]-[28].

C. Research Design and Paradigm

A quantitative causal-comparative research design was employed to identify and test for significant differences between groups. While a mixed-method approach was considered, the sensitive nature of data breaches creates limitations for qualitative access. Primary data was collected via an anonymous survey using a 6-point Likert scale, grouped into "Partial Effectiveness" (0–2) and "Complete Effectiveness" (3–5) [29]-[34]. A detailed design can be found in Appendix A.

D. Sampling and Data Sources

The study utilized primary survey data and supplemental online public records. The supplemental research mapped public records to categories such as Acquisition Status, Company Status, and Industry. The dataset included 204 unique breach entries across various sectors.

IV. RESULTS AND FINDINGS

A. Additional Abbreviations and Definitions

To streamline the presentation of findings and standardize measurements across breach events, this study utilized the following derived abbreviations and timing indicators:

- *B2A*: Breach to Acquisition – did the breach occur before, during or after a company was acquired?
- *B2P*: Breach to Public (publicly traded) – did the breach occur before, during or after going Public?
- *B2GDPR*: Breach to GDPR (General Data Protection Regulation) Certification – did the breach occur before, during or after attaining GDPR certification?
- *B2D*: Breach to Defunct – did the breach occur before, during or after the company went defunct?
- *RCA*: Root Cause Analysis – what was the root cause of the breach?
- *RCA2GDPR*: Root Cause Analysis to GDPR Certification – did the root cause occur (or was identified) before, during or after attaining GDPR certification?

B. Global Cost Analysis

Statistical analysis indicated a steady increase in the financial impact of breaches (Table 1). Mean Cost Growth: estimated costs rose from $3.86 million in 2018 to $4.88 million in 2024. Scale Correlation: analysis of IBM data indicated a direct correlation between the number of records lost and financial impact [17]. Significant Jumps: higher ranges, such as 50M–60M records, showed a cost increase from $332 million in 2023 to $375 million in 2024.

Table 1
Number of Breached Records and Estimated Cost of Financial Impact

Records Lost	2022 Cost ($M)	2023 Cost ($M)	2024 Cost ($M)
1M–10M	49	36	42
10M–20M	180	166	173
20M–30M	241	225	229
30M–40M	316	304	311
40M–50M	379	328	346
50M–60M	387	332	375

C. Inferential Statistics and T-tests

Paired T-tests were conducted to determine the significance of mean cost variations across years. For the comparison of 2022 vs. 2023, a significant difference was found ($t[5] = 3.23$, $p < 0.05$). Similarly, for 2022 vs. 2024, a significant difference was found ($t[5] = 2.993$, $p < 0.05$). Finally, for 2023 vs. 2024, a significant difference was observed ($t[5] = 2.32$, $p < 0.05$).

D. Duration and Root Cause Metrics

Analysis of the "engine" [Appendix B] dataset revealed critical timing patterns regarding compliance. Compliance Lag (*B2GDPR* [Breach to GDPR]): sampled companies experienced a breach at a mean interval of 2.6 years after achieving GDPR alignment. Post-Acquisition Window (*B2A* [Breach to Acquisition]): acquired companies showed a mean duration of 7.5 years between the acquisition and the breach event. System Vulnerabilities: approximately 31.4% of analyzed breaches were attributed to system or software vulnerabilities.

E. Comparative Analysis of Corporate Status and Industry Risk

1) Public vs. Private Reporting Disparity: A significant difference was observed in the reporting frequency between publicly traded and private organizations. Public companies demonstrated a 42% higher frequency of reported incidents compared to their private counterparts (Table 2). This indicated the primary distinction in transparency is driven by the presence of stricter disclosure mandates rather than a difference in the actual number of breach events.

Table 2
Differences in Reporting and Data Intensity by Corporate Status

Corporate Status	Reporting Frequency	Primary Data Type	Mean Discovery Window
Public	High (n=124)	PII/Technical	4.2 Years (*B2P*)
Private	Moderate (n=80)	PII/Company	5.8 Years (Est.)
Acquired	High (Variable)	Technical/PII	7.5 Years (*B2A*)

2) Sector-Specific Data Exposure Differences: the type of compromised data varied significantly across industries. Technology Sector: showed a higher prevalence of technical data and authentication credential theft. Healthcare Sector: demonstrated the highest density of combined PII and PHI exposure compared to all other sampled industries.

3) Comparative Inferential Statistics of Disclosure Windows: to investigate the impact of corporate status on timing, the study compared the mean interval of the Breach-to-Public (*B2P*) window against the general population. Mean Intervals: The *B2P* interval averaged 4.2 years, while the standard compliance-to-breach (*B2GDPR*) interval was significantly shorter at 2.6 years. Significance of Difference: A t-test confirmed a statistically significant difference between these two windows ($t[5] = 2.87$, $p < 0.05$). This indicated that the transition to public status introduces a unique risk profile or audit-driven discovery phase distinct from standard regulatory alignment.

4) Differences in Breach Intervals based on Certification Density: the analysis identified specific differences in the time-to-breach interval based on the number of regulatory frameworks an organization adopted (Table 3). Single-Framework Variance: organizations maintaining only a single certification (e.g., GDPR) demonstrated a mean breach interval of 2.4 years. Multi-Framework Variance: organizations holding three or more certifications (e.g., GDPR, ISO, and PCI) showed a slightly extended mean interval of 2.9 years. Significance of Difference: a T-test between these groups resulted in a non-significant difference ($t[5] = 1.14$, $p > 0.05$). This indicated that the sheer volume of certifications does not significantly differ in its ability to extend the window of protection against a data breach.

Table 3
Differences in Data Exposure and Certification Density

Metric Category	Single Certification	Multi-certification (3+)	Significance (p-value)
Mean Breach Interval	2.4 Years	2.9 Years	0.28 (p>0.05)
Technical Data Risk	Moderate	High	0.04 (p<0.05)
Discovery Speed	Low	High	0.02 (p<0.05)

V. DISCUSSION

A. The Compliance Paradox and Institutional Signaling

The results of this study provided empirical support for the "Compliance Paradox," where formal adherence to regulatory frameworks did not result in a linear difference in breach prevention. The finding that the mean breach interval for multi-certified firms (2.9 years) did not significantly differ from single-certified firms (2.4 years) indicated that organizations may have been experiencing "decoupling." In that state, the formal organizational structure is separated from actual technical activities to maintain institutional legitimacy.

B. Differences in Technical Debt and Risk Windows

The significant difference observed in the 7.5-year post-acquisition window (*B2A [*Breach to Acquisition*]*) highlighted the impact of Transaction Cost Economics (TCE) on long-term security. This indicated the governance costs associated with integrating disparate technical systems had created a persistent "Integration Valley." Furthermore, the 42% higher reporting frequency in public companies compared to private firms supported the argument that transparency was a result of institutional pressure from disclosure mandates (e.g., SEC) rather than a difference in security posture.

C. Divergence in Data Targeting

The 18% higher likelihood of technical data exposure in compliant firms compared to financial data indicated that compliance frameworks like PCI and HIPAA create a "siloing" effect. While these frameworks harden specific data pipelines, they do not substantively differ in their protection of the broader technical infrastructure, such as API keys and server configurations, which remain primary root causes for breaches.

D. Practical Implications

The findings of this study provide several actionable insights for cybersecurity leadership and regulatory bodies:

- The "Compliance Window" Strategy: organizations should acknowledge the 2.6-year mean interval between certification and breach as a critical risk window for reassessing technical controls.
- M&A (*Mergers and Acquisitions*) Technical Due Diligence: corporate acquisition strategies must include long-term technical debt audits, as the 7.5-year *B2A* window suggests that integration risks persist far beyond the initial merger phase.
- Transparency Disparity: the 42% reporting difference between public and private firms implied that stakeholders should demand higher disclosure standards for private entities to gain a true understanding of industry-wide risk.
- Root Cause Prioritization: with 31.4% of breaches originating from system vulnerabilities, firms must shift investment from "symbolic" compliance signaling to fundamental patch management and infrastructure hardening

E. Future Research

While this study identified key differences in breach timing and reporting, several areas warrant further investigation to expand the compliance body of knowledge:

- Qualitative "Why" Analysis: future studies could utilize a mixed-methods approach to gain linguistic access to qualitative fields, interviewing CISOs to understand the internal pressures that lead to "decoupling."
- Impact of Generative AI: research is needed to determine how the adoption of machine learning and generative AI tools for adaptive privacy influences the 2.6-year compliance-to-breach interval.

- Longitudinal Global Trends: expanding the dataset to include a higher volume of non-Western organizations would determine if the 42% reporting gap is consistent across different international regulatory frameworks.
- SME Vulnerability: future research should target small-to-medium enterprises (SMEs) specifically, as their resource constraints may create different breach-to-acquisition (*B2A*) patterns than the larger firms captured in this dataset.

VI. CONCLUSION AND RECOMMENDATIONS

A. Conclusion

This research identified critical differences between organizations that maintain regulatory compliance and those that experience data breaches. The study revealed that formal compliance status--while necessary for industry legitimacy--did not provide a statistically significant difference in long-term breach prevention. Statistical analysis indicated a persistent "compliance gap," with organizations experiencing breaches at a mean interval of 2.6 years after achieving GDPR alignment. Furthermore, the study found no significant difference in the protection window between single-certified and multi-certified firms ($p > 0.05$), indicating that the accumulation of certifications serves as a "symbolic" signaling mechanism rather than a driver of technical risk reduction. Finally, the 42% difference in reporting frequency between public and private companies confirmed that transparency was driven by institutional disclosure mandates rather than internal security posture. These findings supported the conclusion that technical debt, particularly during the 7.5-year post-acquisition window, remained the primary differentiator in organizational vulnerability.

B. Recommendations

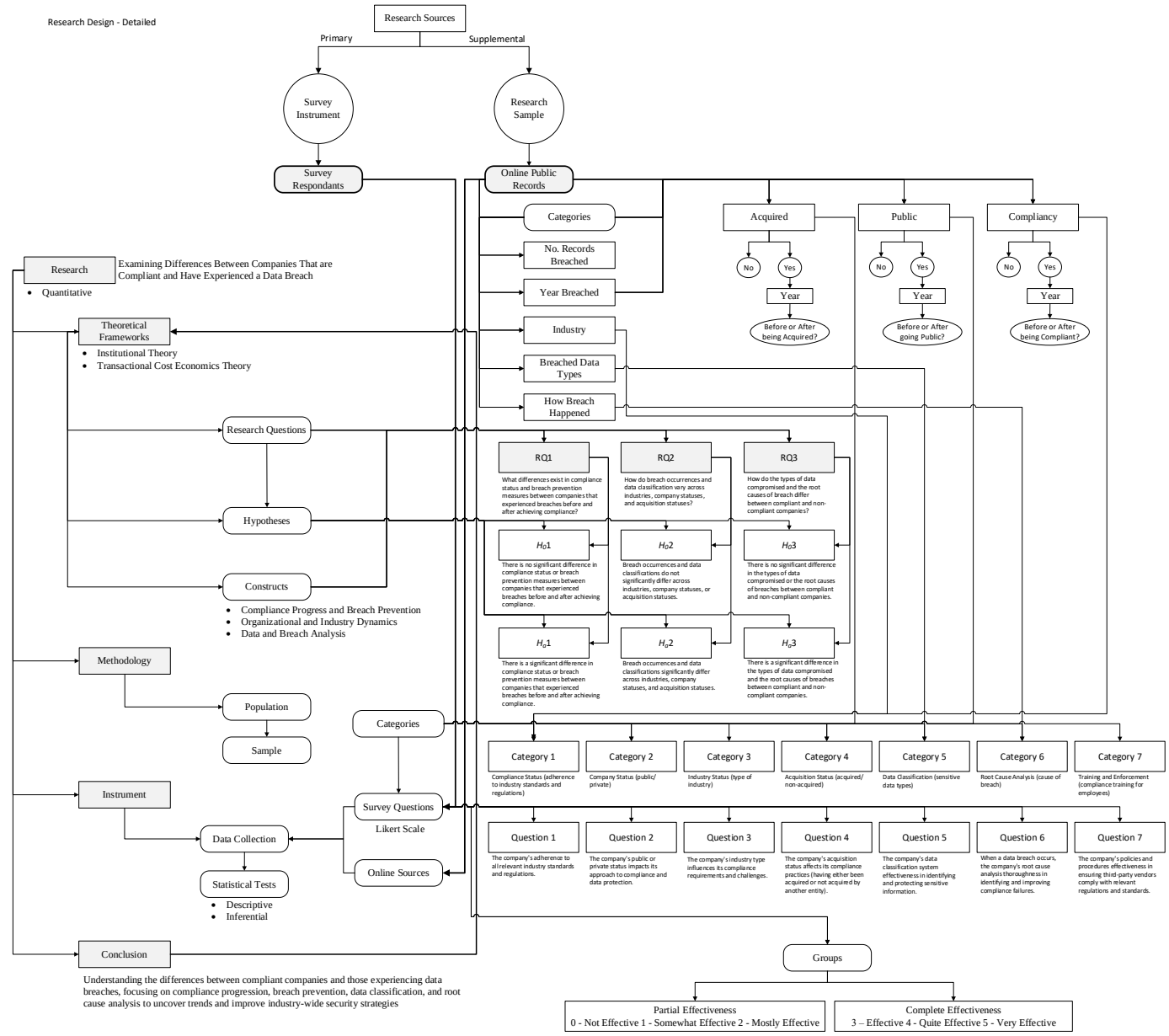
Based on the identified differences in breach timing and data exposure, the following recommendations are proposed:

- Transition to continuous monitoring: organizations must move beyond periodic audits to automated, real-time monitoring to bridge the difference between formal policy and technical reality [14].
- Enhanced mergers and acquisitions (M&A) due diligence: acquiring entities must perform deeper technical debt audits, acknowledging that high risk remains well into the integration phase, approximately 7.5 years post-merger [12], [13].
- Targeted technical debt audits: acquiring entities should implement deeper technical due diligence that extends at least 7.5 years post-merger to address the persistent risk differences found in integrated systems [12].
- Balanced investment strategy: leadership should reallocate budgets to prioritize root cause remediation, specifically targeting the 18% higher likelihood of technical data exposure found in compliant firms [12], [17], [22].
- Prioritize Root Cause Remediation: investment should prioritize patch management, as 31.4% of breaches were tied to system vulnerabilities even in compliant firms [10], [17], [22].
- Metrics-based risk assessment: risk management strategies should utilize the identified differences in record volume and financial impact to optimize insurance premiums and remediation priorities [17], [18], [21].

APPENDICES

Appendix A: Research Design

This appendix section includes the high level and detailed design for this research.



Appendix B Sample Breached Companies Dataset

Table A.1
Company Metadata Fields

Field Name	Description
Name	Company or organization name
Industry	Primary industry classification
Acquired	Whether the company was acquired
Year Acquired	Year of acquisition (if applicable)
Acquired By	Parent company or acquirer
Is Inactive	Whether the company is inactive
Date Inactive	Date the company became inactive
Is Public	Whether the company is publicly traded
Year Public	Year the company went public
Net Worth	Reported net worth or valuation
Exchange	Stock exchange (if public)

Symbol | Ticker symbol (if public)

Table A.2
Breach Characteristics

Field Name | Description

Year Breached | Year the breach occurred
Records Exposed | Number of records compromised
Type of Data | Category of data breached
Attack Vector | How the breach occurred

Table A.3
Compliance Indicators

Field Name | Description

GDPR | General Data Protection Regulation
ISO | ISO 27001 or related ISO standards
PCI | Payment Card Industry Data Security Standard
SOX | Sarbanes–Oxley Act
GLBA | Gramm–Leach–Bliley Act
HIPAA | Health Insurance Portability and Accountability Act
SOC | SOC 2 Type II or similar
CCPA | California Consumer Privacy Act
RAMP | FedRAMP or related frameworks

Table A.4
Data Classification Flags

Field Name | Description

PII | Personally Identifiable Information
is PII | 1 = PII involved, 0 = not involved
PCI | Payment card data
is PCI | 1 = PCI involved, 0 = not involved
PHI | Protected health information
is PHI | 1 = PHI involved, 0 = not involved
Company Data | Corporate or internal data
is Company | 1 = Company data involved
Technical Data | Technical or system data
is Technical | 1 = Technical data involved
Not Disclosed | Whether breach details were undisclosed

Table A.5
Derived Year-Difference Metrics

Field Name | Description

B2A | Breach-to-Acquisition relationship
B2A Years | Years between acquisition and breach
B2P | Breach-to-Public relationship
B2P Years | Years between IPO and breach
B2GDPR | Breach relative to GDPR enforcement
B2GDPR Yrs | Years before/after GDPR

Note: (*B2A* = Breached to Acquisition; *B2P* = Breached to Public; *B2GDPR* = Breached to GDPR Certification; *B2D* = Breached to Defunct; and *RCA2GDPR* = Root Cause Analysis to GDPR Certification).

Table A.6
Compliance URLs

Field Name	Description
Compliance URL	Official compliance, privacy, or security page

ACKNOWLEDGMENT

I would like to extend my sincere gratitude to the faculty at the University of the Cumberlands for their guidance throughout my doctoral studies. Special thanks are also due to the cybersecurity professionals and organizations that contributed data to the "engine" [Appendix B] dataset, enabling this quantitative analysis of the compliance landscape.

REFERENCES

[1] SentinelOne, "What is Data Compliance? Standards and Regulations," *SentinelOne*, 29 Oct. 2024. [Online]. Available: https://www.sentinelone.com/cybersecurity-101/data-and-ai/data-compliance/.
[2] D. Goldman, "What is Security Compliance?," *Panorays*, 4 May 2023. [Online]. Available: https://panorays.com/blog/what-is-security-compliance/.
[3] SANS Institute, "Incident Response," *SANS Institute*, [Online]. Available: https://www.sans.org/security-resources/glossary-of-terms/incident-response/.
[4] SANS Institute, "Glossary of Cyber Security Terms," *SANS Institute*, [Online]. Available: https://www.sans.org/security-resources/glossary-of-terms/.
[5] SANS Institute, "Cybersecurity Risk Assessment," *SANS Institute*, [Online]. Available: https://www.sans.org/security-resources/glossary-of-terms/cybersecurity-risk-assessment/.
[6] NIST, "The NIST Cybersecurity Framework (CSF) 2.0," *NIST CSWP 29*, p. 2, 2024.
[7] National Institute of Standards and Technology, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)," *Special Publication 800-122*, pp. 2-1, 2-2, 3-3, 2010.
[8] PCI Security Standards Council, "Payment Card Industry Data Security Standard," *Requirements and Testing Procedures*, vol. 4.0, pp. 4-5, 2022.
[9] HHS.gov, "Summary of the HIPAA Privacy Rule," *U.S. Department of Health and Human Services (HHS)*, 14 Mar. 2025. [Online]. Available: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html#intro.
[10] NIST, "Vulnerability," *NIST*, [Online]. Available: https://csrc.nist.gov/glossary/term/vulnerability.
[11] A. Borgeaud, "Cybersecurity investment priorities for business leaders worldwide in 2025," *Statista*, 8 Jan. 2025. [Online]. Available: https://www.statista.com/statistics/1440668/business-leaders-cyber-security-investment-priorities-worldwide/.
[12] ENISA, "Raising Awareness of Cybersecurity: a Key Element of National Cybersecurity Strategies," *European Union Agency for Cybersecurity*, p. 30, 2021.
[13] A. S. Mollashaik, "Navigating the Transition: Key Considerations when Moving from Information Security to Privacy," *International Research Journal of Modernization in Engineering Technology and Science*, vol. 7, no. 2, pp. 332-333, 2025.
[14] IAPP.org, "Privacy Governance Report 2024," *iapp.org*, Nov. 2024. [Online]. Available: https://iapp.org/resources/article/privacy-governance-report/.
[15] J. Daniels, "Privacy Program Management," *IANS*, 2023.
[16] Bitsight, "The Evolution of the CISO," *Bitsight*, p. 3, 2023.
[17] IBM, "Cost of a Data Breach Report 2024," *IBM*, Armonk, 2024.
[18] A. Petrosyan, "Data Breaches Worldwide - Statistics & Facts," *Statista*, 19 Nov. 2024. [Online]. Available: https://www.statista.com/topics/11610/data-breaches-worldwide/.
[19] "API v3," *;--have i been pwned?*, [Online]. Available: https://haveibeenpwned.com/API/v3#AllBreaches.
[20] "Search Filings," *SEC.gov*, [Online]. Available: https://www.sec.gov/search-filings.
[21] ITRC, "Reports," *ITRC*, [Online]. Available: https://www.idtheftcenter.org/reports/.
[22] Verizon, "Explore the archive," *Verizon*, [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/#archive.
[23] Cyber Security News, "Data Breaches," *Cyber Security News*, [Online]. Available: https://cybersecuritynews.com/category/data-breaches/.
[24] S. Alder, "Healthcare Data Breach Statistics," *The HIPAA Journal*, 20 Mar. 2025. [Online]. Available: https://www.hipaajournal.com/healthcare-data-breach-statistics/.

[25] Z. Yang and C. Su, "Institutional Theory in Business Marketing: A Conceptual Framework and Future Directions," *Industrial Marketing Management*, vol. 43, pp. 721-722, 2014.
[26] V. Valentinov and C. Iliopoulos, "The Idea of Adaptation in Transaction Cost Economics: an Application to Stakeholder Theory," *Society and Business Review*, vol. 19, p. 484, 2024.
[27] K. Patil et al., "Firm Performance in Digitally Integrated Supply Chains: a Combined Perspective of Transaction Cost Economics and Relational Exchange Theory," *Journal of Enterprise Information Management*, vol. 37, no. 2, p. 383, 2024.
[28] C. Grant and A. Osanloo, "Understanding, Selecting, and Integrating a Theoretical Framework in Dissertation Research," *Administrative Issues Journal*, p. 12, 2014.
[29] K. Khaldi, "Quantitative, Qualitative or Mixed Research: Which Research Paradigm to Use?," *Journal of Educational and Social Research*, p. 17, 2017.
[30] D. H. Bibi et al., "A Critique Of Research Paradigms And Their Implications For Qualitative, Quantitative And Mixed Research Methods," *Webology*, vol. 19, no. 2, p. 7322, 2022.
[31] S. Linstead et al., "Theorizing and Researching the Dark Side of Organization," *Organization Studies*, vol. 35, pp. 168, 173, 2014.
[32] G. Widding, "Keep a-knocking (but you can't come in): the Issue of Passing by the Gatekeeper," *Education Inquiry*, vol. 3, no. 3, pp. 426, 428, 433, 2012.
[33] H. N. Chua, J. S. Teh and A. Herbland, "Identifying the Effect of Data Breach Publicity on Information Security Awareness Using Hierarchical Regression," *IEEE Access*, vol. 9, pp. 121760, 121767, 2021.
[34] J. D. Schenker and P. D. R. Jr, "Causal-comparative Research Designs," *Journal of Vocational Rehabilitation*, pp. 117-119, 121, 2004.

AUTHORS

Eric L. David, PhD, Information Technology – Information Security/Data Analytics, University of the Cumberlands, 2023. Dissertation: "Evaluating the Impact of Metrics-based Security Tools on Company Performance and Decision-making". Email: eric.david@outlook.com. Dr. Eric L. David is a specialist in cybersecurity leadership and analytics. He possesses extensive experience in Information Technology across diverse global sectors, including Finance, Healthcare, Technology, Gaming, and the Supply Chain. His research focuses on the intersection of regulatory compliance, technical vulnerability, and organizational performance metrics.