

Assignment 2.1: Creating a Risk Analysis Report

Joshua A. Wortz

University of San Diego

CSOL-530

Cameron Carter, MS

05/17/2025

Introduction

Cybersecurity threats are increasing in scale, frequency, and complexity across all sectors. As organizations become more reliant on interconnected systems and digital services, the potential impact of a security breach continues to rise. In this evolving threat landscape, decision-makers must look beyond intuition and anecdotal experience and adopt data-driven approaches to cybersecurity risk management. The 2024 Verizon Data Breach Investigations Report (DBIR), now in its 17th edition, is a foundational source of empirical threat intelligence. This report analyzes real-world breaches and incidents to uncover patterns in attacker behavior, exploited vulnerabilities, and organizational weaknesses. Using these insights, this analysis applies data-driven decision-making (DDDM) principles to identify high-priority cybersecurity risks and recommend targeted mitigation strategies. The ultimate goal is to help organizations understand where they are vulnerable and how best to allocate limited resources to reduce the likelihood and impact of breaches.

Key Cybersecurity Risks

Among the most significant trends reported in the 2024 DBIR is the dramatic rise in exploiting vulnerabilities as an initial access vector. Exploitation nearly tripled in frequency compared to the previous year, representing a 180% increase, primarily due to attacks that leveraged zero-day vulnerabilities such as those found in MOVEit file transfer software. These attacks, often carried out by ransomware and extortion groups, made web applications one of the most commonly targeted assets across all industries (Verizon, 2024). This trend underscores the continued challenge organizations face in patching software quickly and highlights the growing impact of software supply chain risks.

Credential theft and abuse also remain dominant in the cyber threat landscape. The DBIR identifies using stolen credentials as the most common action in breaches, present in approximately 24% of confirmed cases. These attacks typically involve unauthorized access to cloud-hosted email and collaboration platforms, with attackers often gaining access through credential stuffing or phishing. Once inside, attackers may exfiltrate sensitive data or move laterally through systems to deploy malware or ransomware (Verizon, 2024).

Ransomware and extortion attacks have become more nuanced and strategic. While the volume of traditional ransomware incidents declined slightly, there has been a corresponding rise in pure extortion cases, which now account for 9% of breaches. When combined, these related tactics represent 32% of breaches overall. The shift illustrates how ransomware groups adapt to avoid detection and increase pressure on victims, often by threatening to release stolen data without encrypting files (Verizon, 2024).

Social engineering tactics, especially business email compromise (BEC), have also grown more prevalent. The report notes that pretexting attacks—where adversaries impersonate executives or partners to manipulate employees—are now more common than phishing. These BEC attacks were present in 24–25% of financially motivated incidents and often resulted in significant financial losses, with a median transaction amount of around \$50,000 (Verizon, 2024).

Finally, human error remains a pervasive issue. Errors, including misconfigurations, misdeliveries, and failures to apply security controls, contributed to 28% of breaches. The expansion of mandatory breach reporting has revealed the frequency of these incidents, many of which might have previously gone unreported. These findings highlight the importance of procedural rigor and security training across all levels of an organization.

Data-Driven Analysis

The Verizon 2024 DBIR analyzed 30,458 real-world security incidents, including 10,626 confirmed data breaches, covering victims from 94 countries. This robust dataset enables a nuanced understanding of cyber risks across industries and organization sizes. Data from the report identifies the most common breach pathways, including vulnerability exploitation, credential misuse, and manipulation of human behavior.

Ransomware and extortion incidents pose especially costly threats. FBI Internet Crime Complaint Center (IC3) data cited in the report shows that the median loss for ransomware victims who paid was \$46,000, with ransom demands ranging from less than \$100 to over \$1 million in some cases (Verizon, 2024). Furthermore, ransomware actors commonly demand a percentage of the victim's revenue, typically around 1.34%, indicating that they are tailoring their attacks to organizational scale. In many cases, the damage extends far beyond the ransom payment, including business interruption, reputational harm, and legal liability.

Credential-based attacks continue to be a low-cost, high-reward strategy for cybercriminals. In 2024, attackers primarily gained access to systems through stolen usernames and passwords. The use of credentials was especially prevalent in web application attacks, which were often directed at cloud email systems or externally exposed administrative interfaces. These findings reinforce the need for strong identity and access management practices (Verizon, 2024).

The human element remains a critical vulnerability, playing a role in 68% of breaches. Whether through error, social engineering, or insider misuse, people represent both a line of defense and a potential point of failure. The report emphasizes that training and awareness can significantly reduce the likelihood of successful phishing or BEC attacks. However, the speed at which users

fall victim remains a challenge. In phishing simulations, the median time from email open to credential entry was less than 60 seconds (Verizon, 2024), leaving minimal time for security systems or personnel to intervene.

Finally, the DBIR's expanded analysis of supply chain risk reveals that 15% of breaches involved third-party or partner systems—a 68% increase from the previous year. These incidents often stemmed from vendor software vulnerabilities or direct compromises of partner systems. The MOVEit breach is a prime example, with over 1,500 breach notifications tied to that single incident. This reinforces the importance of vendor risk management and secure-by-design procurement practices (Verizon, 2024).

Recommended Risk Mitigation Strategies

Given the data above, risk mitigation strategies should focus on technical and human-centric controls. The first area of emphasis should be vulnerability management. Organizations must improve their ability to detect and remediate high-priority vulnerabilities, particularly those listed in the CISA Known Exploited Vulnerabilities (KEV) catalog. According to the DBIR, 50% of these vulnerabilities remain unpatched for over 55 days, with exploitation often occurring within five days of public disclosure. Organizations should implement automated patch management systems, prioritize KEV vulnerabilities, and conduct frequent external attack surface assessments to identify exposed systems (Verizon, 2024).

The second strategy involves enhancing credential protection and access controls. Multi-factor authentication (MFA) should be mandated across all privileged and externally accessible accounts. Additionally, password policies should discourage reuse, and tools such as password

managers can reduce user friction. Behavioral analytics and log monitoring should be used to detect unusual login activity or access anomalies that may indicate account compromise.

Third, organizations should invest in robust security awareness training. Since the human element contributes to over two-thirds of breaches, targeted training can help employees recognize phishing, pretexting, and social engineering attacks. Simulated phishing campaigns, combined with rapid feedback and reporting mechanisms, can create a culture of vigilance. Furthermore, establishing clear playbooks for incident response, especially in the case of ransomware or extortion attempts, can reduce confusion and minimize damage when incidents occur.

These controls should not exist in isolation. A layered security approach that combines preventative, detective, and responsive capabilities is essential. Security leaders must continuously evaluate their risk landscape, informed by empirical data, and align their defenses to the most likely and most damaging attack scenarios.

Conclusion and Future Considerations

The findings from the 2024 DBIR make it clear that cyber threats are not only persistent but increasingly sophisticated. Exploited vulnerabilities, stolen credentials, and human errors remain the top contributors to industry data breaches. However, these risks are not insurmountable. By adopting data-driven decision-making practices, organizations can prioritize controls that are most effective at reducing the impact and likelihood of these attacks.

Looking to the future, organizations must also recognize that cybersecurity is no longer confined to internal systems. With the rise in third-party and supply chain compromises, due diligence in

vendor selection and a commitment to secure-by-design principles will become even more critical. Regulatory trends, such as increased breach reporting mandates, will provide greater transparency and create market incentives for security improvements.

Effective cybersecurity governance ultimately depends on cultural maturity, technical capability, and data-informed leadership. Organizations that embrace these principles will be better equipped to defend against today's threats and adapt to tomorrow's.

References

Verizon. (2024). *2024 Data Breach Investigations Report*.

<https://www.verizon.com/business/resources/reports/dbir/>

CISA. (2023). *Secure by Design*. Cybersecurity and Infrastructure Security Agency.

<https://www.cisa.gov/securebydesign>

Microsoft. (2024, February 14). *Staying ahead of threat actors in the age of AI*. Microsoft

Security Blog. <https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/>