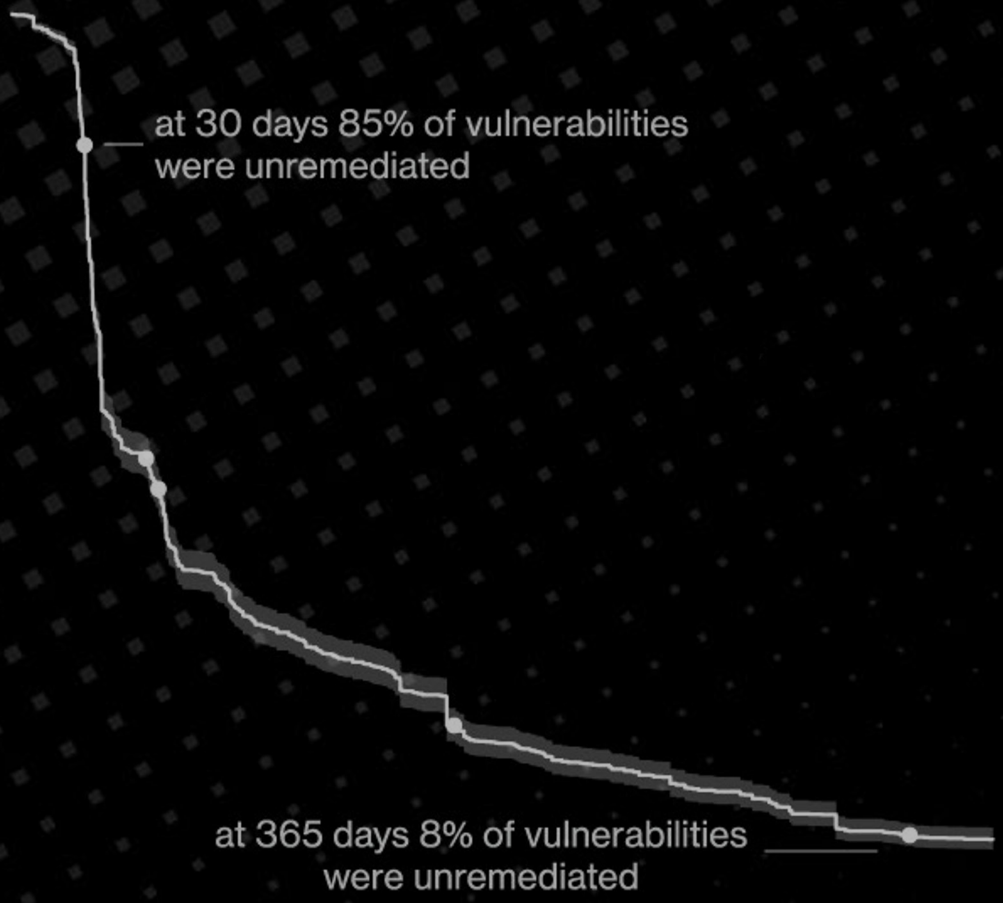
Post DBIR 2024
7 Ways to Reduce Your Cyber Risk

2024 Verizon Data Breach Investigations Report (DBIR):
The Rise of Vulnerability Exploitation



Balbix®

The Verizon DBIR is the most anticipated annual report on data breaches with many incredible insights, and this year is no exception. The most surprising finding is the rapid explosion in vulnerability exploitation, which now constitutes one of the most critical paths to initiating breaches.

Balbix is a data contributor to Verizon DBIR, and we have poured over this report to provide seven key actionable takeaways to enable you and your organization to navigate the riskiest areas of cyber risk and deliver suggestions to improve your security.

Download the

2024 Verizon Business Data Breach Investigation Report

Key Findings

Key DBIR Finding #1

Vulnerability Exploits Are Exploding

This year has seen a **180%** increase in vulnerability exploits, with the MOVEit vulnerability and other zero-day exploits increasingly leveraged by ransomware and extortion-related threat actors.

Recommendation:

Use a Risk-Based Approach to Remediating Vulnerabilities

Shift to a risk-based approach to fixing vulnerabilities associated with internet-facing assets. Cyber Risk Quantification (CRQ) can help you prioritize vulnerabilities by financial impact, zeroing in on and quickly remediating the most severe ones.

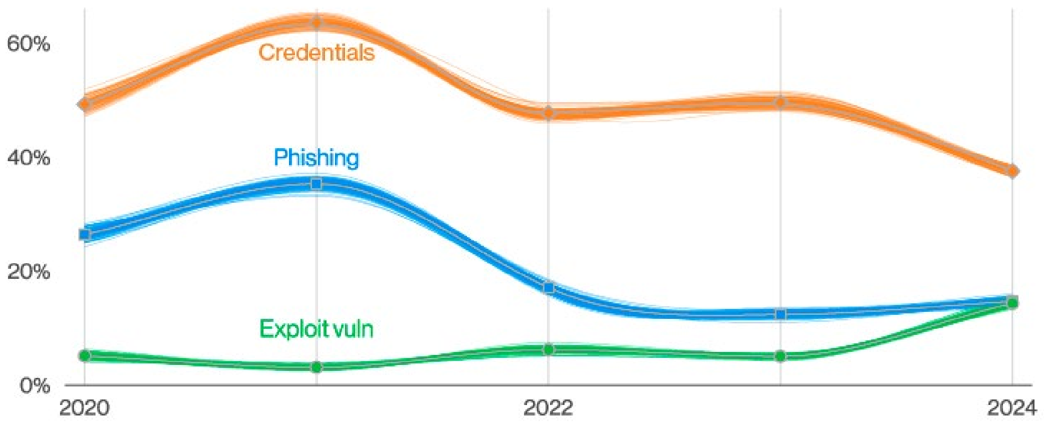


Figure 6. Select ways-in enumerations in non-Error, non-Misuse breaches over time

Key DBIR Finding #2

Don't Wait for Vulnerabilities to Get on KEV

The median time from initial vulnerability publication to first detection of adversary scanning activity for CISA KEV is **five days, compared to 68 days** for non-CISA KEV CVEs.

Recommendation:

Prioritize Remediation of CISA KEV Listed Vulnerabilities

With a risk-based approach, you should be able to remediate high-impact vulnerabilities before they are listed in the CISA KEV catalog. But, when a vulnerability is listed in the CISA KEV, you should immediately prioritize it for remediation since adversaries are exploiting these vulnerabilities.

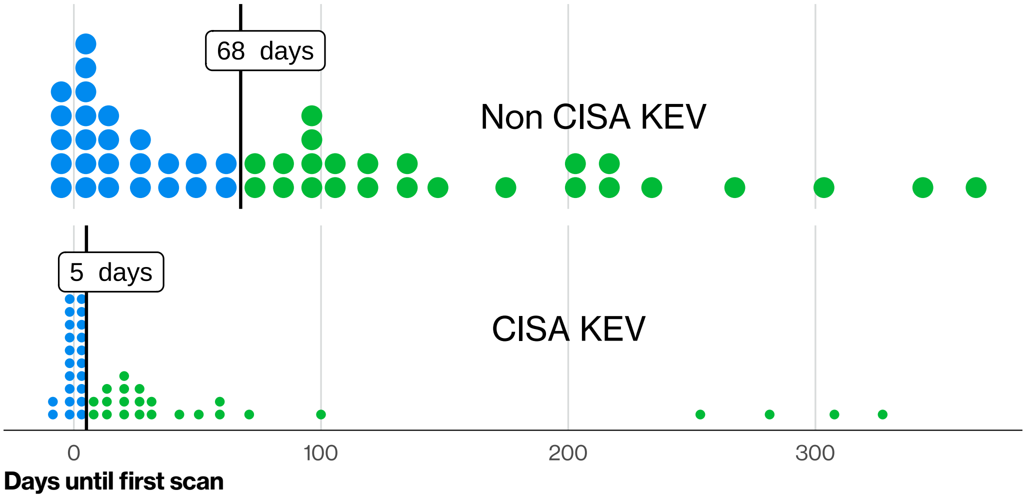


Figure 20. Time from publication of vulnerability to first scan seen (from 2020 onward)

Note: The CISA KEV, or the Cybersecurity & Infrastructure Security Agency's Known Exploited Vulnerabilities (KEV) catalog, is a curated list of vulnerabilities known to be actively exploited by cybercriminals. This resource is maintained by CISA, an agency of the United States Department of Homeland Security responsible for enhancing the security, resilience, and reliability of the nation's cybersecurity and communications infrastructure.

Key DBIR Finding #3

CISA KEV Remediation Takes Too Long

By doing a survival analysis of vulnerability management data and focusing on the vulnerabilities in the CISA Known Exploited Vulnerabilities (KEV) catalog (an area of focus in vulnerability management), the report found it takes around **55 days** to remediate **50%** of those critical vulnerabilities once their patches are available. The patching doesn't start picking up until after the 30-day mark, and by the end of the year, around **8%** are still open.

Recommendation:

Track Vulnerability Management Metrics

Track vulnerability management metrics such as Mean Open Vulnerability Age (MOVA) and Mean Time to Remediate (MTTR) to benchmark your program's performance and identify areas for improvement (e.g., material assets and high-priority vulnerabilities).

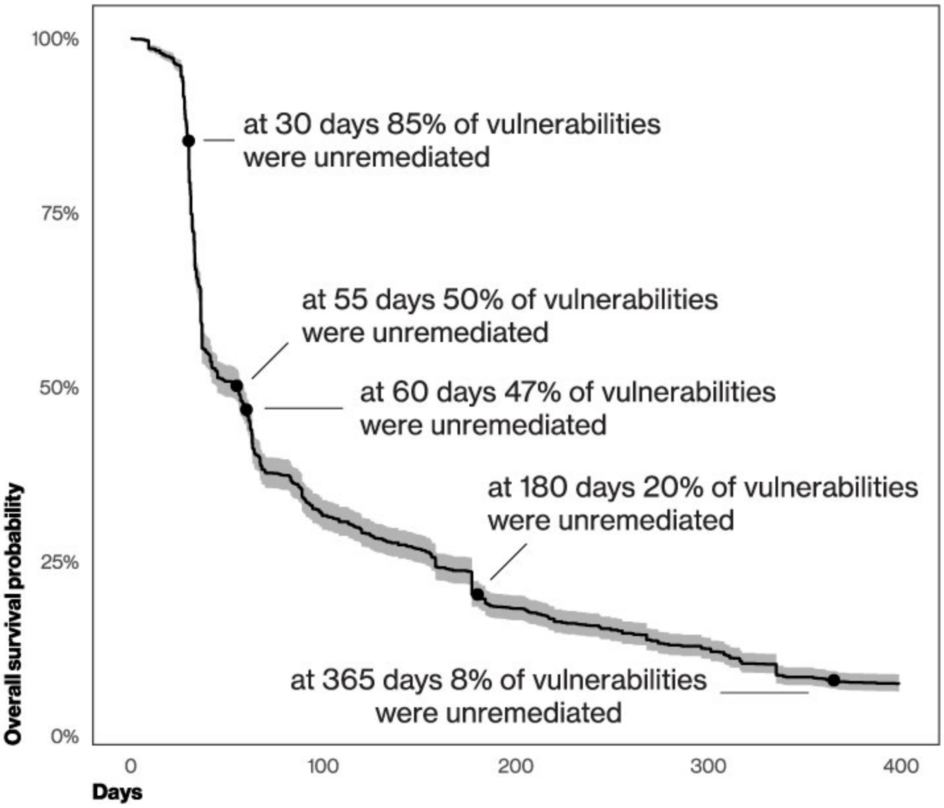


Figure 19. Survival analysis of CISA KEV vulnerabilities

Key DBIR Finding #4

Third-Party Vulnerabilities Are on the Rise

Third-party vulnerabilities (e.g., SaaS, business, and open-source apps) are rising. These vulnerabilities can lead to breaches like the SolarWinds attack. Supply chain interconnection influenced **15%** of the breaches this year, a significant increase from **9%** last year.

Recommendation:

Understand Your Software Supply Chain

Maintain an accurate and up-to-date Software Bill of Materials (SBOM). Without an SBOM, identifying third-party vulnerabilities could take weeks or months. Many companies took a long time to discover all their instances of Log4j. Also, there is a growing reliance on FOSS (free and open source software) and the criticality of SBOM in responding to sophisticated attacks such as the recent XZ Utils Backdoor attack.

Additionally, monitor systems to detect unusual activity or potential breaches in real time. This allows for immediate response and mitigation of security threats throughout the supply chain.

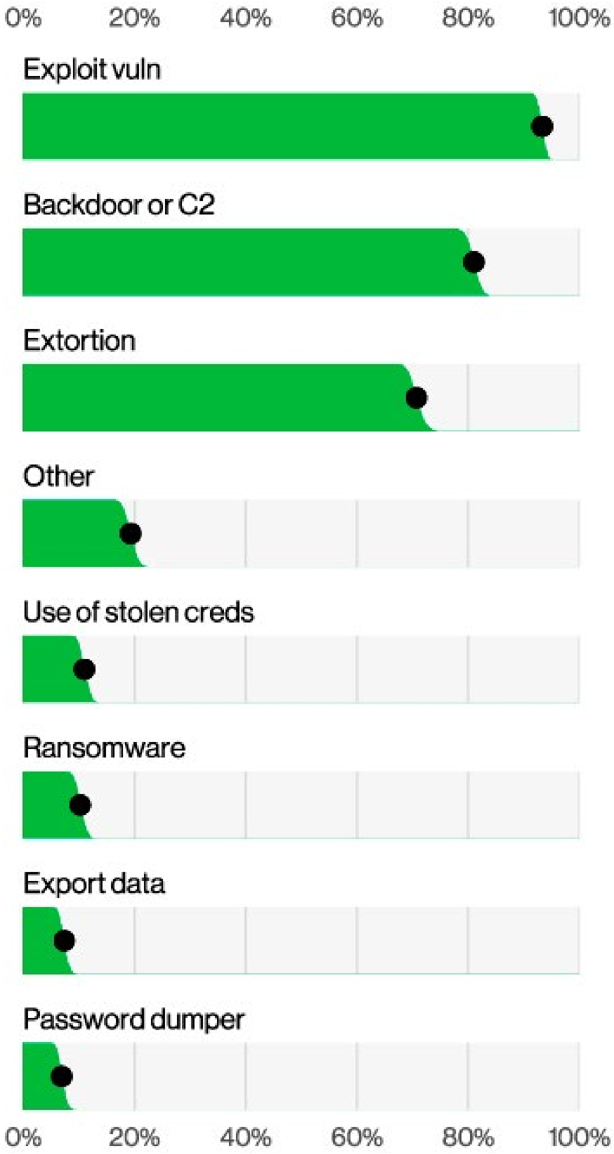


Figure 10. Action varieties in selected supply chain interconnection breaches (n=1,075)

Key DBIR Finding #5

Misconfigurations Are Falling but Still Pose a Considerable Risk

Misconfigurations were seen in approximately **10%** of breaches. While on a downward trend for the last three years due to more systems becoming more secure by default, misconfigurations still pose a considerable risk of exploitation.

Recommendation:

Monitor Software Configurations

Leverage automated techniques to identify and remediate misconfigurations. These methods can help scan your systems for deviations from desired configurations and automate applying corrective actions. Also, it is best to harden systems via stricter enforcement of configuration controls.

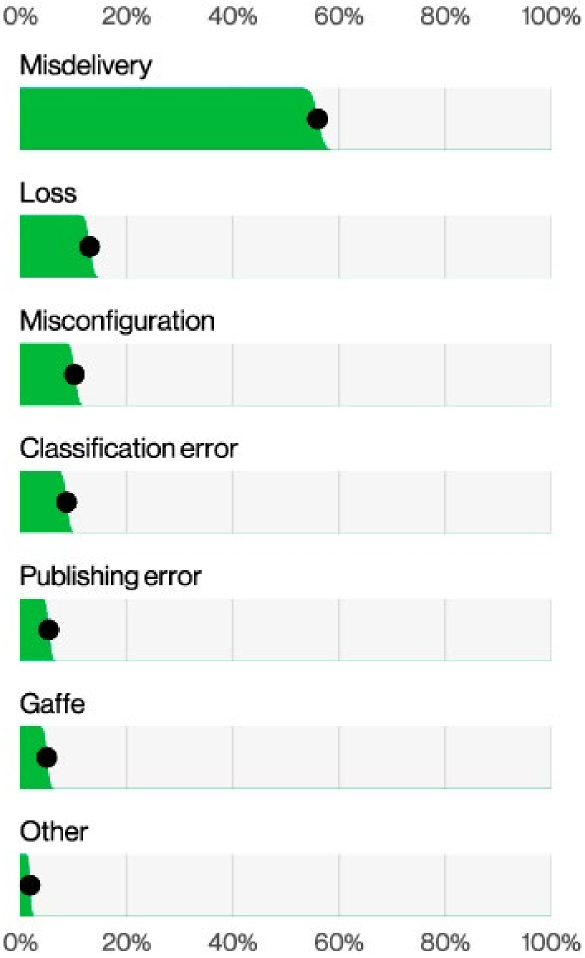


Figure 46. Top Action varieties in Miscellaneous Errors breaches (n=2,586)

Key DBIR Finding #6

Ransomware/extortion Is Still Dominant

Roughly **one-third** of all breaches involve Ransomware or Extortion. Extortion attacks, which are less familiar to many, may or may not involve actual access to data like ransomware but use the threat of damage or disclosure to coerce payment. These attacks have risen over the past year and are now a component of **9%** of all breaches (as opposed to a decline in Ransomware to **23%**.) Over the past three years, the combination of Ransomware and other Extortion breaches accounted for almost two-thirds of financially motivated attacks (fluctuating between **59%** and **66%**).

Recommendation:

Backup Data and Prioritize Remediation

Ransomware often exploits vulnerabilities in software and operating systems. As your first (and ongoing) proactive measure, you should deploy data backup and restoration mechanisms and provide continuous backup and data monitoring for critical systems.

A multi-layered security approach also reduces the initial risk of infections by providing multiple defensive barriers. The key to this is monitoring all systems, software and applications for high-severity vulnerabilities and patching them before they can be exploited by ransomware. Focus on specifically identifying vulnerabilities linked to ransomware and other malware to prioritize remediation efforts in a risk-based manner.

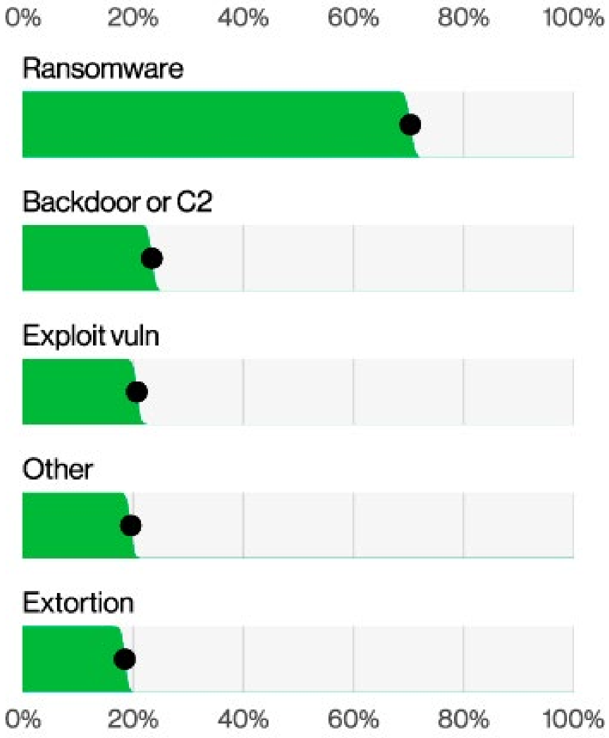


Figure 28. Top Action varieties in System Intrusion incidents

Key DBIR Finding #7

Privilege Misuse Is Growing

Social engineering and abuse of privileges have been an evergreen challenge. Yet, the latter is increasingly used by internal bad actors (**35%**, a significant increase from last year's **20%**.) vs. external attackers (**65%**), though external actors still perform most breaches. Primary motives this year are Financial (**88%**) and espionage (**46%**).

Recommendation:

Monitor and Control Identities

First, adopt a zero-trust mindset, maintaining strict access controls to your systems and data and not trusting anyone by default, even those inside your network. Second, implement the principle of least privilege by continuously monitoring and right-sizing user identities and maintaining only the access users need, especially when joining, moving, and leaving the organization. Over-privileged internal users should be monitored since broad access can magnify a breach's blast radius dramatically. Finally, you should consistently implement MFA (Multi-Factor Authentication).

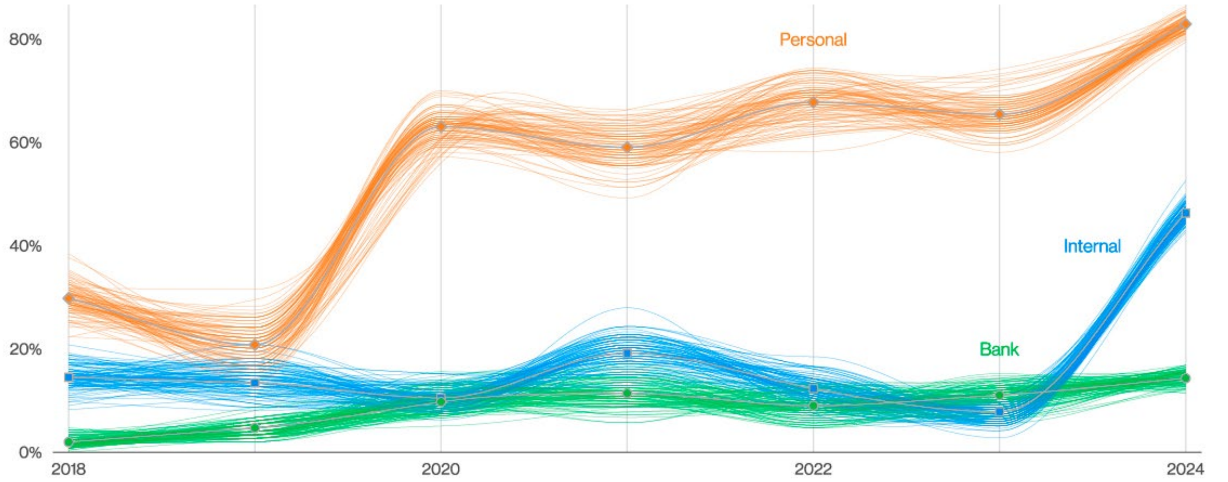


Figure 55. Top Confidentiality data varieties over time in Privilege Misuse breaches

GenAI in Attacks — More Hype Than Reality

One overall observation from the DBIR report is that Verizon looked at the emerging field of generative artificial intelligence (GenAI) in attacks and its potential effects. However, nothing in the incident data indicated its use is currently rising. You should still monitor this as GenAI will eventually have the potential to be very impactful from an adversary perspective in the future. Fortunately, AI-powered security solutions like Balbix are currently ahead of the hackers in using AI, though it's an ongoing race.

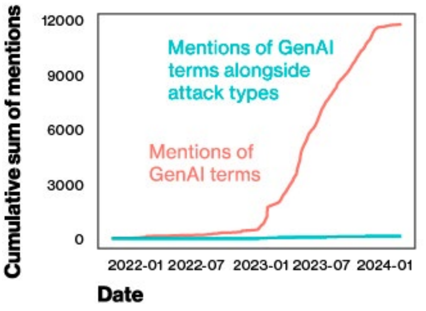


Figure 14. Cumulative sum of GenAI in criminal forums

Conclusion

The findings in this year's report underscore the urgency with which organizations must take a risk-based approach to reduce their exposure to vulnerability exploitation and misconfigurations and implement risk management solutions that prioritize risks and significantly reduce remediation times. The seven actionable takeaways provided are designed to guide you through the complexities of the current threat landscape, helping you not only to identify but effectively mitigate the areas of highest risk.

By implementing these suggestions, your organization can enhance its defensive mechanisms, stay ahead of potential threats, and foster a more secure operational environment. Embracing these insights will not only safeguard your data and systems but also reinforce your organization's commitment to maintaining cyber resilience. In the digital age, an informed and proactive approach to cybersecurity is not just an option — it is a necessity.

Thank you to the entire DBIR team, especially C. David Hylender, Philippe Langlois, Alex Pinto and Suzanne Widup for working tirelessly on this report and arming the defenders with data to continue waging the good fight.