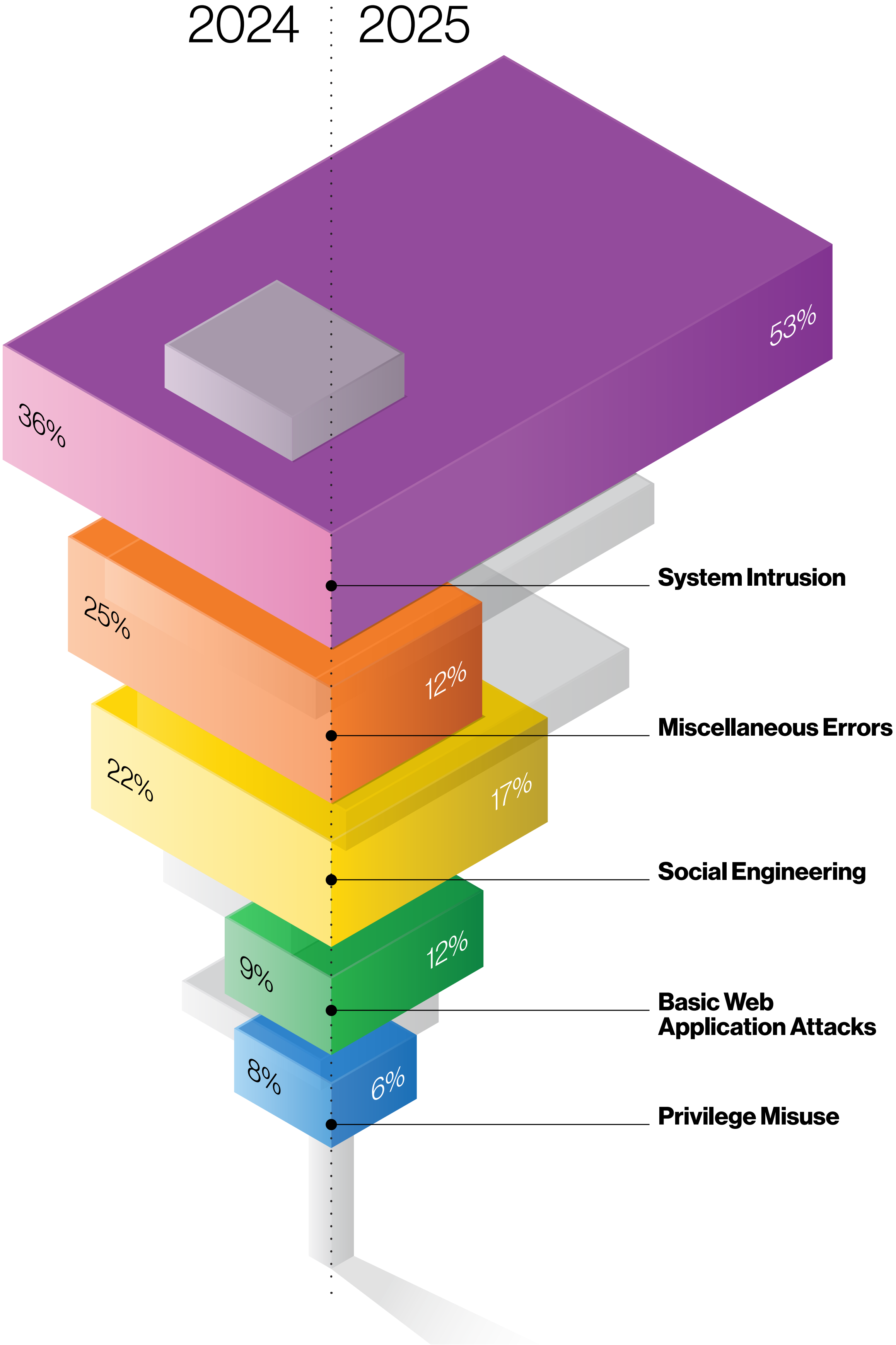
# 2025 Data Breach Investigations Report

## Executive Summary

verizon business


2024
2025
36%
53%
25%
12%
22%
17%
9%
12%
8%
6%
System Intrusion
Miscellaneous Errors
Social Engineering
Basic Web Application Attacks
Privilege Misuse

## About the cover

Third-party involvement in breaches was an ever-present subject in incidents throughout this past year. Third parties can not only act as custodians to customers' data, but they can also underpin critical parts of organizations' operations.

Our incredible design team rose to the challenge of representing the balancing act an organization's security programs have to perform with the growing dependence on those third parties. If the impossibly balanced shape on the cover makes you uncomfortable, you have begun to understand the challenges modern Chief Information Security Officers (CISOs) face in the current environment.

Throughout its "spine," you can find encoded the Incident Classification Patterns that were most prevalent in breaches in our incident dataset (with the previous year's data oriented to the left of the center and the current year's data to the right). The inner cover represents those quantities in a less abstract way.

The shape might look too fragile to continue standing, but the fact that it is holding steady is a monument to all the hard work and collaboration that the industry has brought to bear. With the proper amount of collaboration, organization and information sharing, we can continue to strengthen cybersecurity efforts and maybe have a good night of sleep or two in the future as a treat.

# Table of contents

**Welcome** 5

**Report highlights/ summary of findings** 6

**Industry highlights** 10

Educational Services 10

Financial and Insurance 11

Healthcare 11

Manufacturing 12

Retail 12

Public Sector 13

**At-a-glance industry facts** 14

**Regional findings** 16

**Stay informed and threat ready.** 18

# Welcome

## Hello, and welcome to Verizon's 2025 Data Breach Investigations Report (DBIR).

We are thrilled to have you with us for this, the 18th annual installment of the DBIR. Whether you are a longtime reader or this is your first rodeo, you will find within the pages of this report a robust examination of the recent state of cybercrime, along with insights on what threats your organization may likely face, who is behind them and what you can do to help protect yourself.

This year, the Verizon DBIR team analyzed 22,052 real-world security incidents, of which 12,195 were confirmed data breaches that occurred inside organizations of all sizes and types. This represents the highest number of breaches ever analyzed in a single report. These incidents and breaches were provided from the case files of the Verizon Threat Research Advisory Center (VTRAC) team, along with the generous support of our global contributors, and from publicly disclosed security incidents. Together, these attacks represent victims from 139 countries around the world.

Although the threat landscape can vary somewhat due to organizational size, mission and location, there are always certain overarching themes that seem to predominate our dataset regardless of any of these variables. This year is no exception. Possibly the most obvious and noteworthy among them is the role that third-party relationships play in how and why breaches occur.

While, to some extent, software vendors have long played a part in unintentionally increasing the attack surface for those who use their products and services, over the last two to three years, it has moved from the occasional (and typically minor to moderate) mishap to a much more widespread and insidious problem that can (and sometimes does) have a devastating effect on enterprises. In fact, this is the case to such an extent that it made the cover visualization for this year's report, and you will find the subject woven throughout this document.

**Please continue reading for report highlights, including the latest breach findings for industries and regions. Please feel free to pass this summary to colleagues and download the full report for a more in-depth view of the threats you might face today.**

# Report highlights/ summary of findings

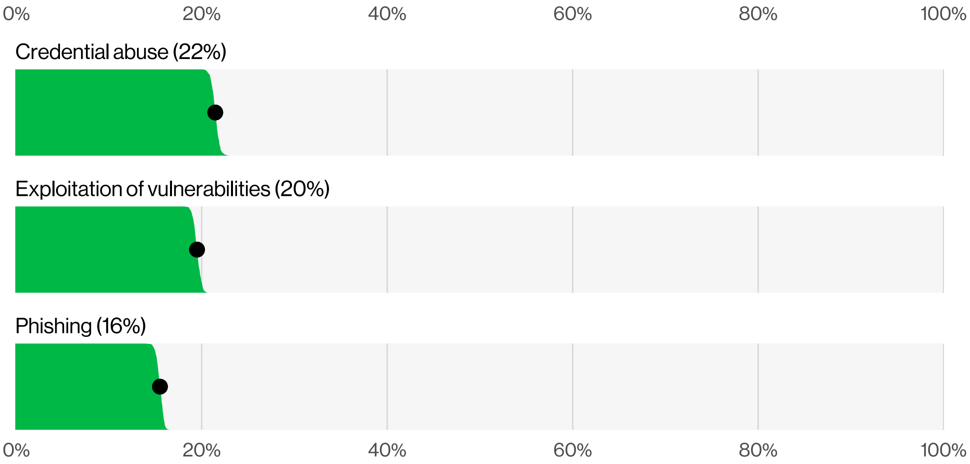


**Figure 1.** Known initial access vectors in non-Error, non-Misuse breaches (n=9,891)

The exploitation of vulnerabilities has seen another year of growth as an initial access vector for breaches, reaching 20%. This value approaches that of credential abuse, which is still the most common vector. This was an increase of 34% in relation to last year's report and was supported, in part, by zero-day exploits targeting edge devices and virtual private networks (VPNs). The percentage of edge devices and VPNs as a target on our exploitation of vulnerabilities action was 22%, and it grew almost eight-fold from the 3% found in last year's report. Organizations worked very hard to patch those edge device vulnerabilities, but our analysis showed only about 54% of those were fully remediated throughout the year, and it took a median of 32 days to accomplish.

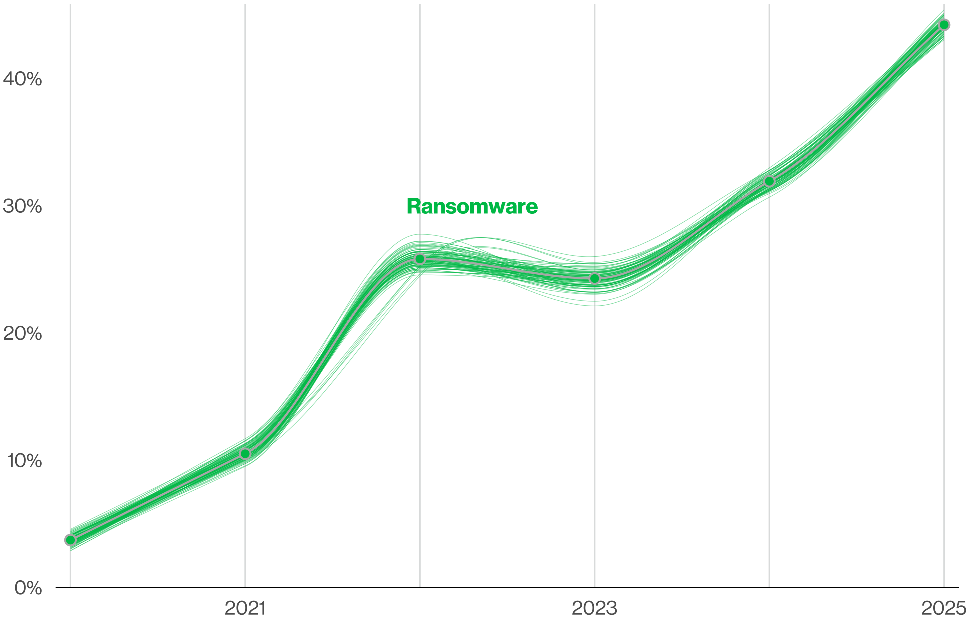


**Figure 2.** Ransomware action over time in breaches (n for 2025 dataset=10,747)

The presence of Ransomware, with or without encryption, in our dataset also saw significant growth—a 37% increase from last year's report. It was present in 44% of all the breaches we reviewed, up from 32%. In some good news, however, the median amount paid to ransomware groups has decreased to $115,000 (from $150,000 last year). 64% of the victim organizations did not pay the ransoms, which was up from 50% two years ago. This could be partially responsible for the declining ransom amounts.

Ransomware is also disproportionally affecting small organizations. In larger organizations, Ransomware is a component of 39% of breaches, while SMBs experienced Ransomware-related breaches to the tune of 88% overall.

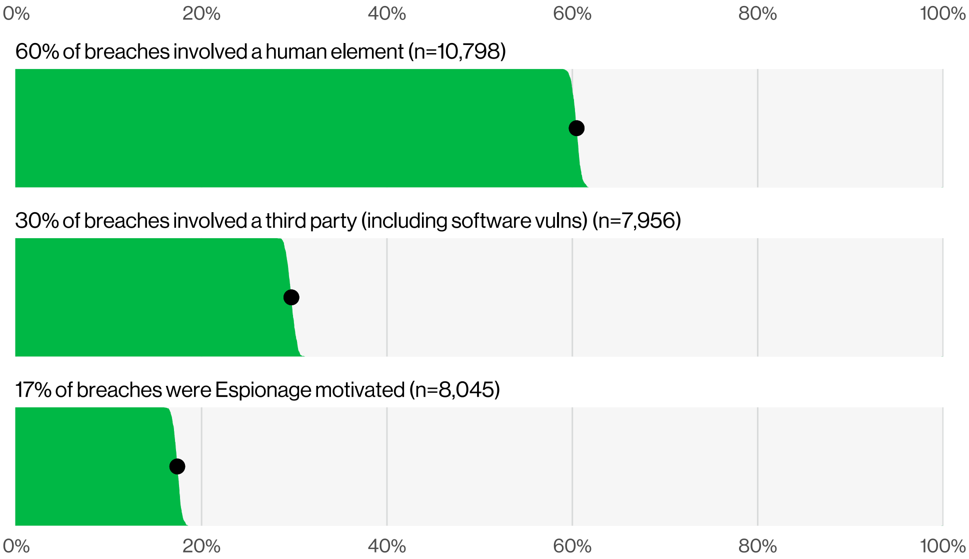


**Figure 3.** Select key enumerations in breaches

Although the involvement of the human element in breaches remained roughly the same as last year, hovering around 60%, the percentages of breaches where a third party was involved doubled, going from 15% to 30%.

There were notable incidents this year involving credential reuse in a third-party environment—in which our research found the median time to remediate leaked secrets discovered in a GitHub repository was 94 days.

We also saw significant growth in Espionage-motivated breaches in our analysis, which are now at 17%. This rise was, in part, due to changes in our contributor makeup. Those breaches leveraged the exploitation of vulnerabilities as an initial access vector 70% of the time, showcasing the risk of running unpatched services. However, we also found that Espionage was not the only thing state-sponsored actors were interested in—approximately 28% of incidents involving those actors had a Financial motive. There has been media speculation that this may be a case of the threat actors double-dipping to pad their compensation.

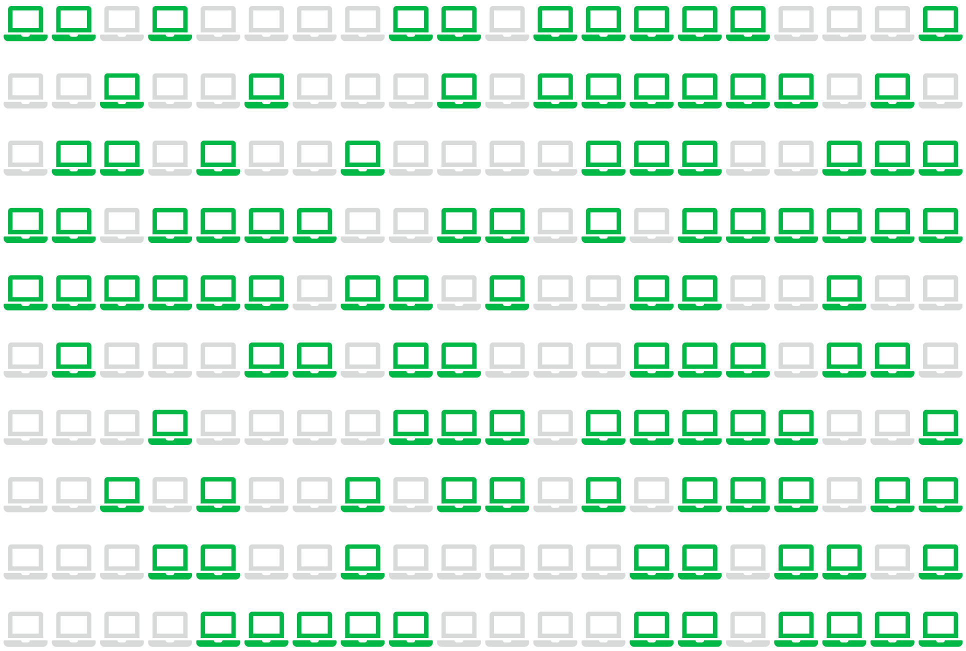


**Figure 4.** Percentage of non-managed devices with corporate logins in infostealer logs (each glyph is 0.5%)

With regard to stolen credentials, analysis performed on information stealer malware (infostealer) credential logs revealed that 30% of the compromised systems can be identified as enterprise-licensed devices. However, 46% of those compromised systems that had corporate logins in their compromised data were non-managed and were hosting both personal and business credentials. These are most likely attributable to a bring your own device (BYOD) program or are enterprise-owned devices being used outside of the permissible policy.

By correlating infostealer logs and marketplace postings with the internet domains of victims that were disclosed by ransomware actors in 2024, we saw that 54% of those victims had their domains show up in the credential dumps (for instance, as URLs the credentials allegedly gave access to), and 40% of the victims had corporate email addresses as part of the compromised credentials. This suggests these credentials could have been leveraged for those ransomware breaches, pointing to potential access broker involvement as a source of initial access vectors.

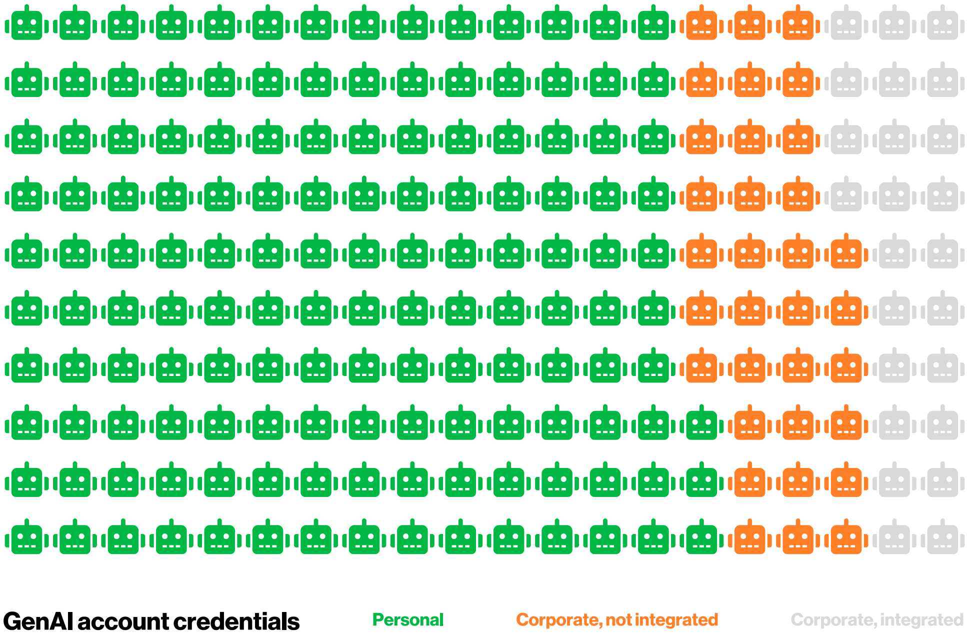


**Figure 5.** Percentage breakdown of GenAI service access account types (each glyph is 0.5%)

As of early 2025, generative artificial intelligence (GenAI) has still not taken over the world, even though there is evidence of its use by threat actors as reported by the AI platforms themselves. Also, according to data provided by one of our partners, synthetically generated text in malicious emails has doubled over the past two years.

A closer-to-home emerging threat from AI is the potential for corporate-sensitive data leakage to the GenAI platforms themselves, as 15% of employees were routinely accessing GenAI systems on their corporate devices (at least once every 15 days). Even more concerning, a large number of those were either using non-corporate emails as the identifiers of their accounts (72%) or were using their corporate emails without integrated authentication systems in place (17%), most likely suggesting use outside of corporate policy.

# Industry highlights

**As mentioned in the introduction, this year we examined 22,052 security incidents, of which 12,195 were confirmed data breaches. In this section, we break those incidents and breaches down and look at them from an industry-specific perspective. As one might imagine, what one industry wrestles with frequently, another industry may rarely encounter. The differences between the threats various industries face often come down to each organization's unique attack surface.**

A multinational financial institution, for instance, may face a different set of threats than a regional logistics company. However, in many cases, there may also be a surprising amount of overlap between the two. At the end of the day, as we point out elsewhere in this report, threat actors appear to care less about an organization's size, industry vertical or geographical location than one might think. Today's cybercriminal is a bit of a pragmatist and largely subscribes to the "I'll be happy to steal whatever you have on hand" view. To really understand this section, you must also keep in mind other variables, such as the differing reporting requirements that might exist between industries and the corresponding level of scrutiny that they may receive, the overall sample size that we have for a given industry and so on. Therefore, we caution you to keep these and other factors in mind when judging the security posture of any particular vertical. Finally, please keep in mind that we classify organizations using the North American Industry Classification System (NAICS) codes.

## Educational Services

**(NAICS 61)**

| | |
|---|---|
| **Frequency** | 1,075 incidents, 851 with confirmed data disclosure |
| **Top patterns** | System Intrusion, Miscellaneous Errors and Social Engineering represent 80% of breaches |
| **Threat actors** | External (62%), Internal (38%) (breaches) |
| **Actor motives** | Financial (88%), Espionage (18%) (breaches) |
| **Data compromised** | Personal (58%), Internal (49%), Other (35%), Credentials (12%) (breaches) |
| **What is the same?** | System Intrusion, Miscellaneous Errors and Social Engineering are still the top three patterns, as they have been for the last two years. |
| **Summary** | While we saw a decrease in the number of both incidents and breaches in the Educational Services industry, the attacks that we did see were along the lines of what we have seen in the past. System Intrusion is far and away the top pattern, and it is driven by financially motivated External actors. |

## Financial and Insurance

**(NAICS 52)**

| | |
|---|---|
| **Frequency** | 3,336 incidents, 927 with confirmed data disclosure |
| **Top patterns** | System Intrusion, Social Engineering and Basic Web Application Attacks represent 74% of breaches |
| **Threat actors** | External (78%), Internal (22%), Partner (1%) (breaches) |
| **Actor motives** | Financial (90%), Espionage (12%) (breaches) |
| **Data compromised** | Personal (54%), Other (44%), Internal (35%), Credentials (22%) (breaches) |
| **What is the same?** | System Intrusion remains the top pattern once again, due to the preponderance of more complex attacks. Dare we hope this is because the adversaries are having to expend more effort? |
| **Summary** | The Financial and Insurance vertical is still dominated by financially motivated threat actors who will usually take any data type they can lay their hands on. However, attacks with the motive of Espionage have increased this year. |

## Healthcare

**(NAICS 62)**

| | |
|---|---|
| **Frequency** | 1,710 incidents, 1,542 with confirmed data disclosure |
| **Top patterns** | System Intrusion, Everything Else and Miscellaneous Errors represent 74% of breaches |
| **Threat actors** | External (67%), Internal (30%), Partner (4%), Multiple (1%) (breaches) |
| **Actor motives** | Financial (90%), Espionage (16%) (breaches) |
| **Data compromised** | Medical (45%), Personal (40%), Internal (32%), Other (24%) (breaches) |
| **What is the same?** | The attack patterns remain the same, although they have changed position since last year. |
| **Summary** | The Healthcare sector remains a prime target for cyberattacks and shows a slight increase in incidents and breaches this year. System Intrusion (including Ransomware) has overtaken Miscellaneous Errors as the top cause of breaches. The rise of Espionage as a motive for attackers in this sector is concerning. |

## Manufacturing

**(NAICS 31-33)**

| | |
|---|---|
| **Frequency** | 3,837 incidents, 1,607 with confirmed data disclosure |
| **Top patterns** | System Intrusion, Social Engineering and Basic Web Application Attacks represent 85% of breaches |
| **Threat actors** | External (86%), Internal (14%) (breaches) |
| **Actor motives** | Financial (87%), Espionage (20%) (breaches) |
| **Data compromised** | Internal (64%), Other (37%), Personal (33%), Credentials (22%) (breaches) |
| **What is the same?** | System Intrusion, Social Engineering and Basic Web Application Attacks are still the top three patterns, with the majority of attacks continuing to come from financially motivated External actors. |
| **Summary** | This year, 1 in 5 breaches were due to Espionage-motivated actors as compared to last year’s 3%. Internal (sensitive plans, reports, email) is, by far, the most commonly stolen data type. And more than 90% of breached organizations were SMBs with fewer than 1,000 employees. |

## Retail

**(NAICS 44-45)**

| | |
|---|---|
| **Frequency** | 837 incidents, 419 with confirmed data disclosure |
| **Top patterns** | System Intrusion, Social Engineering and Basic Web Application Attacks represent 93% of breaches |
| **Threat actors** | External (96%), Internal (3%), Partner (1%) (breaches) |
| **Actor motives** | Financial (100%), Espionage (9%) (breaches) |
| **Data compromised** | Internal (65%), Other (30%), Credentials (26%), Payment (12%) (breaches) |
| **What is the same?** | The top three patterns in this industry have not changed from last year—neither their membership nor their order. |
| **Summary** | The Retail industry has seen an increase in cyber incidents, though the focus has shifted from Payment card data to other data types that are easier to access. There was a notable rise in Espionage-motivated attacks as compared to last year. Defenders should be aware of more sophisticated and harder-to-detect threats. |

## Public Sector

**(NAICS 92)**

| | |
|---|---|
| **Frequency** | 1,422 incidents, 946 with confirmed data disclosure |
| **Top patterns** | System Intrusion, Miscellaneous Errors and Basic Web Application Attacks represent 78% of breaches |
| **Threat actors** | External (67%), Internal (33%), Partner (1%) (breaches) |
| **Actor motives** | Financial (76%), Espionage (29%), Ideology (2%) (breaches) |
| **Data compromised** | Personal (47%), Internal (44%), Other (41%),<br>Secrets (17%) (breaches) |
| **What is the same?** | This industry continues to be plagued by sophisticated attackers looking to gain access to the trove of data collected by governments about their constituents. Though the majority of breaches were from External actors, a significant number were from Internal actors making simple mistakes. |
| **Summary** | While we show a drop in reported incidents due to the makeup of contributors this year, the number of confirmed breaches remained steady. This means attackers are not easing up on government targets. Ransomware remains a major threat, hitting 30% of breaches across all levels of government. Errors remain a persistent issue, with Misdelivery in the lead. |

# At-a-glance industry facts

**While we do not have sufficient space, time or, in some cases, data to examine all industry verticals in depth, we have provided Table 1 below, which illustrates high-level information on the industries that we do not touch upon in greater detail.**

| Industry (NAICS) | Frequency | Top patterns | Threat actors | Actor motives | Data compromised |
|---|---|---|---|---|---|
| Agriculture (11) | 80 incidents, 55 with confirmed data disclosure | System Intrusion, Basic Web Application Attacks and Social Engineering represent 96% of breaches | External (96%), Internal (4%) (breaches) | Financial (98%), Espionage (33%), Ideology (2%) (breaches) | Internal (67%), Other (39%), Secrets (35%) (breaches) |
| Administrative (56) | 153 incidents, 145 with confirmed data disclosure | System Intrusion, Social Engineering and Miscellaneous Errors represent 97% of breaches | External (95%), Internal (3%), Partner (2%) (breaches) | Financial (100%) (breaches) | Internal (83%), Credentials (31%), Personal (10%), Other (8%) (breaches) |
| Construction (23) | 307 incidents, 252 with confirmed data disclosure | System Intrusion, Social Engineering and Basic Web Application Attacks represent 96% of breaches | External (97%), Internal (3%) (breaches) | Financial (77%), Espionage (23%) (breaches) | Internal (77%), Credentials (31%), Other (23%), Secrets (21%) (breaches) |
| Entertainment (71) | 493 incidents, 293 with confirmed data disclosure | System Intrusion, Social Engineering and Miscellaneous Errors represent 76% of breaches | External (71%), Internal (29%) (breaches) | Financial (97%), Espionage (18%), Ideology (3%), Fun (1%) (breaches) | Personal (58%), Other (39%), Internal (32%), Credentials (18%) (breaches) |
| Information (51) | 1,589 incidents, 784 with confirmed data disclosure | System Intrusion, Basic Web Application Attacks and Social Engineering represent 82% of breaches | External (83%), Internal (17%), Partner (1%) (breaches) | Financial (78%), Espionage (36%), Ideology (1%) (breaches) | Other (62%), Internal (51%), Personal (37%), Secrets (27%) (breaches) |

**Table 1.** At-a-glance table for victim industries without a section

| Industry (NAICS) | Frequency | Top patterns | Threat actors | Actor motives | Data compromised |
|---|---|---|---|---|---|
| Management (55) | 113 incidents, 107 with confirmed data disclosure | System Intrusion, Social Engineering and Privilege Misuse represent 99% of breaches | External (97%), Partner (2%), Internal (1%) (breaches) | Financial (99%), Espionage (1%) (breaches) | Internal (95%), Credentials (33%), Medical (1%), Personal (1%), System (1%) (breaches) |
| Mining (21) | 64 incidents, 52 with confirmed data disclosure | System Intrusion, Social Engineering and Basic Web Application Attacks represent 96% of breaches | External (98%), Internal (6%), Multiple (4%) (breaches) | Financial (100%), Espionage (3%), Grudge (3%) (breaches) | Internal (59%), Credentials (43%), System (20%), Other (18%) (breaches) |
| Other Services (81) | 683 incidents, 583 with confirmed data disclosure | System Intrusion, Social Engineering and Miscellaneous Errors represent 79% of breaches | External (68%), Internal (33%) (breaches) | Financial (69%), Espionage (31%) (breaches) | Personal (57%), Internal (48%), Other (44%), Secrets (18%) (breaches) |
| Professional (54) | 2,549 incidents, 1,147 with confirmed data disclosure | System Intrusion, Social Engineering and Basic Web Application Attacks represent 91% of breaches | External (93%), Internal (7%), Partner (1%) (breaches) | Financial (88%), Espionage (17%) (breaches) | Internal (70%), Other (25%), Credentials (24%), Personal (24%) (breaches) |
| Real Estate (53) | 339 incidents, 320 with confirmed data disclosure | System Intrusion, Social Engineering and Miscellaneous Errors represent 84% of breaches | External (64%), Internal (36%) (breaches) | Financial (100%) (breaches) | Personal (70%), Internal (40%), Other (27%), Bank (17%) (breaches) |
| Transportation (48–49) | 361 incidents, 248 with confirmed data disclosure | System Intrusion, Basic Web Application Attacks and Social Engineering represent 91% of breaches | External (94%), Internal (7%), Multiple (2%), Partner (1%) (breaches) | Financial (98%), Espionage (16%), Ideology (1%) (breaches) | Internal (67%), Other (25%), Credentials (22%), Personal (20%) (breaches) |
| Utilities (22) | 358 incidents, 213 with confirmed data disclosure | System Intrusion, Social Engineering and Basic Web Application Attacks represent 92% of breaches | External (92%), Internal (8%), Multiple (1%) (breaches) | Financial (70%), Espionage (66%), Grudge (1%) (breaches) | Internal (80%), Secrets (61%), Other (42%) (breaches) |
| Wholesale Trade (42) | 330 incidents, 319 with confirmed data disclosure | System Intrusion, Social Engineering and Privilege Misuse represent 98% of breaches | External (97%), Internal (3%) (breaches) | Financial (100%) (breaches) | Internal (93%), Credentials (24%), Other (3%), Personal (3%), System (3%) (breaches) |

**Table 1.** At-a-glance table for victim industries without a section (continued)

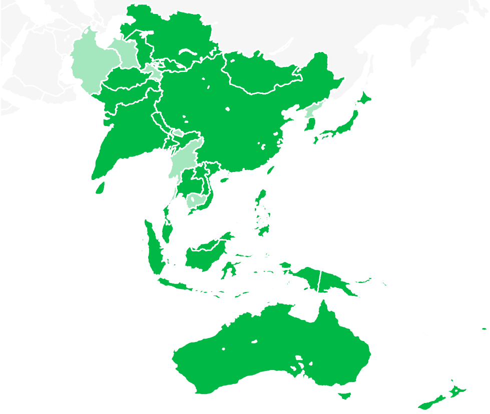
# Regional findings

**We are often asked how cybercrime differs (or doesn't) when viewed from one region of the world to another. In this section, we are excited to again examine cybercrime from a macro-regional perspective. Our visibility into any given area is influenced by regional disclosure laws, our own dataset and where our data contributors conduct business, to name only a few. We hope that you find this global perspective helpful and informative.**

**If you would like to help feature your area among these pages, please contact us about becoming a data contributor and encourage your partners and clients to do the same.**

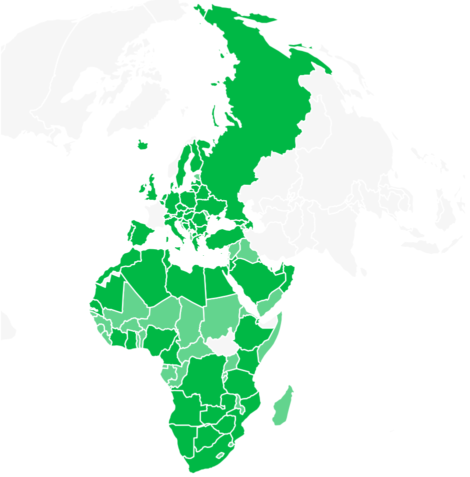
🟩 Regions with records   ▩ Regions without records

## Asia and the Pacific (APAC)



| | |
|---|---|
| **Frequency** | 2,687 incidents, 1,374 with confirmed data disclosure |
| **Top patterns** | System Intrusion, Social Engineering and Basic Web Application Attacks represent 97% of breaches |
| **Threat actors** | External (99%), Internal (1%) (breaches) |
| **Actor motives** | Financial (83%), Espionage (34%) (breaches) |
| **Data compromised** | Internal (78%), Other (41%), Secrets (33%) (breaches) |

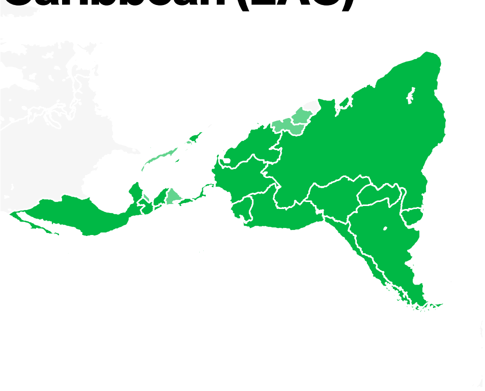
## Europe, Middle East and Africa (EMEA)



| | |
|---|---|
| **Frequency** | 9,062 incidents, 5,321 with confirmed data disclosure |
| **Top patterns** | System Intrusion, Social Engineering and Miscellaneous Errors represent 89% of breaches |
| **Threat actors** | External (71%), Internal (29%) (breaches) |
| **Actor motives** | Financial (87%), Espionage (18%) (breaches) |
| **Data compromised** | Internal (62%), Personal (49%), Other (37%), Secrets (13%) (breaches) |

🟩 Regions with records ▨ Regions without records

## Latin America and Caribbean (LAC)



| | |
|---|---|
| **Frequency** | 657 incidents, 413 with confirmed data disclosure |
| **Top patterns** | System Intrusion, Social Engineering and Basic Web Application Attacks represent 99% of breaches |
| **Threat actors** | External (100%), Partner (1%), Multiple (1%) (breaches) |
| **Actor motives** | Financial (84%), Espionage (27%) (breaches) |
| **Data compromised** | Internal (97%), Secrets (27%), Other (24%) (breaches) |

## Northern America (NA)

| | |
|---|---|
| **Frequency** | 6,361 incidents, 2,867 with confirmed data disclosure |
| **Top patterns** | System Intrusion, Everything Else and Social Engineering represent 90% of breaches |
| **Threat actors** | External (91%), Internal (5%), Partner (5%), Multiple (1%) (breaches) |
| **Actor motives** | Financial (95%), Espionage (9%) (breaches) |
| **Data compromised** | Internal (49%), Medical (35%), Credentials (23%), Other (17%) (breaches) |

# Stay informed and threat ready.

**Facing today's threats requires intelligence from a source you can trust.**

**The full DBIR contains details on the actors, actions and patterns that can help you prepare your defenses and educate your organization. Get the intelligence you need to help protect your organization.**

**Read the full 2025 DBIR at verizon.com/dbir.**

## Want to make the world of cybersecurity a safer place?

If your organization aggregates incident or security data and is interested in becoming a contributor to the annual Verizon DBIR (and we hope you are), the process is very easy and straightforward. Please email us at dbircontributor@verizon.com.

Please feel free to provide us feedback for improving the DBIR at dbir@verizon.com, reach out to Verizon Business (or one of the authors) on LinkedIn and check out the VERIS GitHub page: https://github.com/vz-risk/veris.