

2025 Data Breach Investigations Report

The authoritative source of cybersecurity
breach information

Neal Maguire
Principal Consultant
Verizon Threat Research Advisory Center



A comprehensive look at data breaches

18

years of the Data Breach
Investigations Report

22,052

incidents reviewed in our
2025 report

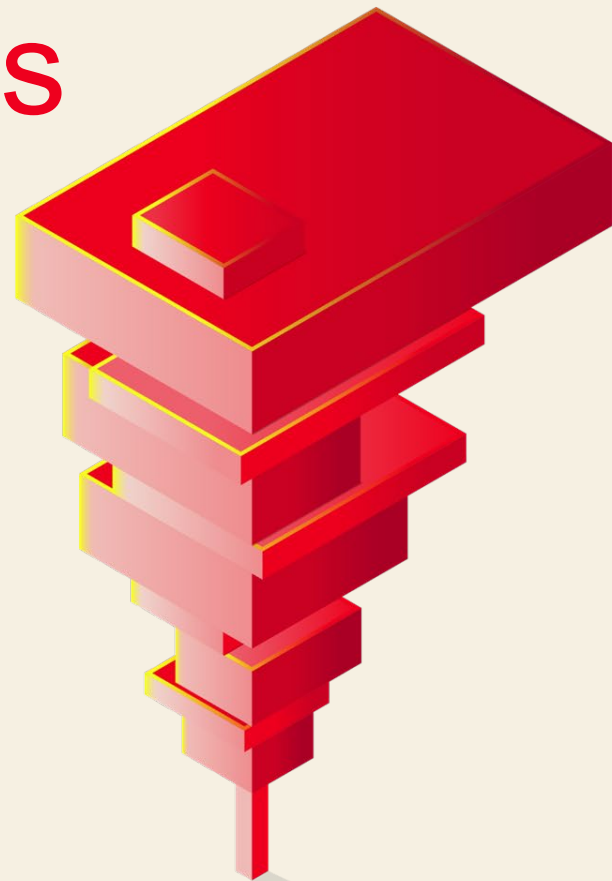
139

victim countries identified

12,195

data breaches analyzed in our
2025 report

Summary of findings



Learn the hackers' playbook

Our 2025 Data Breach Investigations Report decoded more than 12,000 data breaches. Here's a snapshot of some of our most critical findings.

Stack your cybersecurity knowledge.

34%



Exploitation of vulnerabilities as an initial access step for a data breach grew by 34%, now accounting for 20% of breaches.

54%

Only about 54% of perimeter device vulnerabilities were fully remediated, and it took a median of 32 days to do so.

60%

Human involvement in security breaches remained about the same as last year —60%.

15%

15% of employees routinely accessed generative AI platforms on their corporate devices —increasing the potential risk for data leaks.



Are you vendor vulnerable?

The percentage of breaches where a third party was involved doubled in the past year, from 15% to 30%.

Developing a unified cybersecurity posture with partners can help reduce vulnerability.

Ransomware is on the rise.

44% of cybersecurity breaches involved ransomware, up 37% from last year.

But ransom payments are down.

The median amount paid to ransomware groups was \$115,000, down from \$150,000 in last year's report. However, our 2025 report shows that most victim organizations—64%—did not pay the ransoms.

Initial access vectors: perimeter device vulnerabilities in 2022

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 (22%), 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 perimeter devices and virtual private networks (VPNs).

Organizations worked very hard to patch those perimeter 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.

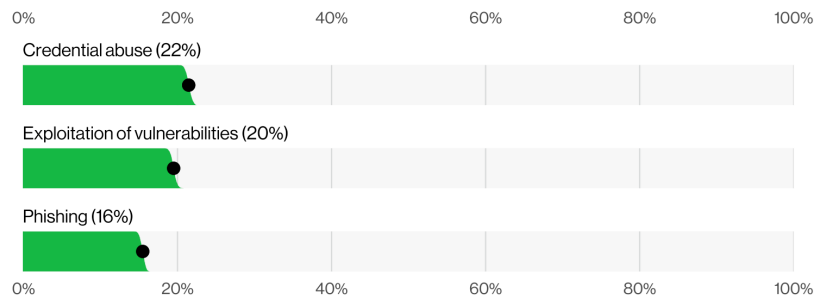


Figure 1. Known initial access vectors in non-Error, non-Misuse breaches (n=9,891)

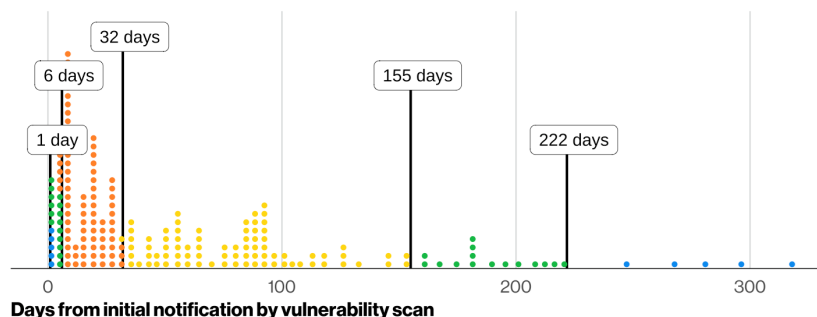


Figure 2. Distribution of the median of days until full remediation of vulnerabilities in our perimeter device subset in a single company (n=431 – each dot is 2.15 unique companies)

Ransomware continues to grow ...

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%.

Ransomware is also disproportionately affecting small organizations. In larger organizations, Ransomware is a component of 39% of breaches, while small- and medium -sized businesses (SMBs) experienced Ransomware -related breaches to the tune of 88% overall.

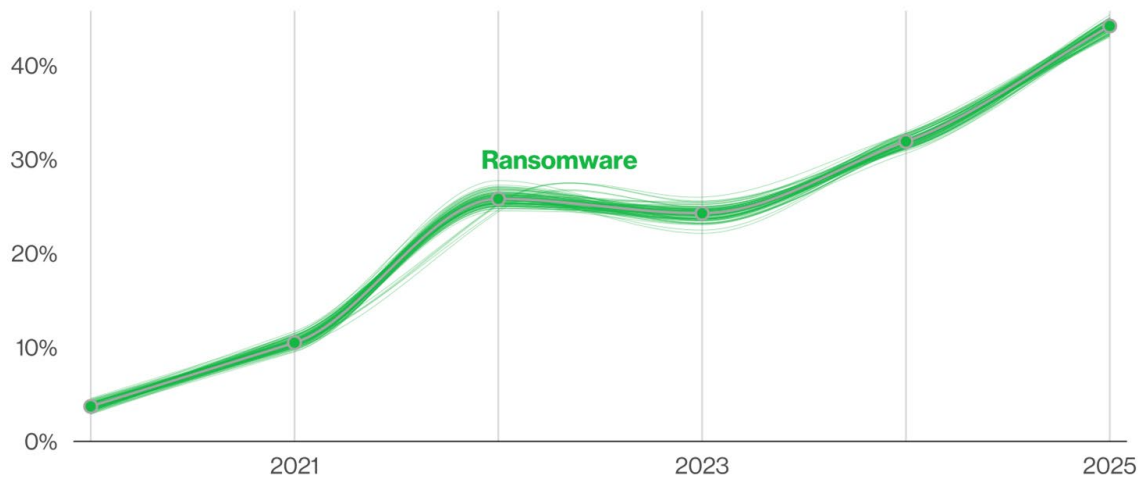


Figure 3. Ransomware action over time in breaches (n for 2025 dataset=10,747)

... but outcomes have changed

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.

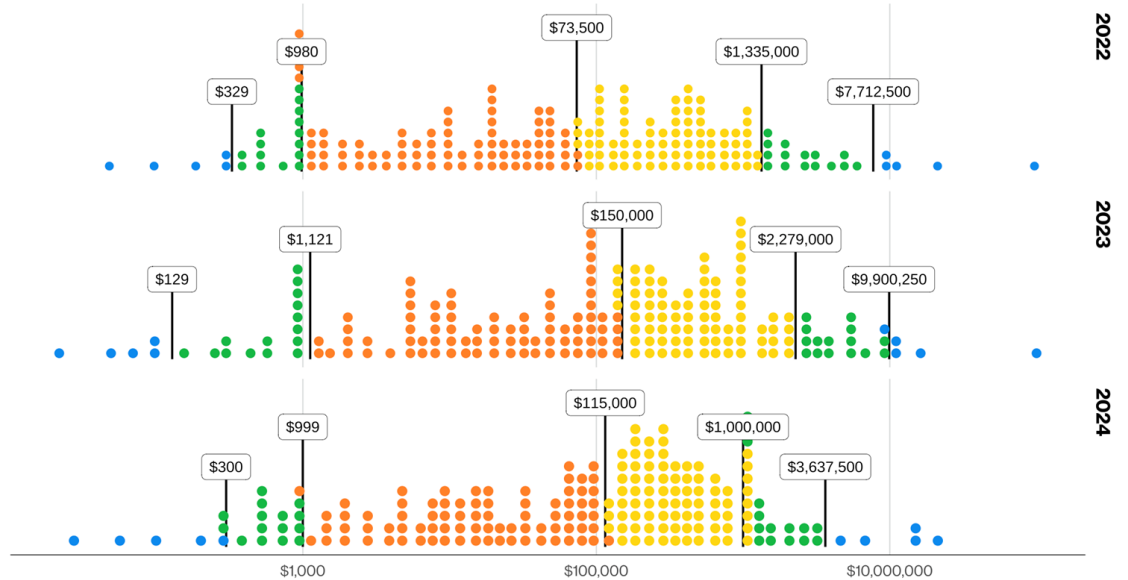


Figure 4. Distribution of loss due to ransom payment in USD (2022–2024)
(n for 2022=664 – each dot is 3.32 events)
(n for 2023=462 – each dot is 2.31 events)
(n for 2024=351 – each dot is 1.75 events)

Third party, thirty percent, targeted passwords

Although the involvement of the human element in breaches remained roughly the same as last year, hovering around 60%, the percentage 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%. Also, approximately 28% of incidents involving state -sponsored actors had a Financial motive.

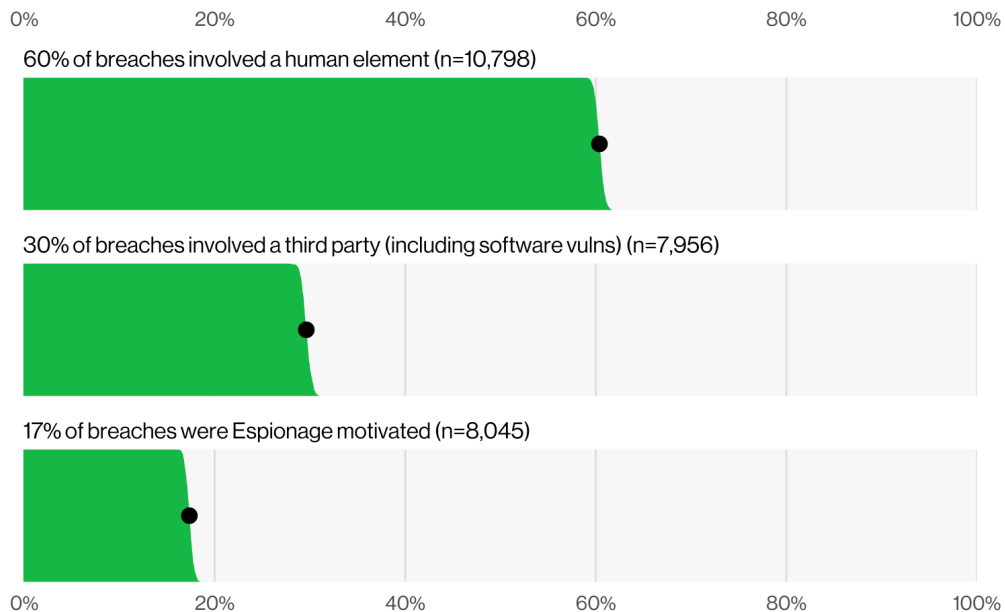


Figure 5. Select key enumerations in breaches

Assume access, ready defenses

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.

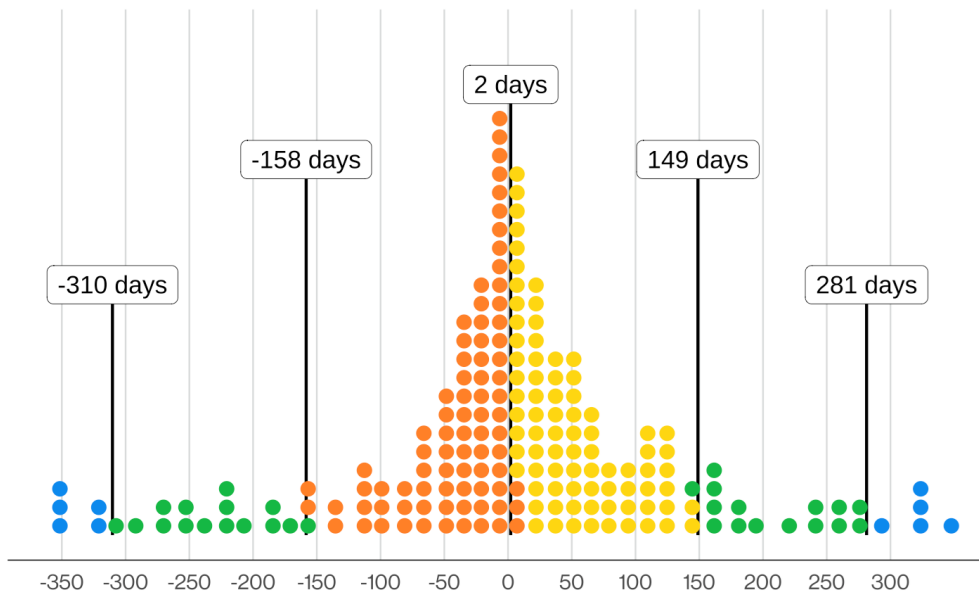


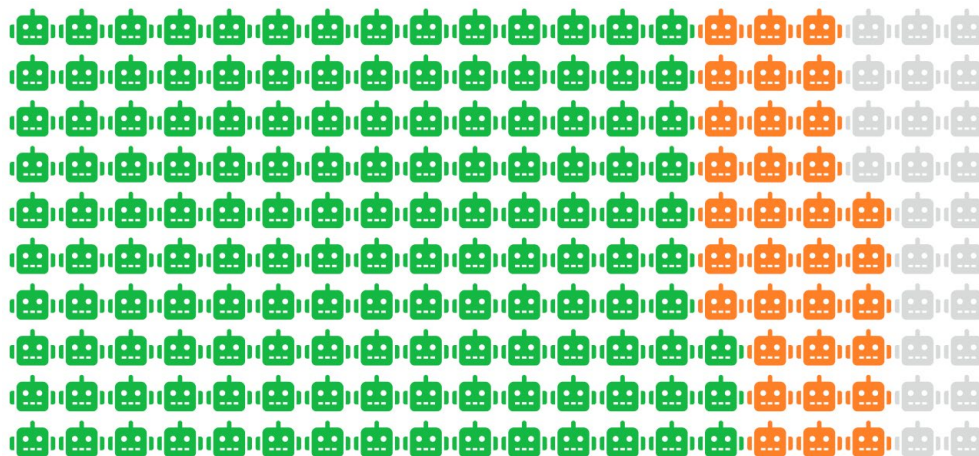
Figure 7. Distribution of difference in days between ransomware posting and infostealer log discovery (n=503 – each dot is 2.52 ransomware victims)

Novel technology, banal threats

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.

There 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).

A large number of those employees 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 that the use was outside of corporate policy.



GenAI account credentials

Personal

Corporate, not integrated

Corporate, integrated

Figure 8. Percentage breakdown of GenAI service access account types (each glyph is 0.5%)

Phishing practice reported beneficial

When we examined the reporting rate of phishing emails, we found that users who had recent training reported simulated phishing emails at a significantly higher rate —about 21% against a base rate of 5%, a four times relative increase.

But there is still work to be done. Those same users only had a slight incremental improvement (only 5% relative impact) on median click rate. And users overall will, in the median case, still click on 1.5% of simulated phishing exercises, even after participating in training sessions.

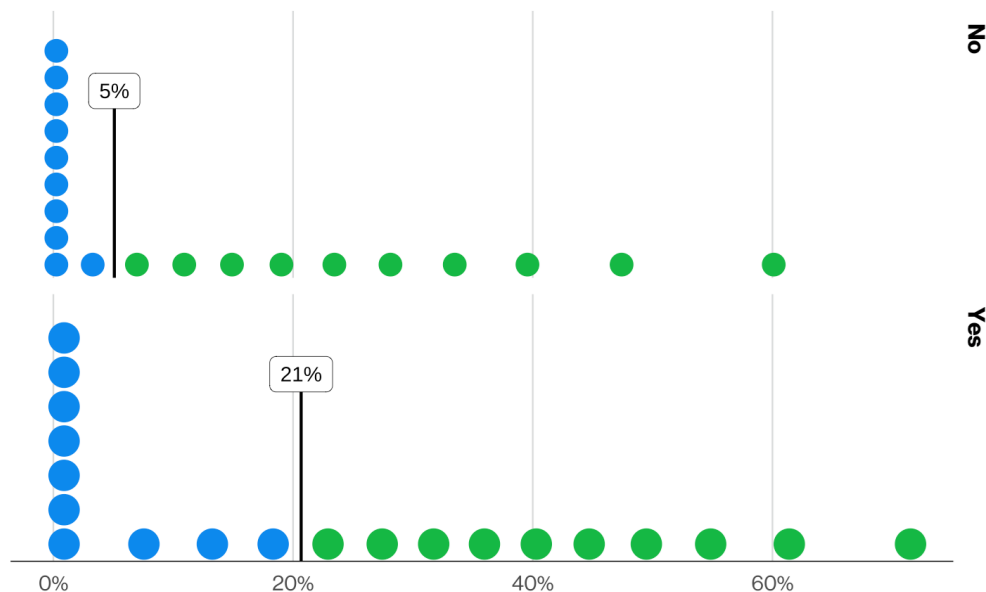


Figure 9. Distribution of phishing simulation campaign report rates by organization recent training status
(n for No=68,492 – each dot is 3,424.60 campaigns)
(n for Yes=36,325 – each dot is 1,816.25 campaigns)

Let's not dwell in the past

Given one of the best sources of information on ransomware breaches right now is when the actors themselves post on their dark web portals, the Actor disclosure variety corresponds to 96% of all our discovery methods.

In non-actor -disclosed breaches, Infrastructure monitoring (18%) and Reported by employee (14%) are the most common discovery methods.

The median dwell time in non -Actor -disclosed breaches has improved a little from the last couple of years, being 24 days in our 2025 dataset as opposed to 30 days in the 2023 report.

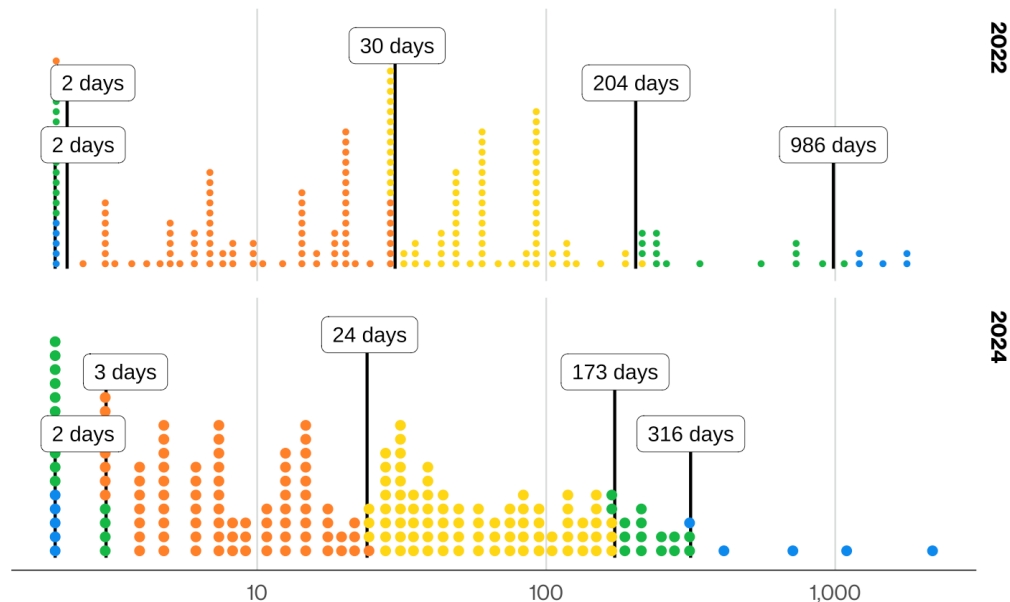
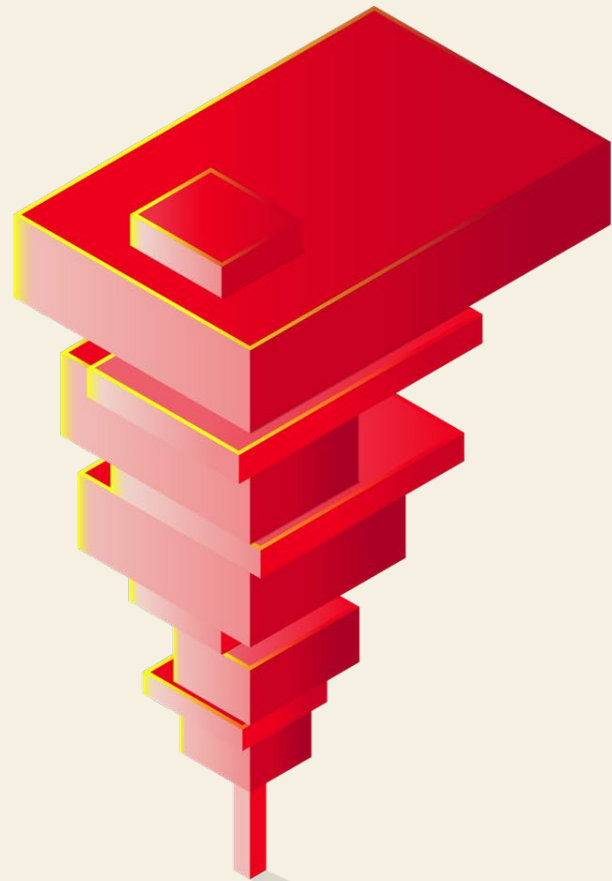


Figure 10. Distribution of dwell time in days in non -Actor -disclosed breaches per year (n for 2022=93 – each dot is 0.46 breaches) (n for 2024=248 – each dot is 1.243 breaches)

Incident patterns review



Breach patterns

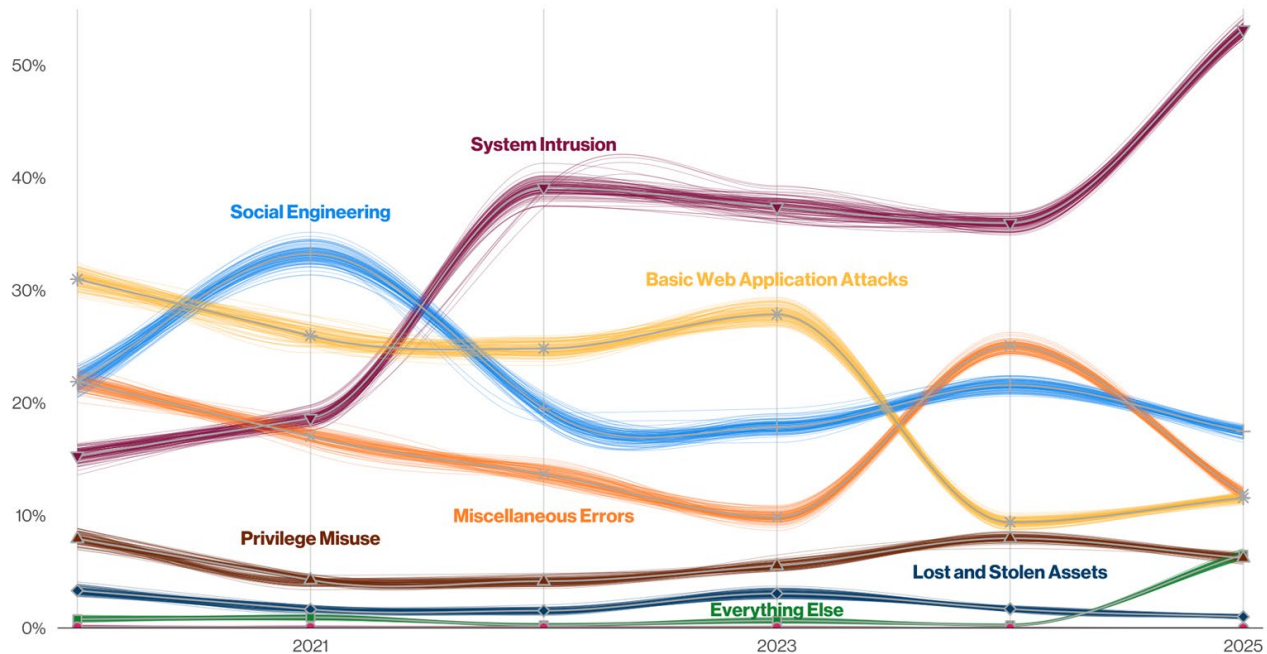


Figure 11. Patterns over time in breaches (n for 2025 dataset=12,195)

System Intrusion

This pattern continues to be largely driven by Ransomware, which is present in 75% of the breaches.

Analyzing the initial access vectors in the Ransomware breaches, we see that exploitation of vulnerabilities is the most common vector, overtaking credential abuse for a couple of years now.

We have not seen this result in the larger dataset (where credential abuse is still the most common one), but this shouldn't be surprising given how much the ransomware operators have been leveraging vulnerabilities on file server software (2023) and perimeter devices (2024).

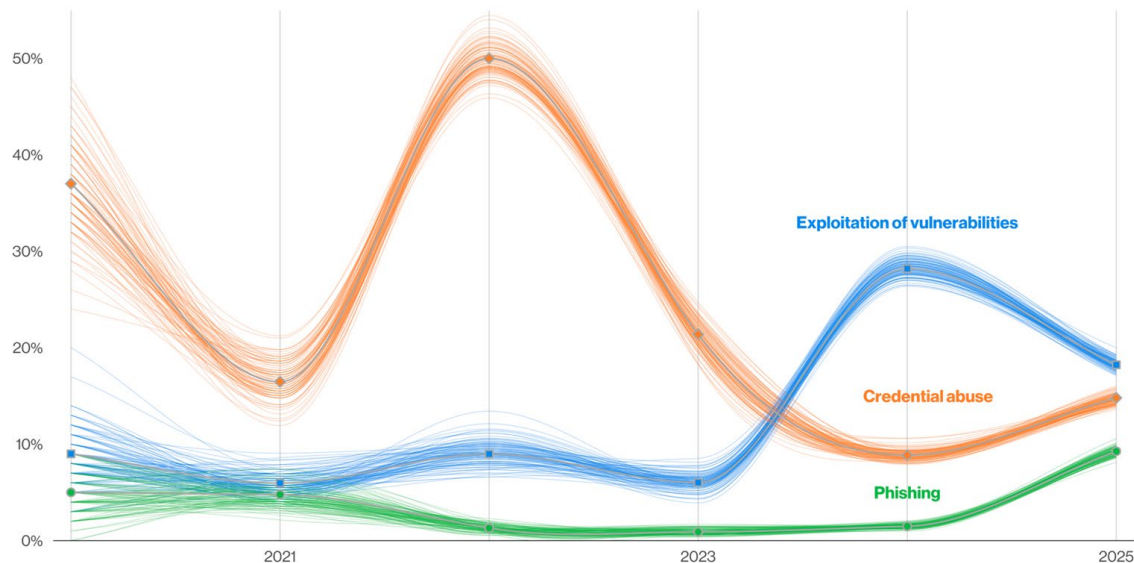


Figure 12. Known initial access vectors over time in Ransomware action breaches (n in 2025 dataset=4,630)

Social Engineering

Social actions in Social Engineering incidents are led by Phishing and Pretexting, unsurprisingly.

Prompt bombing is of special interest, in which users are bombarded with multifactor authentication (MFA) login requests, showing up in 14% of incidents.

Other types of techniques used to bypass MFA, such as Adversary -in-the-Middle (AiTM), Password dumping and Hijacking (like SIM swapping), only show up in 4% of the entire breach dataset for this year's report.

In 2024 alone, according to the FBI Internet Crime Complaint Center (IC3), more than \$6.3 billion was transferred as part of Business Email Compromise (BEC) scams. The median amount of money extracted from victims has settled around the \$50,000 mark.

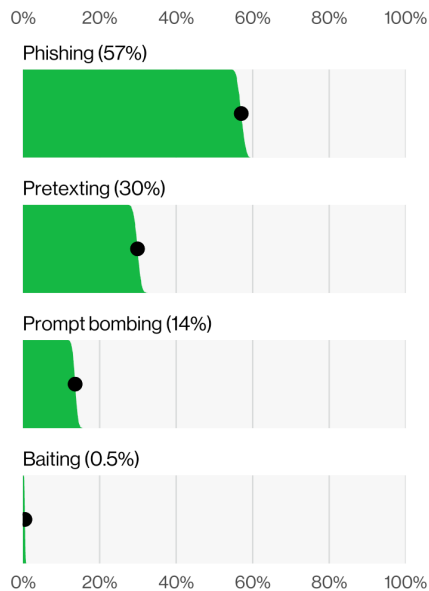


Figure 13. Top select Social action varieties in Social Engineering incidents (n=3,208)

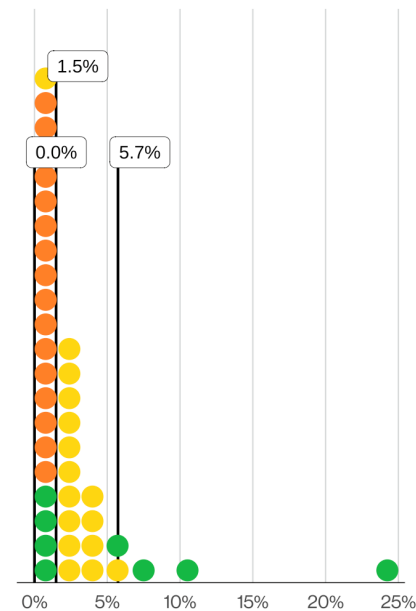


Figure 14. Distribution of phishing simulation campaign click rate by organization (n=7,743 – each dot is 193.58 organizations)

Basic Web Application Attacks

In this pattern, about 88% of the breaches involve the Use of stolen credentials, which sometimes serves as both the first and only action, while other times, it is just one piece of a larger attack chain.

You also have to contend with brute forcing (“guessed credentials”) along with the establishment of Backdoors or C2s (command and controls).

For the last couple of years, Espionage has hovered around 10% to 20% of the Basic Web Application Attacks breaches, but this year it accounts for an eye-opening 62%.

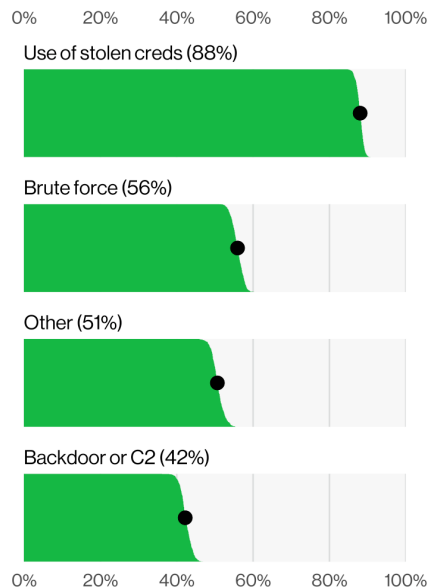


Figure 15. Top Action varieties in Basic Web Application Attacks breaches (n=1,021)

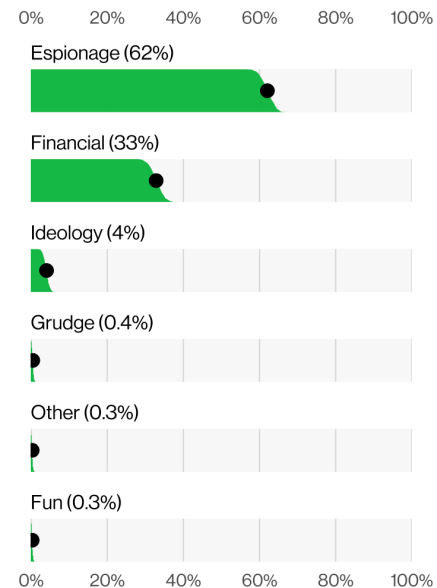


Figure 16. Top Actor motives in Basic Web Application Attacks breaches (n=688)

Miscellaneous Errors

The top three action varieties were Misdelivery, Misconfiguration and Publishing error, which was a change from last year's top three.

The data types we see affected by Miscellaneous Errors breaches are primarily of the Personal variety.

And while this Personal information includes data points such as date of birth, mailing address and other tidbits useful for identity theft, we are also seeing some of the more sensitive varieties showing up to a lesser degree.

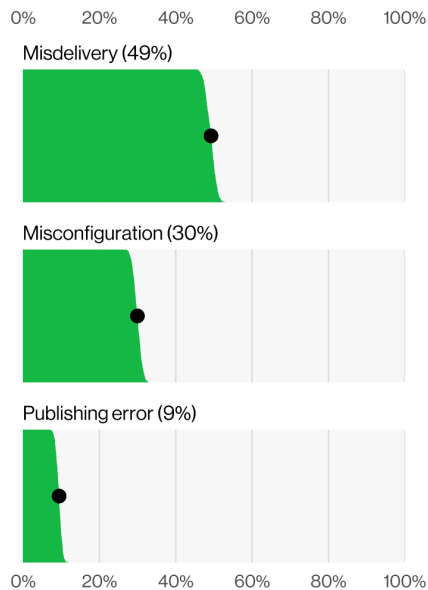


Figure 17. Top Action varieties in Miscellaneous Errors breaches (n=1,399)

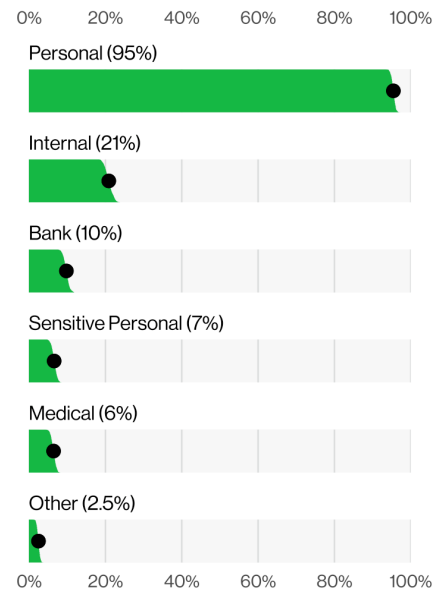
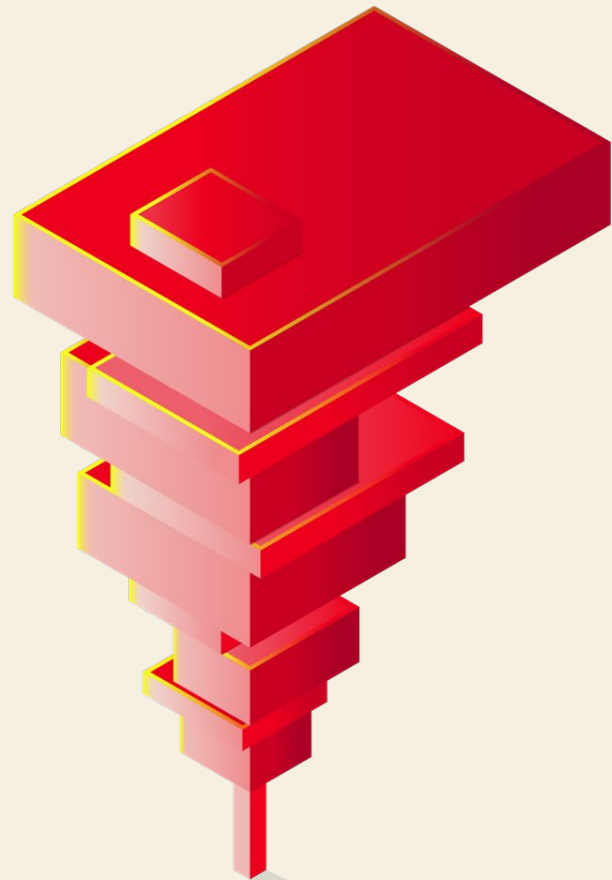


Figure 18. Top Data varieties in Miscellaneous Errors breaches (n=1,341)

Industry tailored insights



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?

The Financial and Insurance vertical is still dominated by financially motivated threat actors who will take any data type they can lay their hands on. However, attacks with the motive of Espionage have increased this year.

Ransomware and Use of stolen credentials (both present in 30% of breaches) are the most common action varieties in breaches in this sector. However, attacks with the motive of Espionage have increased to 12% this year from 5% last year.

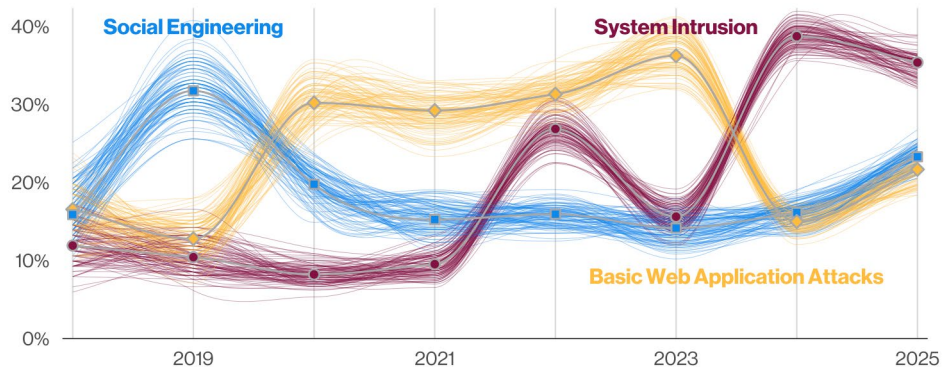


Figure 24. Top patterns over time in Financial and Insurance breaches

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.

Healthcare 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. Espionage-motivated attacks jumped from just 1% in last year's report to 16% this year.

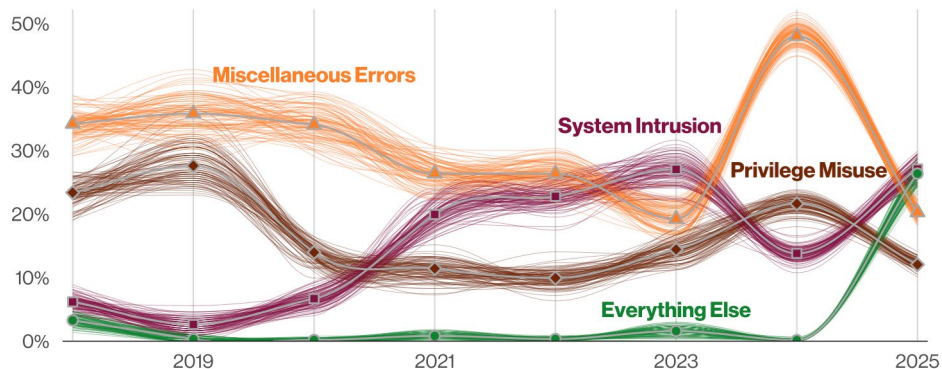


Figure 25. Top patterns over time in Healthcare breaches

Manufacturing (NAICS 333)

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.

20% of breaches were due to Espionage -motivated actors as compared to last year's 3%.

Malware action in Manufacturing breaches has risen to 66% this year, with 71% of this malware representing Ransomware.

More than 90% of breached organizations were SMBs with fewer than 1,000 employees.

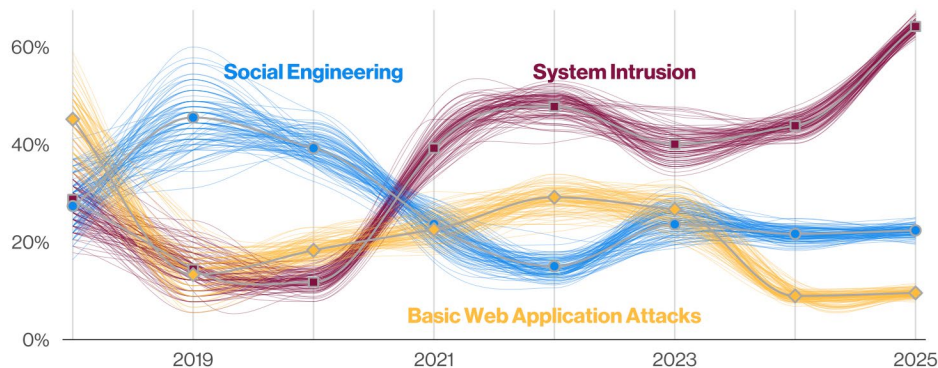
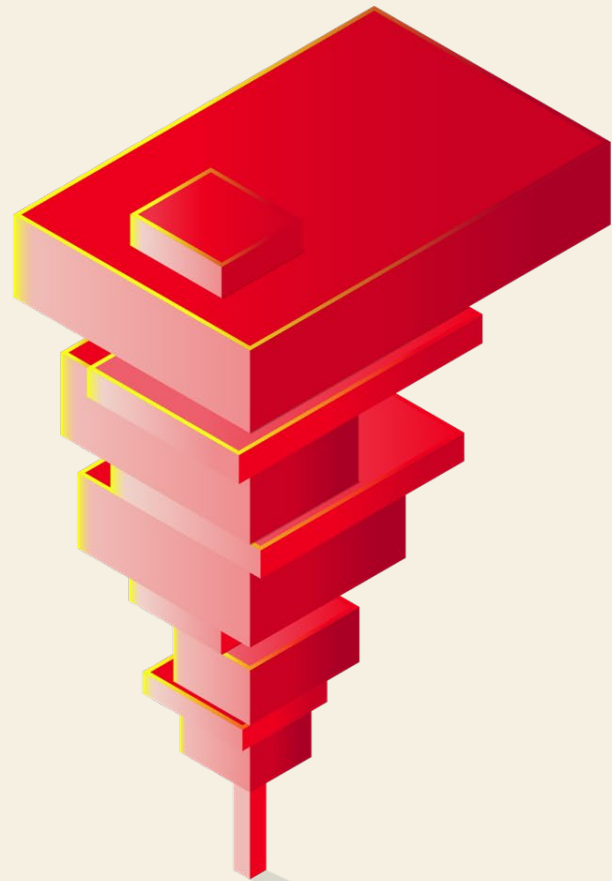


Figure 26. Top patterns over time in Manufacturing breaches

Focused analysis SMB



SMB analysis

Ransomware groups don't seem to care what size an organization is; they appear to be quite happy to breach smaller organizations and adjust their ransom demands when needed.

While Errors account for almost one in five (18%) breaches in large organizations, they are merely a footnote for SMBs at 1%.

Social attacks, on the other hand, account for roughly similar percentages for SMBs (18%) and large organizations (13%) and are almost exclusively of the Phishing variety. However, Pretexting attacks are more common in SMBs than in large organizations.

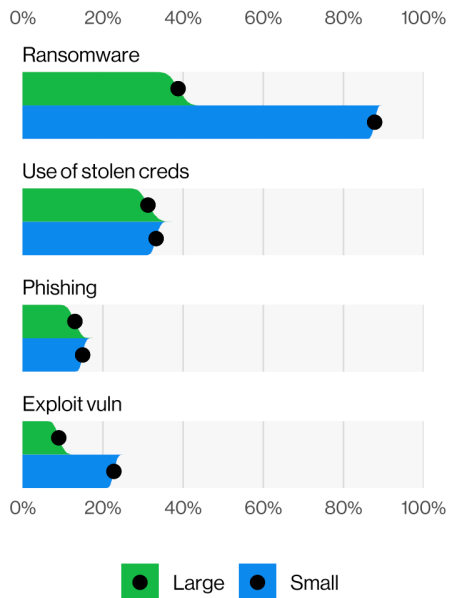


Figure 28. Top Action varieties by victim organization size (n=645)

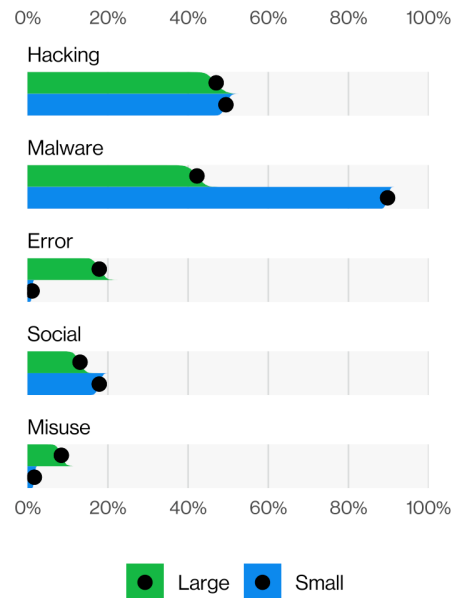
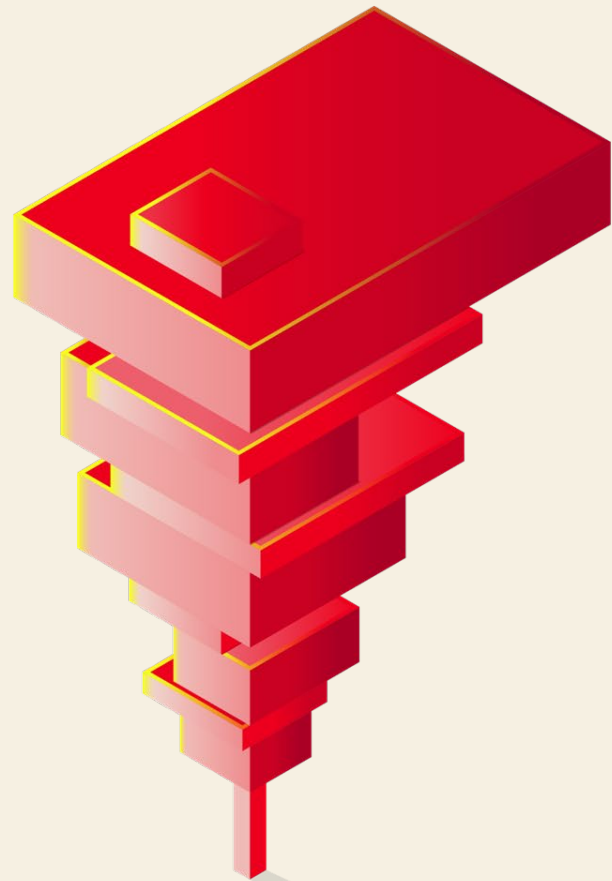


Figure 29. Top Actions by victim organization size (n=751)

Regional insights



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)
What is the same?	The top three patterns remain the same this year as last year in the EMEA threat landscape.

System Intrusion increased from 27% of breaches last year to 53% of breaches this year.

Social Engineering is the second most common incident pattern, with Phishing showing up in 19% of all EMEA breaches.

Internal actors are reasonably well represented (29%) in EMEA. These insiders are mostly composed of employees committing unintentional mistakes (19%), such as Misdelivery, but there was a small number of misuse cases (8%), as well.

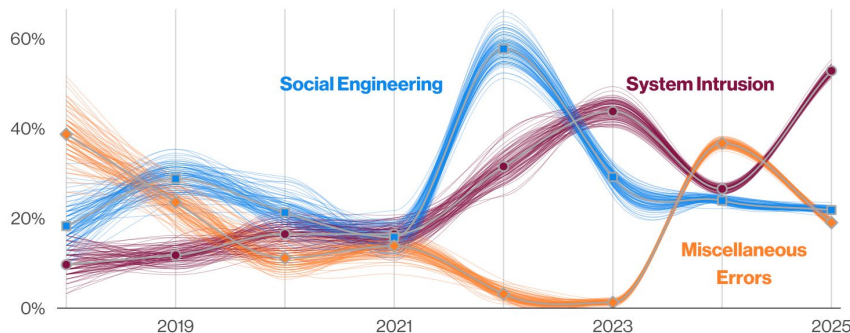


Figure 36. Top patterns over time in EMEA breaches

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)
What is the same?	The System Intrusion pattern continues to be predominant in the APAC threat landscape.

System Intrusion rose to 83% of all breaches from an already impressive 39% in last year's report.

Social Engineering had reached a peak in the 2021 Data Breach Investigations Report, but it has been slowly declining percentage-wise ever since. It now accounts for 20% of breaches in APAC.

Malware increased from 58% last year to 83% this year, with Ransomware accounting for 51% of the total breaches in this region.

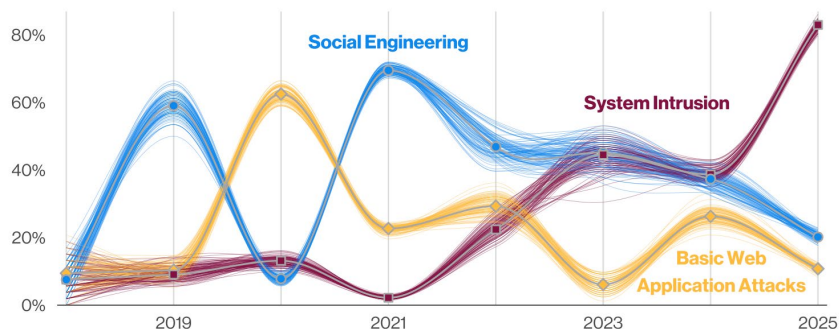


Figure 35. Top patterns over time in APAC breaches

Questions?

DBIR: [verizon.com/dbir](https://www.verizon.com/dbir)
Email: [dbir@verizon.com](mailto:dbircontributor@verizon.com)

If you are 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.

verizon
business