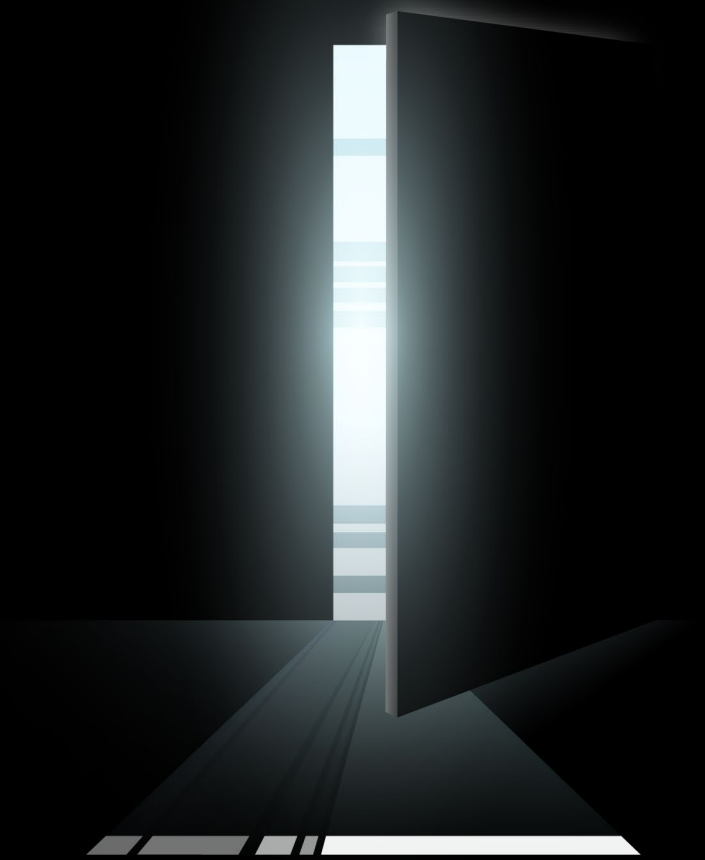
2024 Data Breach Investigations Report

The authoritative source of cybersecurity breach information

Summary of findings



A comprehensive look at data security patterns

17
years

94
countries

30,458
incidents reviewed in our 2024 report

10,626
data breaches analyzed in our 2024 report

Learn how they're getting in.

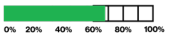
Our 2024 Data Breach Investigations Report analyzed a record high number of breaches. Here's what we learned.

Pathways to breaches

180%

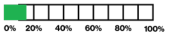
Exploitation of vulnerabilities as an initial access step for a breach grew by 180% over last year.

68%



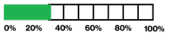
68% of all breaches involved a non-malicious human element.

15%



15% of breaches involved third parties, including data custodians or hosting partner infrastructures.

31%



31% of all breaches over the past 10 years have involved the Use of stolen credentials.

What it costs

$46,000 was the median loss associated with financially motivated incidents involving Ransomware or Extortion of some kind.[1]

$50,000 was the median loss attributed to Business Email Compromise in 2022 and 2023.[1]

Falling for scams is fast.

The median time for users to fall for phishing emails is < 60 seconds.

Response is slow.

It takes around 55 days for organizations to remediate 50% of critical vulnerabilities after patches are available.

1. According to the FBI's Internet Crime Complaint Center (IC3) ransomware complaint data.

Ways in: Vulnerability growth in 2023

External actors leveraged a variety of techniques to gain entry to an organization, which we describe in our “ways-in” analysis.

The exploitation of vulnerabilities as the initial access step for a breach has almost tripled (180% growth) since last year. MOVEit and other zero-day exploits that were used by ransomware actors contributed.

Exploit vuln is now accountable for 14% of breaches. Credentials accounted for 38% and Phishing for 15%. Web applications was the most common vector of entry, followed by Email.

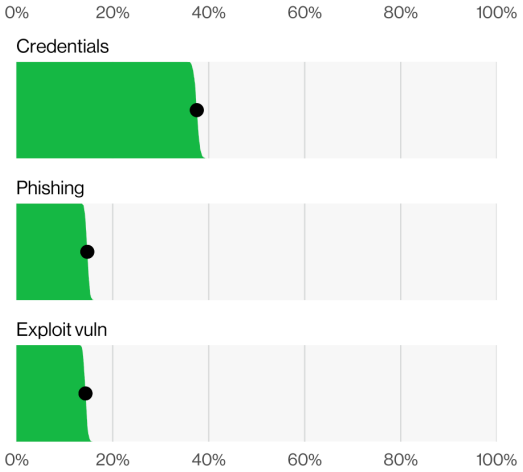


Figure 1. Select ways-in enumerations in non-Error, non-Misuse breaches (n=6,963)

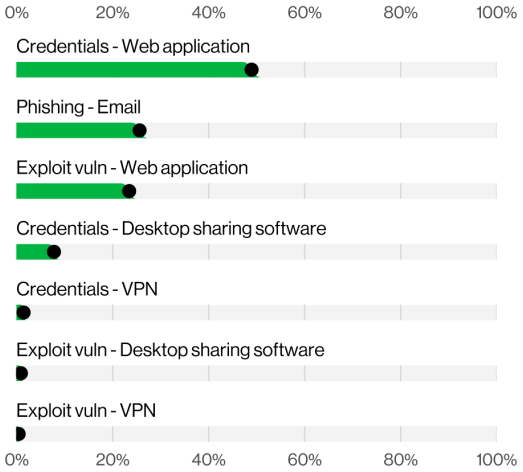


Figure 2. Select ways-in variety and vector enumerations in non-Error, non-Misuse breaches (n=2,770)

Exploitation of vulnerabilities paints an unsustainable picture.

Even when considering only the Cybersecurity Infrastructure and Security Agency (CISA) Known Exploited Vulnerabilities (KEV) catalog, it takes organizations around 55 days to remediate 50% of those critical vulnerabilities after their patches are available.

On the flip side, the median time for detecting the first scan for a CISA KEV vulnerability is five days from publication in the Common Vulnerabilities and Exposures (CVE) database (not from the patch being available).

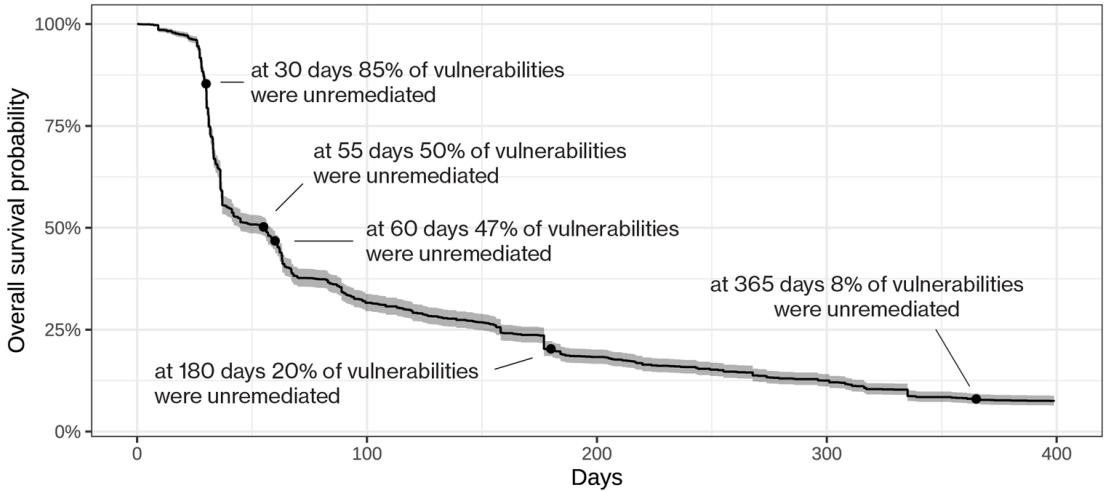


Figure 3. Survival analysis of CISA KEV vulnerability remediation data

Credential abuse and phishing continue strong.

Over the past 10 years, the Use of stolen credentials has appeared in almost one-third (31%) of all breaches, and a good part of those stolen credentials can be clearly attributed to Phishing.

Reviewing phishing simulation data, the median time for users to fall for phishing emails is less than 60 seconds.

On the flip side, reporting practices have been going up steadily, with 20% of users identifying and reporting phishing in simulation engagements and 11% of the users who did click the email also reporting it.

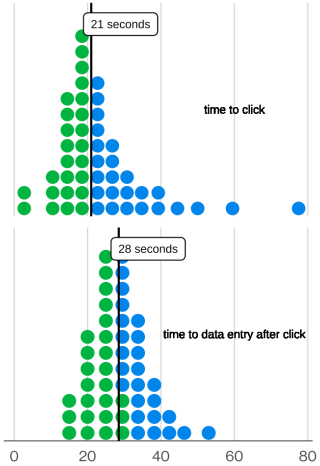


Figure 4. Distribution of time between email opening, clicking and data entry in phishing simulations (n=24,456)

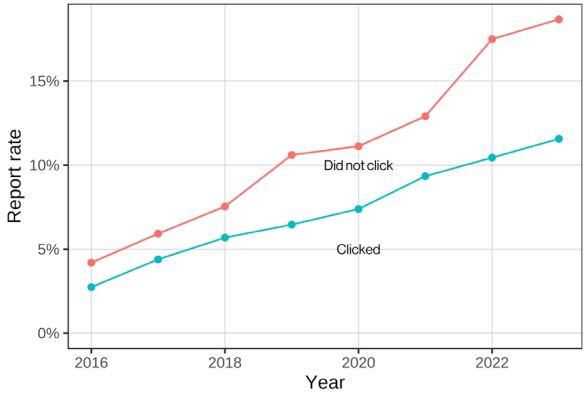


Figure 5. Phishing email report rate by click status

Top data-driven and custom metric-related findings

More than two-thirds (68%) of breaches involved a non-malicious human element. These breaches were caused by a person who either fell victim to a Social Engineering attack or made some type of Error.

15% of breaches involved a third party, including data custodians or hosting partner infrastructures being breached, and direct or indirect software supply chain issues.

Our dataset saw a growth of breaches involving Errors, now at 28%, as we broadened our contributor base to include several new mandatory breach notification entities.

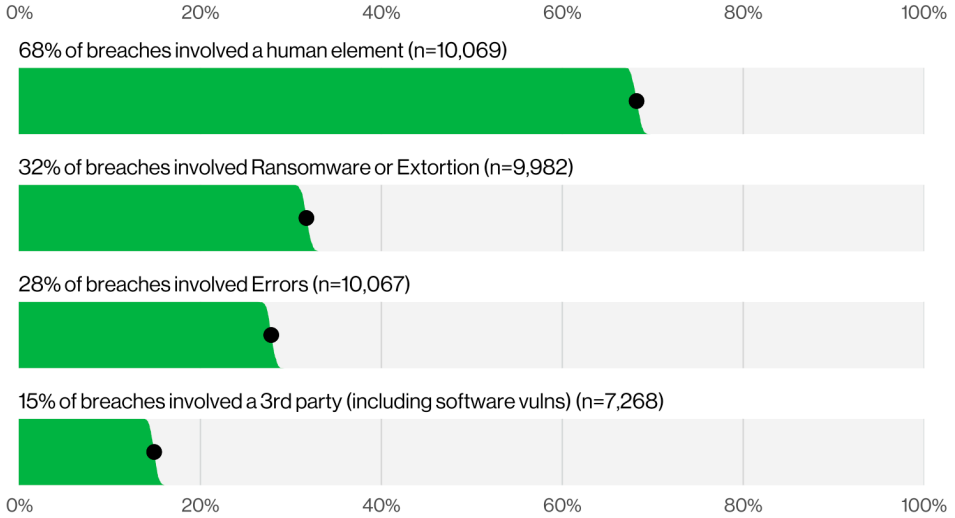


Figure 6. Select key enumerations in breaches

Ransomware and friends

Roughly one-third of all breaches involved Ransomware or some other Extortion technique. Pure Extortion attacks have risen over the past year
and are now a component of 9% of
all breaches.

The shift of traditional ransomware actors toward these newer techniques resulted in a bit of a decline in Ransomware to 23%.

However, when combined, given that they share threat actors, they represent a strong growth to 32% of breaches. Ransomware was a top threat across 92% of industries.

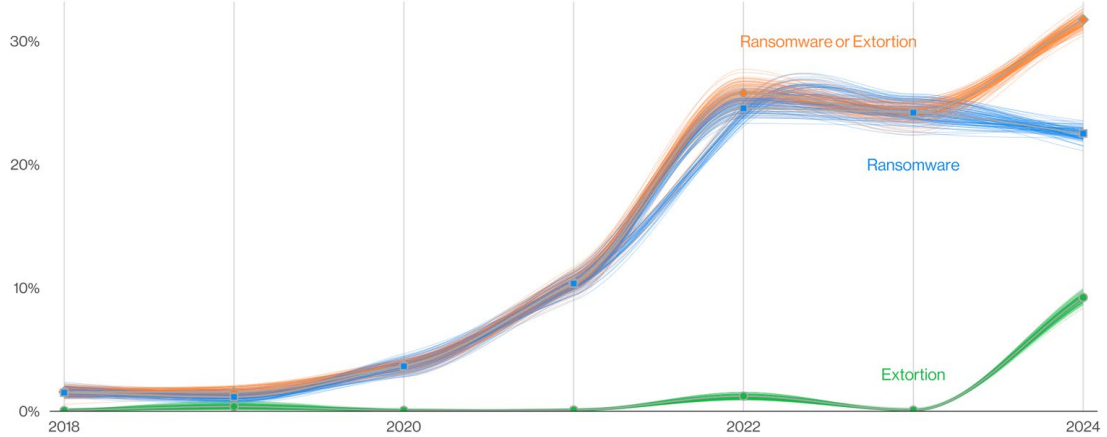


Figure 7. Ransomware and Extortion breaches over time

(Not) working hard for the money

Financially motivated threat actors will typically stick to the attack techniques that will give them the most return on investment.

Over the past three years, the combination of Ransomware and other Extortion breaches accounted for almost two-thirds (between 59% and 66%) of those attacks. The median loss in ransomware cases has been $46,000.[1]

Over the past two years, we have seen incidents involving Pretexting (the majority of which had Business Email Compromise [BEC] as the outcome) accounting for one-fourth (between 24% and 25%) of financially motivated attacks. In both years, the median transaction amount of a BEC was around $50,000.

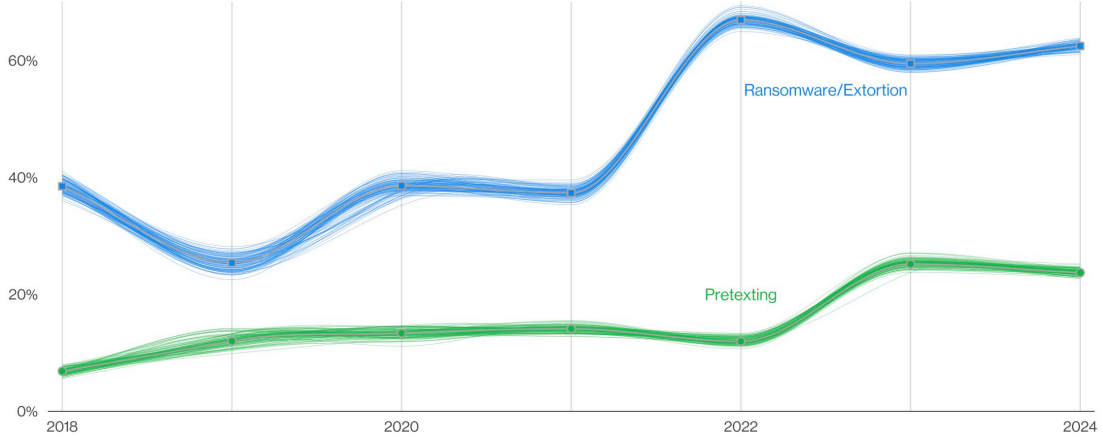


Figure 8. Select action varieties in Financial motive over time

1. According to the FBI's Internet Crime Complaint Center ransomware complaint data.

Incident patterns review

Breach patterns

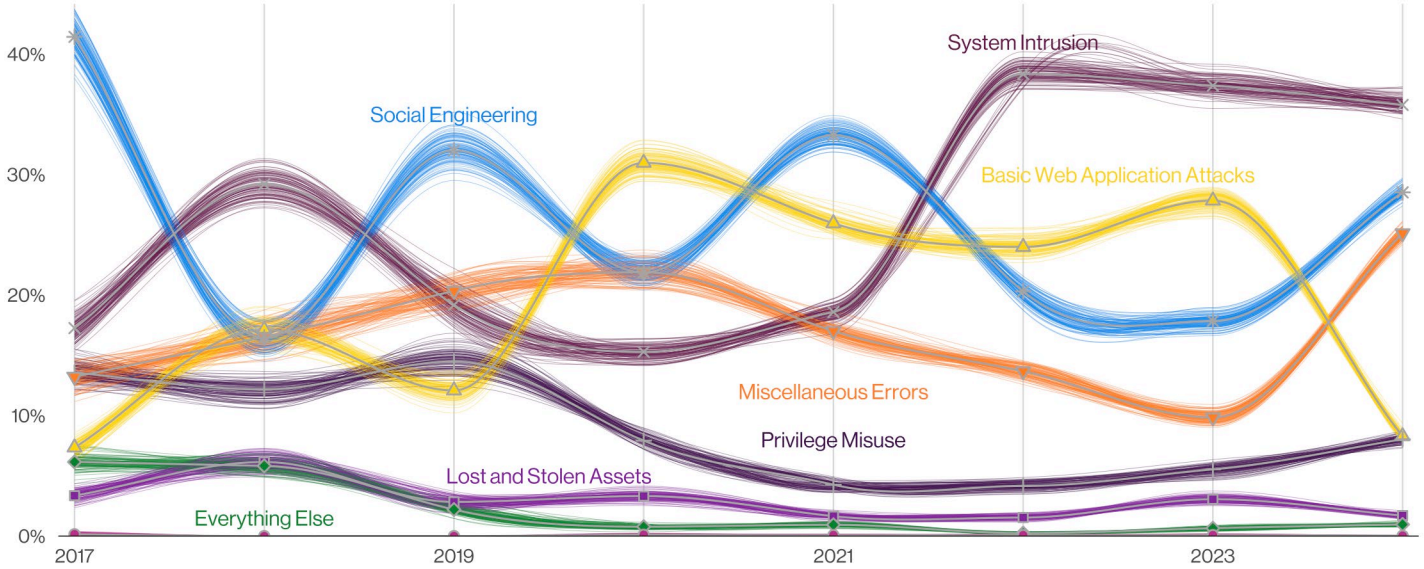


Figure 9. Patterns over time in breaches

System Intrusion

For the third year in a row, System Intrusion leads with 35% of breaches.

70% of System Intrusion incidents involved Ransomware as attackers continued to leverage a bevy of different techniques to compromise an organization and monetize its access.

92% of our industries have Ransomware (or some type of Extortion) as one of their top three actions. Education was the most impacted by MOVEit-related breaches (> 50%).

The median loss associated with Ransomware/Extortion breaches ranged between $3 (three dollars) and $1,141,467 for 95% of the cases. Only 4% of complaints had registered any adjusted loss in FBI IC3 complaints.

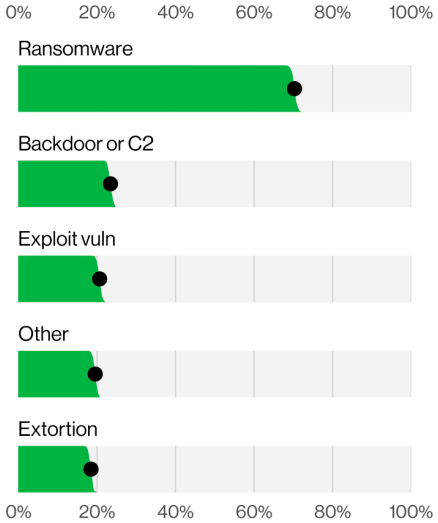


Figure 10. Top Action varieties in System Intrusion incidents

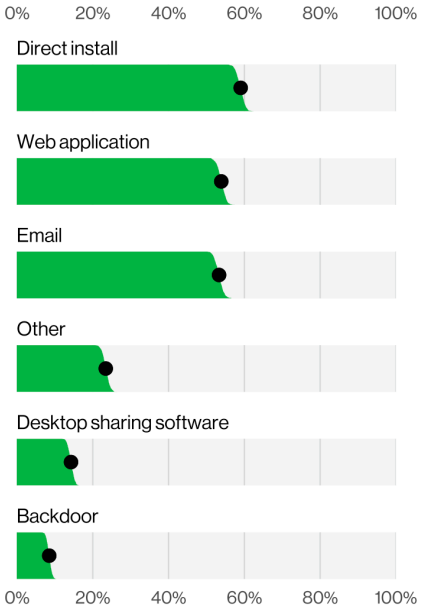


Figure 11. Top Action vectors for System Intrusion incidents (n=1,789)

Social Engineering

We have not seen a dramatic rise in Pretexting like we did last year. However, it is also true that it hasn't decreased. More than 40% of incidents involved Pretexting and 31% involved Phishing.

Social Engineering accounts for 29% of breaches and 12% of incidents. Extortion-based attacks were also classified here, giving this pattern a big bump.

Based on FBI IC3 data, the median amount stolen in a BEC has remained stable at around $50,000. The FBI's response team was able to recoup just under 80% of the lost money for more than 50% of the cases.

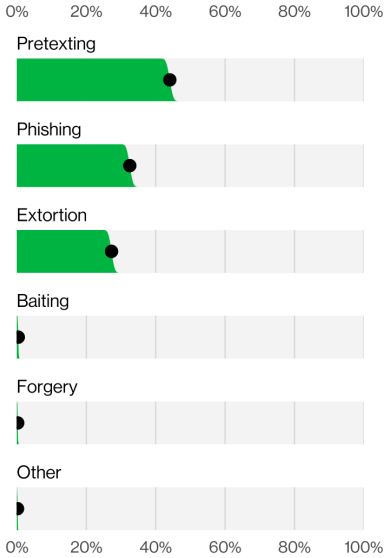


Figure 12. Top Action varieties in Social Engineering incidents (n=3,647)

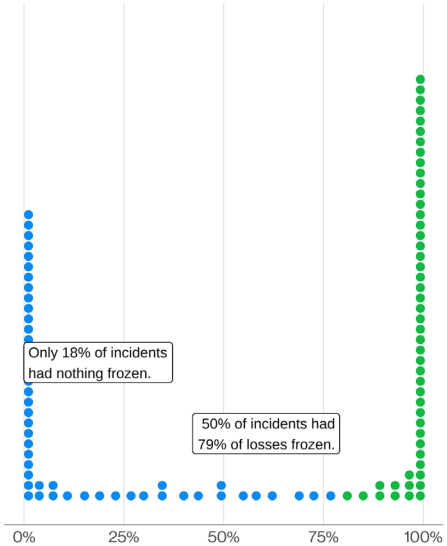


Figure 13. Percentage of adjusted losses distribution for BECs (n=2,041). Based on FBI IC3 complaints in which a transaction occurred.

Miscellaneous Errors

This pattern is significantly up—25% as opposed to 9% last year. The growth is due in large part to mandatory reporting entities, suggesting that that Errors are a more prevalent cause of breaches.

End-users accounted for 87% of errors as opposed to 20% in last year's report; while System administrators dropped to only 11% (from 46% last year). This drop is in large part the result of the corresponding rise in Misdelivery.

Data compromised included Personal (94%), Internal (34%) and Bank (14%).

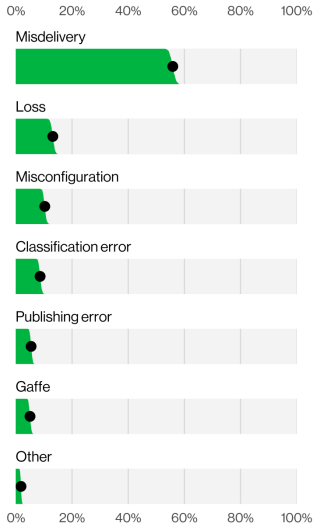


Figure 14. Top Action varieties in Miscellaneous Errors breaches (n=2,586)

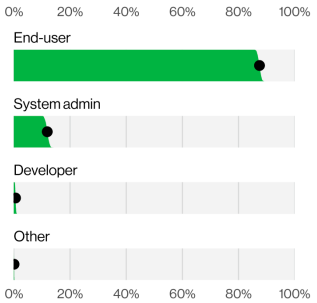


Figure 15. Top Actor varieties in Miscellaneous Errors breaches (n=2,260)

Basic Web Application Attacks

Basic Web Application Attacks breaches and incidents tend to be largely driven by attacks against Credentials, which are then leveraged to access a variety of resources. They represented 8% of the dataset.

77% of Basic Web Application Attacks breaches involve the Use of stolen credentials.

13% of breaches in this pattern involve the Exploit vuln action.

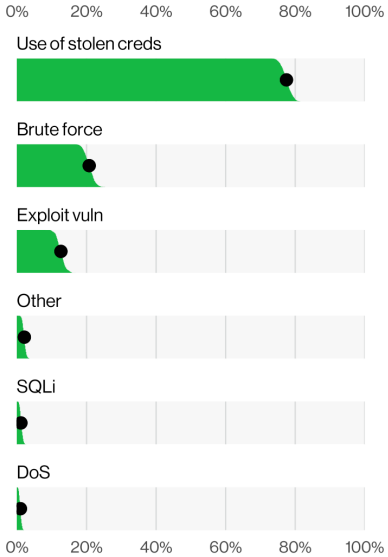


Figure 16. Top Hacking actions in Basic Web Application Attacks breaches (n=713)

Denial of Service

Denial of Service was responsible for 55% of incidents analyzed this year.

Content delivery network (CDN)–monitored, web application–focused Denial of Service attacks show a median attack size of 1.6 gigabits per second (Gbps), with the 97.5th percentile of those attacks increasing to 170 Gbps from the previous high of 124 Gbps. Those attacks are usually short duration, with large volumes—50% of those attacks are less than five minutes long.

Attacks on ISP-level defenses, including individuals, are significantly smaller in size and duration, with a median time of nine minutes.

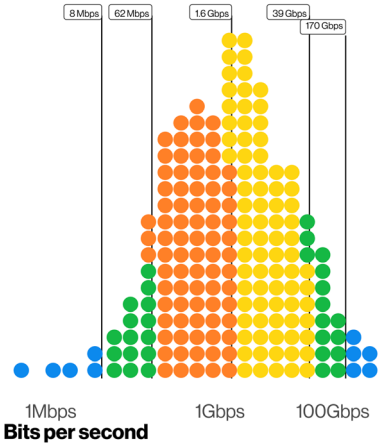


Figure 17. Bits per second in CDN distributed DoS (DDoS) incidents (n=10,713, log scale)

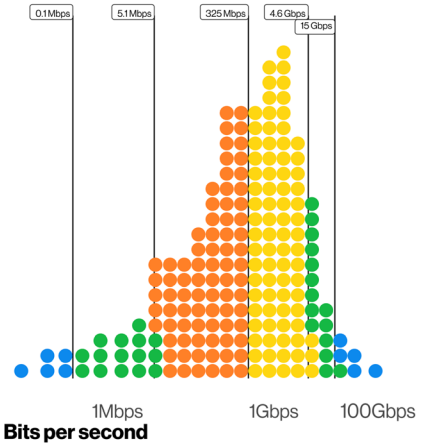
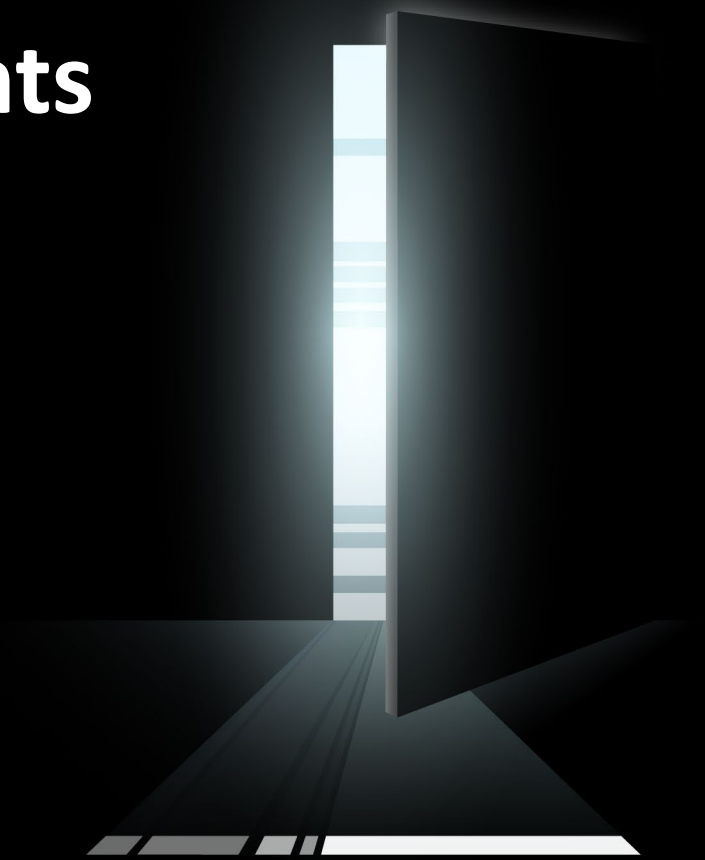


Figure 18. Bits per second in ISP-level DDoS incidents (n=800,155, log scale)

Industry-tailored insights



Accommodation and Food Services (NAICS 72)

Frequency	220 incidents, 106 with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering and Basic Web Application Attacks represent 92% of breaches
Threat actors	External (92%), Internal (9%), Multiple (1%) (breaches)
Actor motives	Financial (100%) (breaches)
Data compromised	Credentials (50%), Personal (28%), Payment (19%), System (19%), Other (16%) (breaches)
What is the same?	Ransomware and social attacks continue to be a persistent problem within this industry, accounting for 35% of incidents.

Social Engineering has increased dramatically and now accounts for 25% of incidents in this sector. Pretexting more than doubled from the previous year and was reported in 20% of incidents.

Ransomware continues to be one of the top action varieties, holding steady at 16% of all incidents.

In other news, Payment card data being compromised has dropped to an all-time low, from 41% of breaches in 2023 to now only 19%.

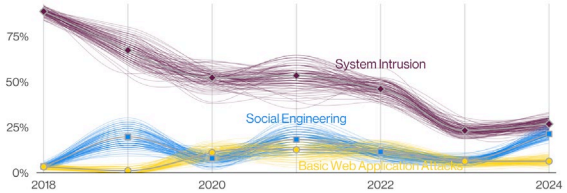


Figure 19. Top patterns in Accommodation and Food Services incidents over time

Educational Services (NAICS 61)

Frequency	1,780 incidents, 1,537 with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering and Miscellaneous Errors represent 90% of breaches
Threat actors	External (68%), Internal (32%) (breaches)
Actor motives	Financial (98%), Espionage (2%) (breaches)
Data compromised	Personal (83%), Internal (20%), Other (18%), Credentials (9%) (breaches)
What is the same?	The same three patterns dominate this vertical as last year. External actors stealing Personal data accounts for the majority of breaches.

Errors of various types committed by internal actors and Extortion from external threat actors constitute the curriculum of this industry.

In errors, Misdelivery is front and center, accounting for 56% of errors. Loss (19%) and Classification error (10%) round off the top three error varieties.

The action types of malware (Backdoor – 57%), hacking (Exploit vuln – 56%) and social (Extortion – 50%) were present in almost the exact same percentages. This is due largely to the MOVEit vulnerability being so prevalent in Education.

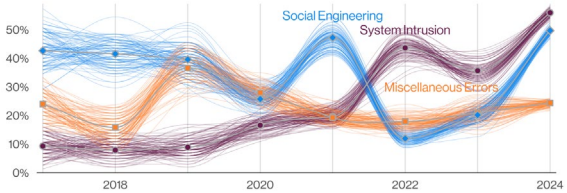


Figure 20. Top patterns in Educational Services breaches over time

Financial and Insurance (NAICS 52)

Frequency	3,348 incidents, 1,115 with confirmed data disclosure
Top patterns	System Intrusion, Miscellaneous Errors and Social Engineering represent 78% of breaches
Threat actors	External (69%), Internal (31%) (breaches)
Actor motives	Financial (95%), Espionage (5%) (breaches)
Data compromised	Personal (75%), Other (30%), Bank (27%), Credentials (22%) (breaches)
What is the same?	Miscellaneous Errors continue to plague this industry. As it did last year, Misdelivery presents an ongoing challenge for this sector.

System Intrusion has overtaken Miscellaneous Errors and Basic Web Application Attacks as the primary threat in Financial and Insurance this year, indicating a shift toward more complex attacks accompanied by a rise in Social Engineering.

Ransomware and the Use of stolen credentials, the bread and butter of the System Intrusion pattern, are very common in this industry.

Lastly, but certainly worthy of mention, is that 8% of the cases in our incident dataset targeting this sector were part of the whirlwind of the MOVEit breach, which shows how far-reaching supply chain breaches can be.

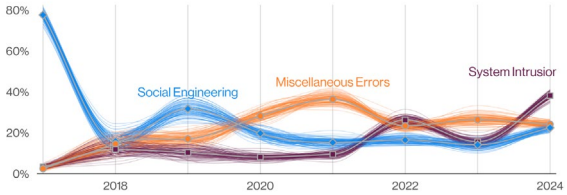


Figure 21. Top patterns in Financial and Insurance breaches over time

Healthcare (NAICS 62)

Frequency	1,378 incidents, 1,220 with confirmed data disclosure
Top patterns	Miscellaneous Errors, Privilege Misuse and System Intrusion represent 83% of breaches.
Threat actors	Internal (70%), External (30%) (breaches)
Actor motives	Financial (98%), Espionage (1%) (breaches)
Data compromised	Personal (75%), Internal (51%), Other (25%), Credentials (13%), (breaches)
What is the same?	System Intrusion breaches remain in the top three attack patterns.

This year's Healthcare sector analysis reveals significant shifts compared to previous years.

Insiders deliberately causing breaches have surged back into second place after a steady decline since 2018.

Interestingly, Personal data has eclipsed Medical data as the preferred target for threat actors.

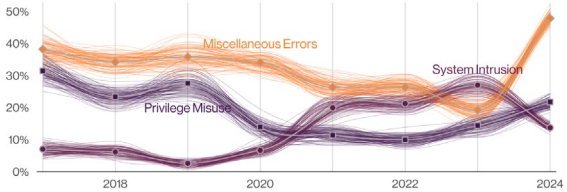


Figure 22. Top patterns in Healthcare breaches over time

Information (NAICS 51)

Frequency	1,367 incidents, 602 with confirmed data disclosure
Top patterns	System Intrusion, Basic Web Application Attacks and Social Engineering represent 79% of breaches
Threat actors	External (79%), Internal (21%), Multiple (1%) (breaches)
Actor motives	Financial (87%), Espionage (14%) (breaches)
Data compromised	Other (46%), Personal (45%), Credentials (27%), Internal (22%) (breaches)
What is the same?	The top three attack patterns remain constant since last year, and their ranked order has also not changed.

The overall breach sample size increased compared to last year, but this sector experienced substantially fewer breaches.

Ransomware and Use of stolen credentials continue to dominate the System Intrusion pattern, while there was a slight decrease in Phishing attacks alongside a rise in Pretexting within the Social Engineering pattern.

There was a mild increase in Espionage motives and state-sponsored actors targeting the industry, emphasizing the need for enhanced detective controls.

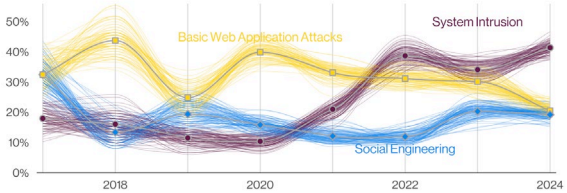


Figure 23. Top patterns in Information breaches over time

Manufacturing (NAICS 31–33)

Frequency	2,305 incidents, 849 with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering and Miscellaneous Errors represent 83% of breaches
Threat actors	External (73%), Internal (27%) (breaches)
Actor motives	Financial (97%), Espionage (3%) (breaches)
Data compromised	Personal (58%), Other (40%), Credentials (28%), Internal (25%) (breaches)
What is the same?	Two of the top patterns from last year are still in place. Financial motivation continues to be the driver behind most attacks.

Manufacturing has seen an increase in Error-related breaches. The installation of malware after hacking in via the Use of stolen credentials is somewhat commonplace.

Social Engineering remains steady with regard to breaches in this vertical due to action varieties
such as Phishing (55%) and Pretexting (42%).

Ransomware accounts for 85% of breaches in the System Intrusion pattern for Manufacturing.

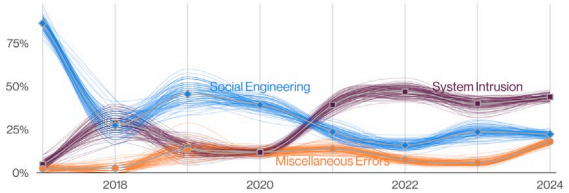


Figure 24. Top patterns in Manufacturing breaches over time

Professional, Scientific and Technical Services (NAICS 54)

Frequency	2,599 incidents, 1,314 with confirmed data disclosure
Top patterns	Social Engineering, System Intrusion and Miscellaneous Errors represent 85% of breaches
Threat actors	External (75%), Internal (25%) (breaches)
Actor motives	Financial (95%), Espionage (6%) (breaches)
Data compromised	Personal (40%), Credentials (38%), Other (33%), Internal (23%) (breaches)
What is the same?	Personal data and Credentials are still the top types of data impacted in this industry.

Social Engineering is one of the top threats facing this industry, accounting for 40% of breaches. In addition, there has been an increase in errors, specifically Misdelivery.

When it comes to intentional breaches, the vast majority of those cases fall into two buckets: Ransomware and the BEC, at 24% and 20% respectively.

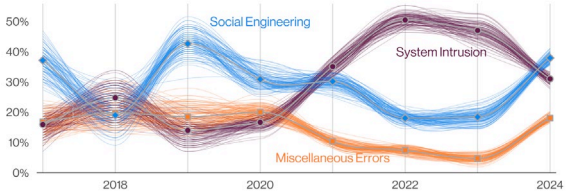


Figure 25. Top patterns in Professional, Scientific and Technical Services breaches over time

Public Administration (NAICS 92)

Frequency	12,217 incidents, 1,085 with confirmed data disclosure
Top patterns	Miscellaneous Errors, System Intrusion and Social Engineering represent 78% of breaches
Threat actors	Internal (59%), External (41%) (breaches)
Actor motives	Financial (71%), Espionage (29%) (breaches)
Data compromised	Personal (72%), Internal (37%), Other (31%), Credentials (17%) (breaches)
What is the same?	System Intrusion and Social Engineering remain top attack patterns in this sector.

Miscellaneous Errors, particularly Misdelivery, have surged to the top spot in this industry.

System Intrusion now ranks second, where Ransomware accounted for 61% of malware-related breaches and Use of stolen credentials for 83% of hacking-related breaches.

The Social Engineering attacks we saw in Public Administration were mostly garden-variety Phishing (66% of breaches) and Pretexting (23%) attacks.

The most common external actors in this vertical were Organized crime (largely Ransomware attacks) at 67% and State-affiliated actors (29%).

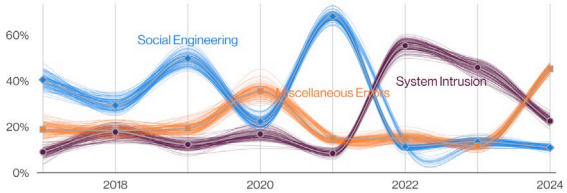


Figure 26. Top patterns in Public Administration breaches over time

Retail (NAICS 44–45)

Frequency	725 incidents, 369 with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering and Basic Web Application Attacks represent 92% of breaches
Threat actors	External (96%), Internal (4%) (breaches)
Actor motives	Financial (99%), Espionage (1%) (breaches)
Data compromised	Credentials (38%), Other (31%), Payment (25%), System (20%) (breaches)
What is the same?	The three attack patterns not only remained consistent but are even in the same ranked order as last year. Threat actors with a Financial motivation continue to target this sector.

While this industry is usually the place where we see Payment card data stolen, the focus of the threat actors has shifted to Credentials.

Pretexting is also increasing, while Phishing has dropped.

Denial of Service attacks remain a problem for Retail organizations, causing disruption to their ability to serve their customers and make sales.

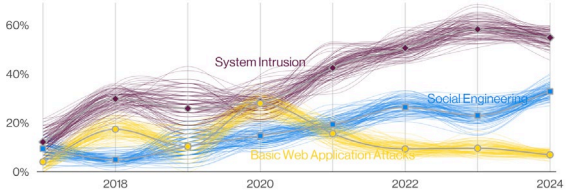
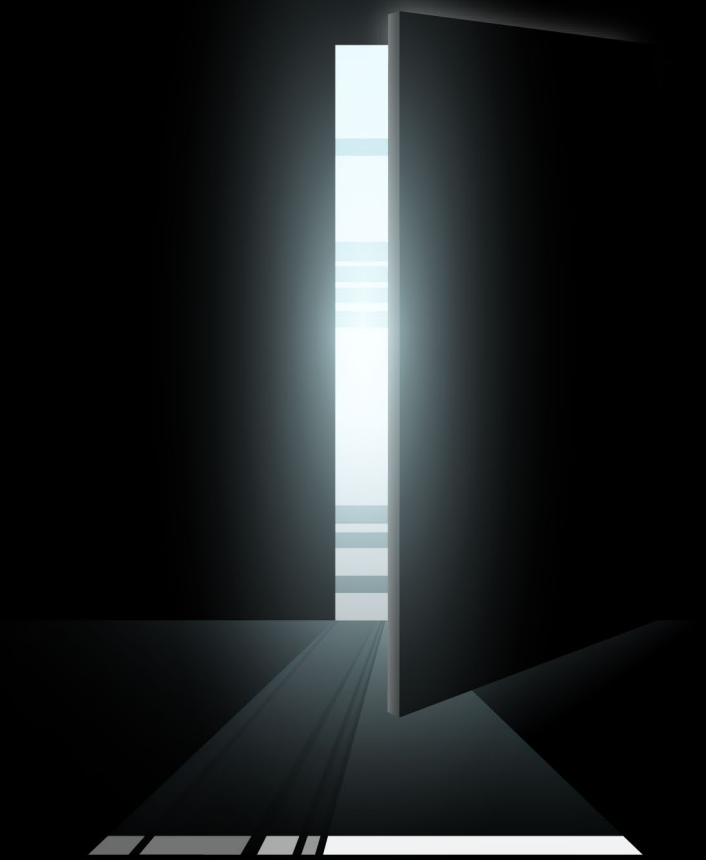


Figure 27. Top patterns in Retail breaches over time

Regions



Regions – detailed breakdown

Region	Frequency	Top patterns	Threat actors	Actor motives	Data compromised
APAC	2,130 incidents, 523 with confirmed data disclosure	System Intrusion, Social Engineering and Basic Web Application Attacks represent 95% of breaches	External (98%), Internal (2%) (breaches)	Financial (75%), Espionage (25%) (breaches)	Credentials (69%), Internal (37%), Secrets (24%), Other (17%) (breaches)
EMEA	8,302 incidents, 6,005 with confirmed data disclosure	Miscellaneous Errors, System Intrusion and Social Engineering represent 87% of breaches	External (51%), Internal (49%) (breaches)	Financial (94%), Espionage (6%) (breaches)	Personal (64%), Other (36%), Internal (33%), Credentials (20%) (breaches)
NA	16,619 incidents, 1,877 with confirmed data disclosure	System Intrusion, Social Engineering and Basic Web Application Attacks represent 91% of breaches	External (93%), Internal (8%) (breaches)	Financial (97%), Espionage (4%) (breaches)	Personal (50%), Credentials (26%), Internal (19%), Other (16%) (breaches)

APAC: Asia Pacific
EMEA: Europe, Middle East and Africa
NA: Northern America

Regions – Northern America

The System Intrusion pattern remains among the top for all regions. The two main action types are hacking via the Use of stolen credentials and malware in the form of Ransomware.

Social Engineering has increased from 29% to 45% when viewed as a whole (mostly driven by Northern America).

Extortion was the greatest driver of this growth in NA as it was present in 46%
of its breaches. Our other Social Engineering favorites had a more timid showing in Northern America breaches: 13% for Phishing and 4% for Pretexting.

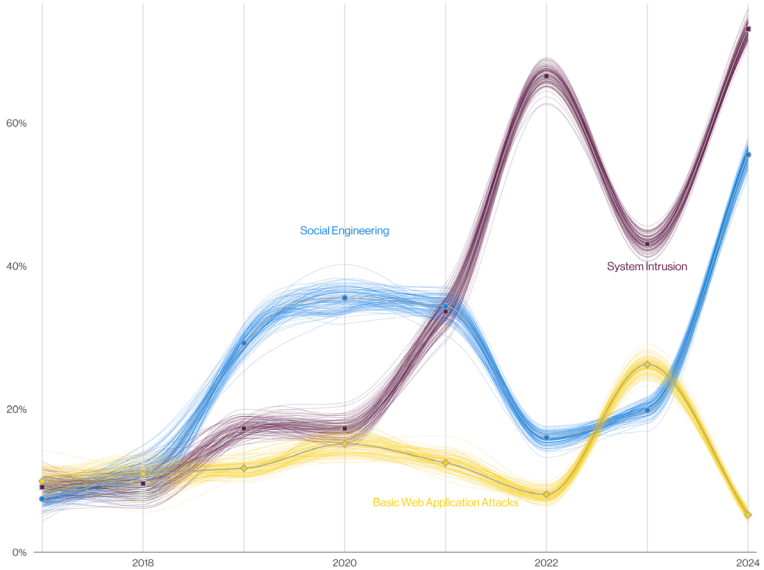


Figure 28. Top patterns in Northern America breaches over time

Regions – APAC and EMEA

With regard to actors, the majority of cybercrime continues to be carried out by financially motivated external parties.

One notable exception is that of APAC, where instead of more than 90% of attacks being financially motivated, we see that the Espionage motive is greater than it is elsewhere and accounts for 25% of breaches (as opposed to between 4% and 6% in the other regions).

Due to the nature of our new contributing agencies in EMEA, we have seen a substantial rise in the Miscellaneous
Errors pattern.

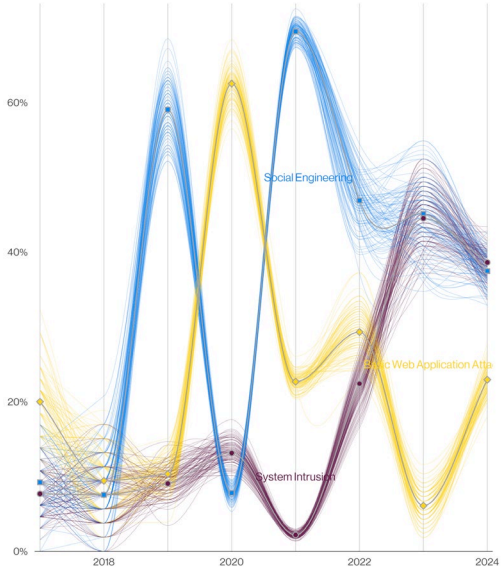


Figure 29. Top patterns in APAC breaches over time

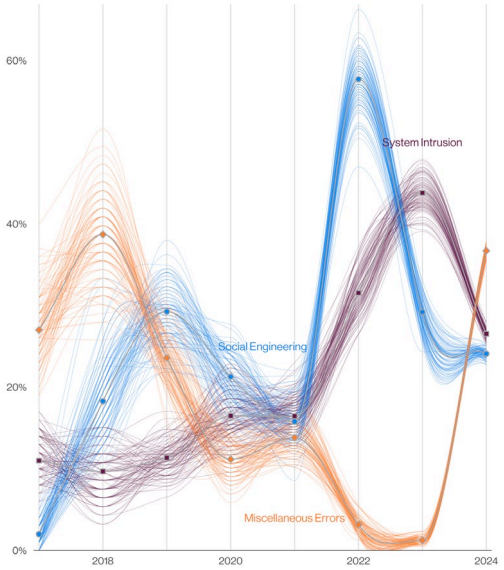


Figure 30. Top patterns in EMEA breaches over time

Questions?

DBIR: verizon.com/dbir
Email: dbir@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.