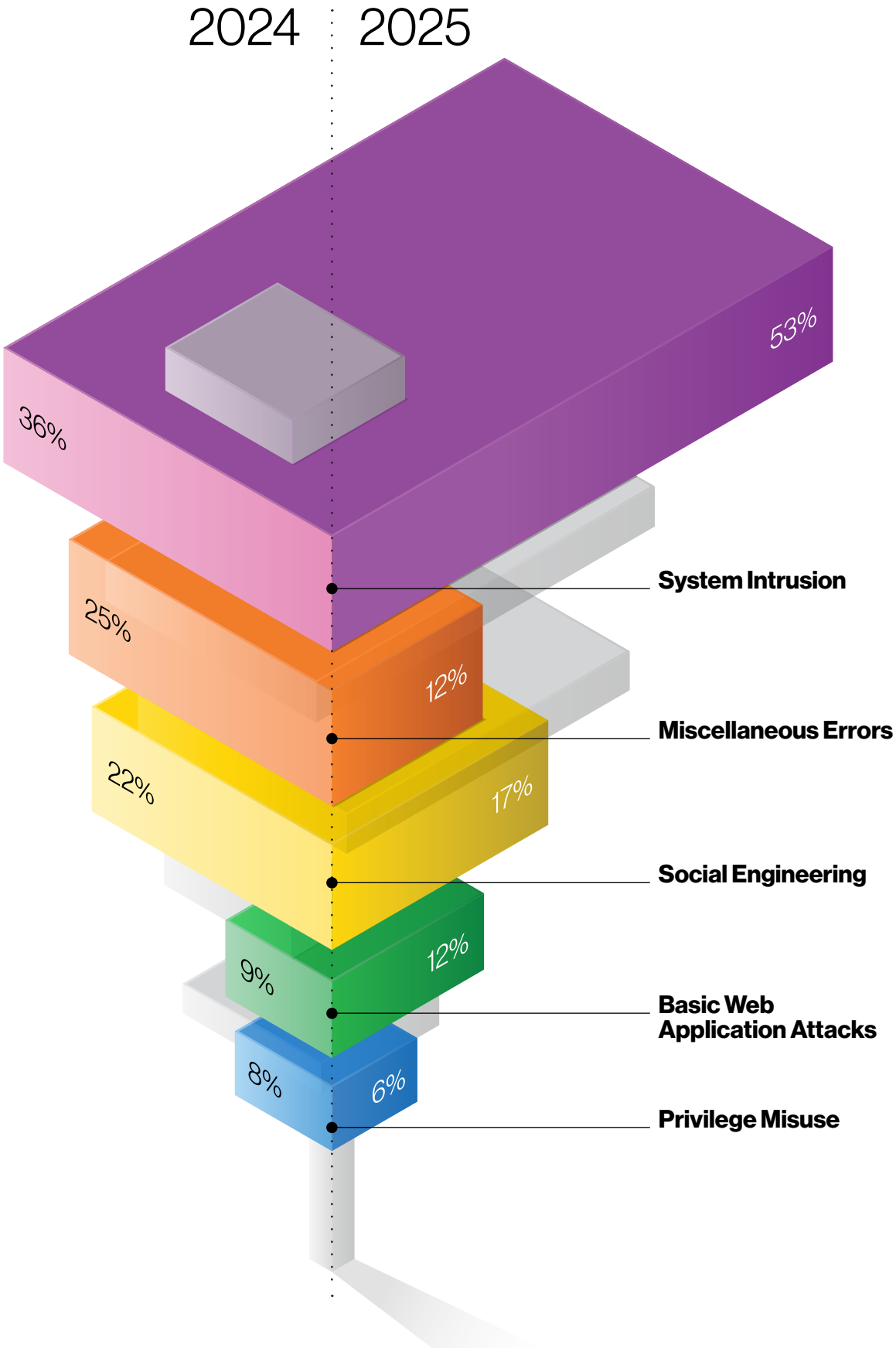
2025 Data Breach Investigations Report

Retail Snapshot

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

Hello, and welcome to the Verizon Data Breach Investigations Report (DBIR) Retail Snapshot.

The DBIR aims to provide security professionals with an in-depth analysis of data-driven, real-world instances of cybercrime and how cyberattacks play out across organizations of different sizes as well as from different verticals and disparate geographic locations. We hope that by doing so, we can provide you with insight into what particular threats your organization is most likely to face and thereby help prepare you to handle them.

As in past years, we will examine what our data has to tell us about threat actors and the tools they employ against enterprises. This year, we analyzed 22,052 real-world security incidents, of which 12,195 were confirmed data breaches (a record high!), with victims spanning 139 countries.

This data represents actual, real-world breaches and incidents 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. We hope you can use this report and the information it contains to increase your awareness of the most common tactics used against organizations at large and your specific industry. It offers strategies to help protect your company and its assets. Read the full report for a more detailed view of the threats you may face today at verizon.com/dbir.

About the 2025 DBIR incident dataset

Each year, the DBIR timeline for in-scope incidents is from Nov 1 of one calendar year through Oct 31 of the next calendar year. Thus, the incidents described in this year's report took place between Nov 1, 2023, and Oct 31, 2024. The 2024 caseload is the primary analytical focus of the 2025 report, but the entire range of data is referenced throughout, notably in trending graphs. The time between the latter date and the date of publication for the report is spent in acquiring the data from our global contributors, anonymizing and aggregating that data, analyzing the dataset, and finally creating the graphics and writing the report.

Industry labels

This snapshot highlights important takeaways for the Retail Trade (NAICS 44–45) sector, which includes establishments primarily engaged in retailing merchandise generally without transformation and rendering services incidental to the sale of merchandise.

In the DBIR, we align with the North American Industry Classification System (NAICS) standard to categorize the victim organizations in our corpus. The standard uses two- to six-digit codes to classify businesses and organizations. Our analysis is typically done at the two-digit level, and we will specify NAICS codes along with an industry label. For example, a chart with a label of Retail (NAICS 44–45) is not indicative of 44–45 as a value. "44–45" is the code for the Retail Trade sector. Detailed information on the codes and the classification system is available here:

https://www.census.gov/naics

22,052
security incidents investigated

12,195
confirmed breaches

Summary of findings

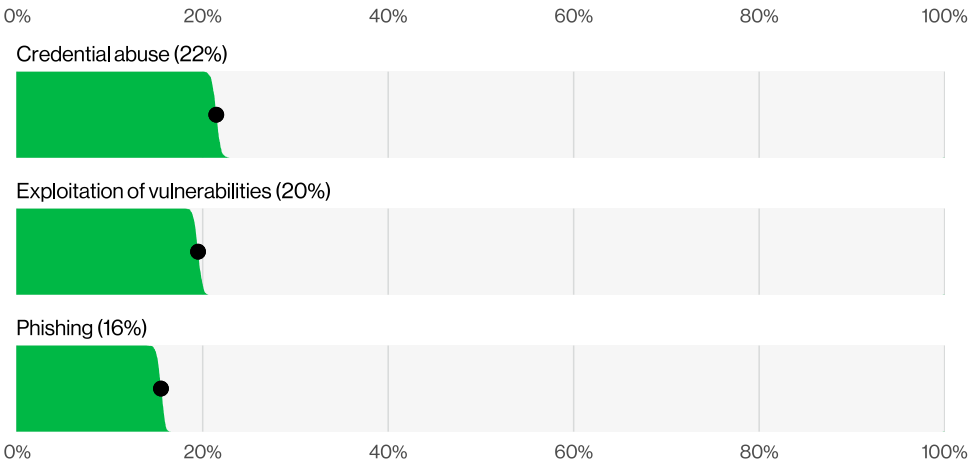


Figure 1. Known initial access vectors in non-Error, non-Misuse breaches (n=9,891)

If you're vulnerable, they will come.

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.

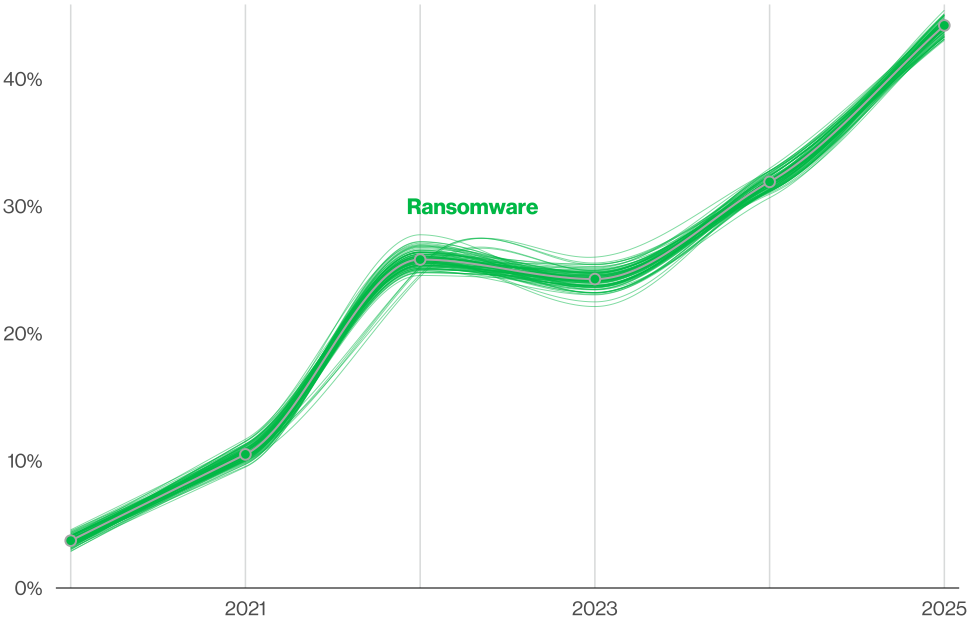


Figure 2. Ransomware action over time in breaches (n for 2025 dataset=10,747)

More organizations are being held hostage.

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 small- and medium-sized businesses (SMBs) experienced Ransomware-related breaches to the tune of 88% overall.

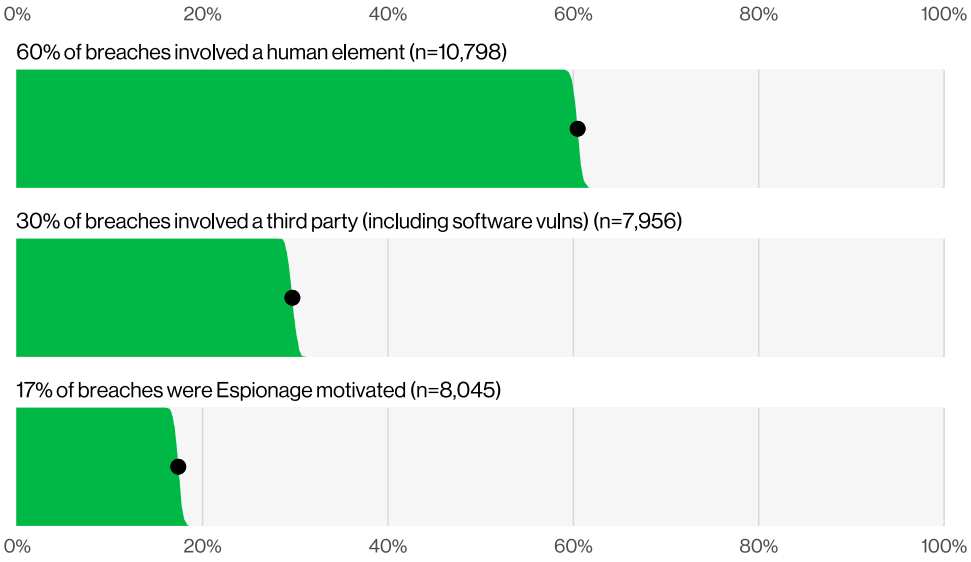


Figure 3. Select key enumerations in breaches

The ways in are shifting.

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.

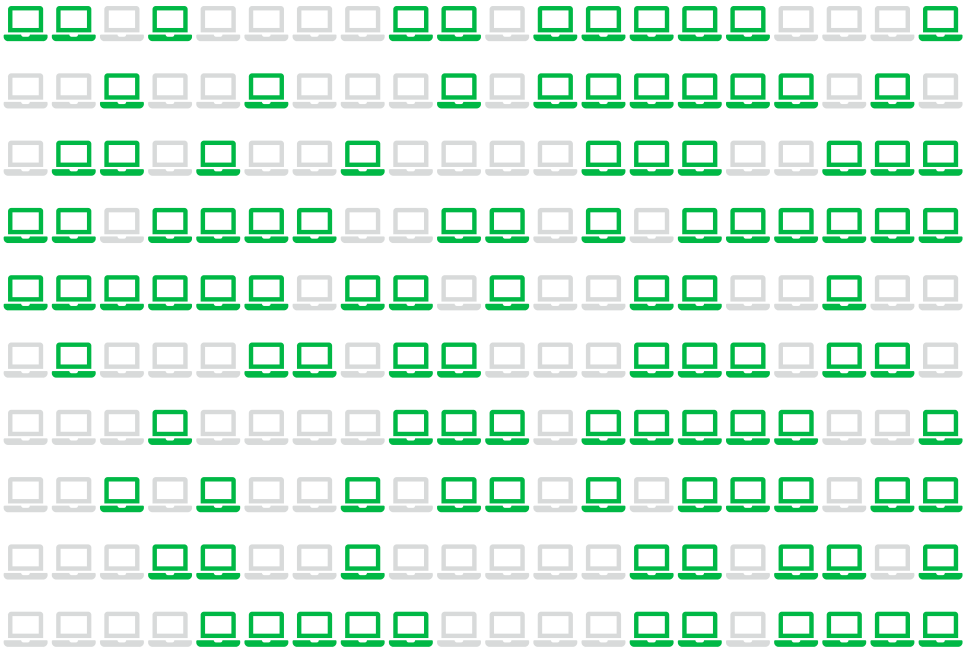


Figure 4. Percentage of non-managed devices with corporate logins in infostealer logs (each glyph is 0.5%)

No device is off-limits.

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%)

AI is not A-OK.

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.

Incident Classification Patterns

The DBIR first introduced the Incident Classification Patterns in 2014 as a useful shorthand for scenarios that occurred very frequently. In 2022, due to changes in attack type and the threat landscape, we revamped and enhanced those patterns, moving from nine to eight—the seven you see in this report and the Everything Else "pattern," which is a catch-all for incidents that don't fit within the orderly confines of the other patterns.

These patterns are based on an elegant machine-learning clustering process, equipped to better capture complex interaction rules, and they are much more focused on what happens during the breach. That makes them better suited for control recommendations, too.

Here are our key findings for each pattern:

System Intrusion These are complex attacks that leverage malware and/or hacking to achieve their objectives, including deploying Ransomware.	• 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).
Social Engineering This attack involves the psychological compromise of a person that alters their behavior into taking an action or breaching confidentiality.	• 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.

Basic Web Application Attacks These attacks are against a Web application, and after the initial compromise, they do not have a large number of additional Actions. It is the "get in, get the data and get out" pattern.	• 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%.
Miscellaneous Errors Incidents where unintentional actions directly compromised a security attribute of an information asset are found in this pattern. This does not include lost devices, which are grouped with theft instead.	• 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.
Privilege Misuse These incidents are predominantly driven by unapproved or malicious use of legitimate privileges.	• While the Privilege Misuse pattern is typically insiders, this year there has been an increase in Partner actors, now at 10%. • Most cases are motivated by direct financial gain, and while we see Espionage in this pattern (10%), it has decreased over last year's high (46%). • System admins are quite low in terms of committing deliberate actions that lead to a breach, whereas they figure rather prominently in terms of accidental breaches (due to their privileges).
Denial of Service These attacks are intended to compromise the availability of networks and systems. This includes both network and application layer attacks.	• This pattern is one of the consistent leaders in the incident patterns, and the size of the median attack has also grown substantially over the years. • Since 2018, there has been over 200% growth in the median for the size and about 1,000% increase in the upper bounds of the bits per second of those attacks. • The top industry targets of Denial of Service are Finance (35%), Manufacturing (28%) and Professional Services (17%).
Lost and Stolen Assets Incidents where an information asset went missing, whether through misplacement or malice, are grouped into this pattern.	• This pattern continues to trend downward in terms of the number of incidents and breaches compared to last year. This is hopefully due to effective controls being put in place on the assets, rendering the data inaccessible even when custody of the item is lost. • Medical data appeared again this year in the top data types affected in these breaches.

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.

While many of us enjoy indulging in some good old fashioned retail therapy, there are a number of people who also enjoy browsing through this industry's data. Unlike a shoplifter who steals the latest viral-on-social-media outfit, these Actors are less trendy and often go after the data they can most easily access. Payment card data used to be frequently targeted in this industry, as one might expect, but surprisingly enough, rather than seeing adversaries calmly strolling out the door with their pockets stuffed full of credit card info, we instead see them going for other data types. Is this because the credit card info has become so well protected that they go for an easier target while they have the access? Sadly, we do not get the "why" in our data, only the "what." But it does make us wonder.

We take a good look at the Magecart breaches that frequently plague this industry in our "System Intrusion" section, so if you want more in-depth detail, head over there and take a look.

This industry did see a small uptick in the number of incidents and breaches—on par with the increased overall numbers in our dataset this year. Although we normally see most of the actors who target this sector having a Financial motive, we saw the Espionage motive increase from a negligible 1% in last year's report to a surprising 9% this year. However, as noted in several other sections, our data contributors have changed, and we are most likely benefitting from increased visibility of this kind of threat actor. Along with a focus on protecting the payment data, defenders need to realize that they may be targeted by somewhat more sophisticated (and harder to detect) Actors, as well.

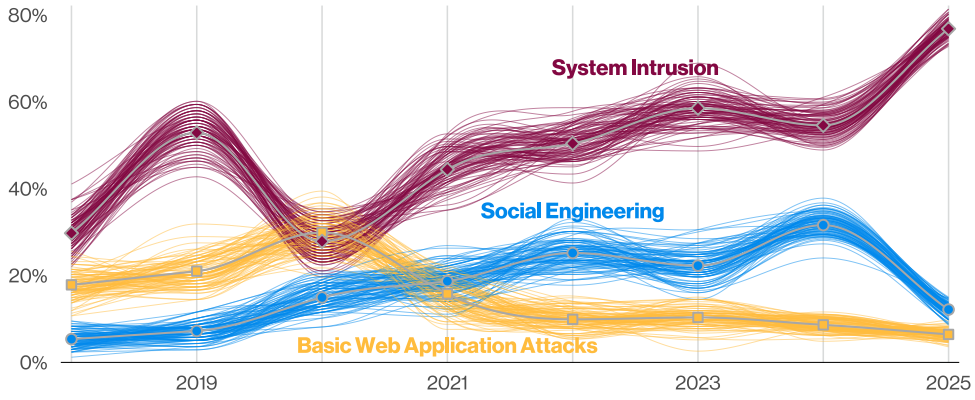


Figure 6. Top patterns over time in Retail breaches

As for our top three patterns, this year shows absolutely no change—not in the makeup of the top three or even what order they rank (Figure 6). And as far as threats go, it seems you will just be facing more of it in the future. The System Intrusion pattern is typically where the more sophisticated attacks land. Ransomware actors fall into this pattern—ransomware is a problem across all industries and is only getting worse. Social Engineering in the second spot means you need to make sure your people know how to spot and appropriately respond to the phishing and pretexting lures they will receive. Controls to stop the attacks from being successful even when the victim falls for the bait should also be a priority. And finally, the Basic Web Application Attacks pattern shows us that the simple attacks seem to still work just fine. Those attacks are largely about credentials and their reuse. It seems to be human nature to reuse a password across multiple sites, and since many of them use an email address for the login, the combination is very useful for criminals in many other places.

Stay informed and threat ready.

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

The full 2025 Data Breach Investigations Report 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.