2026 Data Breach Investigations Report

Retail snapshot

verizon business

2026

- **61%** System Intrusion
- **17%** Social Engineering
- **10%** Basic Web Application Attacks
- **8%** Miscellaneous Errors
- **3%** Privilege Misuse

2025

- **53%** System Intrusion
- **18%** Basic Web Application Attacks
- **17%** Social Engineering
- **12%** Miscellaneous Errors
- **7%** Privilege Misuse

2024

- **36%** System Intrusion
- **25%** Miscellaneous Errors
- **22%** Social Engineering
- **9%** Basic Web Application Attacks
- **8%** Privilege Misuse

About the cover

"The only constant is change" is an aphorism commonly ascribed to Greek philosopher Heraclitus. There has been no historical evidence uncovered that he had any hands-on experience with cybersecurity, but he would be right at home in our field with this mentality. But even as the threat landscape constantly evolves and changes, the 2026 edition of the Data Breach Investigations Report (DBIR) invites you to consider the importance of the fundamentals of cybersecurity as the best way to brave all of this change. A little cyber-stoicism, if you will.

On our cover, you can see concentric rings, each one representing a year of our data, floating down and settling onto the foundation of our cybersecurity knowledge. They add to our understanding and complement our defensive strategies and are segmented by the incident patterns from the past four years.

Our own 2026 report is the topmost ring, followed by 2025, 2024 and 2023, the last one already settled into the foundation.

There are more zero days and critical vulnerabilities year over year (YoY), generative artificial intelligence (GenAI) augmented malware is now a common occurrence, and complex forms of social engineering are becoming more successful as the prelude to a breach. Their speed may be increasing, their scale might be a concern, but those are all challenges defenders have been facing for a long time. This new world should require more focus, more agility, but does not necessitate an upheaval. Refinement, not revolution. We will be ready for the future if we continue to collaborate and work together for the greater good.

Also, yes, those are technically donut charts. Sorry, not sorry.

Table of contents

Welcome

Welcome to Verizon's 2026 Data Breach Investigations Report! Hello again to those who've been with us over the years – and to those joining the DBIR community for the first time, it's great to have you. As always, we're glad you're here.

In this 19th edition of the Verizon DBIR, we dig into more than 31,000 actual real-world security incidents, of which more than 22,000 were confirmed data breaches involving organizations in 145 countries. This represents the largest number of breaches we have ever examined in a single report! Yes, we realize that we have said that before, but what can we say? It's still true because the number of cases we examine continues to increase YoY. We leave it up to you to determine if that is a good thing or a not so good thing. For the victim organizations, it is undoubtedly the latter, but for our purposes of illuminating threats to your business, it is firmly in the former camp.

If we were to give this report an overarching theme, it would be "keeping a strong foundation in the face of change." Few people would argue that change, in every aspect of modern life, confronts us at an ever-increasing pace these days. The insights we try to provide in this report attempt to equip enterprises to meet cybersecurity changes in the most effective manner possible. And even though this report's dataset covers Oct 2024 through Nov 2025, both the DBIR team and Verizon are keenly aware of the growing impact and capabilities of AI-augmented vulnerability research and weaponization so far in 2026 based on early indicators and trends observed at the time of publication, and will provide some forward-looking commentary in regards to that where applicable.

We have observed that, in some areas, cybercrime has shifted in meaningful ways since the publication of the 2025 report. In others, it is less a matter of change and more a matter of speed and scale. Exploitation of vulnerabilities, discussed in several sections of the report, has now emerged as the most common way attackers gain initial access into an organization's environment, which underlines the ongoing importance of getting the basics right. Additionally, as the ancient prophecies[1] foretold, threat actors are increasingly relying on GenAI to assist them with various stages of their attacks, such as choosing targets, gaining a foothold within those targets, conducting vulnerability research, and developing malware and other tools to make their efforts more effective and efficient. Meanwhile, Social Engineering, a longtime fan favorite, is evolving, as well, with attackers increasingly using voice and other mobile-centric techniques to catch people off guard in the middle of the workday.

Please continue reading for report highlights, including the latest breach findings for industries and regions. And 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.

1. And by ancient, we mean predicted in the past two DBIR reports and mentioned a couple paragraphs ago.

How to use this report

First-time readers:

Before you get started on the 2026 DBIR, it might be a good idea to take a look at this section first. We have been doing this report for quite a while now, and we appreciate that the verbiage we use can be a bit obtuse at times. We use very deliberate naming conventions, terms and definitions and spend a lot of time making sure we are consistent throughout the report. Hopefully this section will help make all of those more familiar. If you are a longtime reader (thank you!) and are already familiar with how to use the DBIR, you are welcome to skip to the next section.

What you will find here

The Data Breach Investigations Report (DBIR) focuses on the analysis of anonymized cybersecurity incident data that Verizon collects every year from almost a hundred data contributors. Those data points are normalized using the Vocabulary for Event Recording and Incident Sharing (VERIS) framework (more about it on the next page), which provides us a great foundation for statistical analysis of this type of data. Given the culture of secrecy (and just how difficult incident response is sometimes) that still permeates these cases, we often don't have all the very specific details of any given incident.

The breadth of data collection is what sets this report apart. Vendor-specific reports are able to talk very authoritatively and in great detail about the cases they investigated themselves, but here we are seeking to bridge different perspectives and contributor types – large incident response outfits, boutique forensics firms, law enforcement from local to country level, cyber insurance brokers and reinsurers – with the hope that it will get us closer to the capital T "Truth" of what is going on in the threat landscape.

VERIS framework resources

The terms "threat actions," "threat actors" and "varieties" will be referenced often. These are part of the VERIS, a framework designed to allow for the consistent, unequivocal collection of security incident details. Here is how they should be interpreted:

Threat actor: Who is behind the event? This could be the external "bad guy" who launches a phishing campaign or an employee who leaves sensitive documents in their seat back pocket.

Threat action: What tactics (actions) were used to affect an asset? VERIS uses seven primary categories of threat actions: Malware, Hacking, Social, Misuse, Physical, Error and Environmental. Examples at a high level are hacking a server, installing malware or influencing human behavior through a social attack.

Variety: More specific enumerations of higher-level categories – e.g., classifying the external "bad guy" as an organized criminal group or recording a hacking action as SQL injection or brute force.

There are also "vectors" and "motives" and "categories," but we do our best in each section to ease folks into the nomenclature and try to make it clear how to interpret those terms. Also, any weird capitalization issues you may find throughout the report are referring to VERIS "Proper Nouns" and have specific meaning tied to them in the framework. As much as in the Fae world, true names have power here.

Learn more here:

- github.com/vz-risk/veris – features the framework's JavaScript Object Notation (JSON) schema with some usage, utility scripts, enumeration listings, mappings to Center for Internet Security (CIS) Critical Security Controls, MITRE ATT&CK and a VERIS Style Guide
- verisframework.org – a slightly more user-friendly website providing information on the framework with examples and enumeration listings

Incident vs. breach

We talk a lot about incidents and breaches and we use the following definitions:

Incident: A security event that compromises the integrity, confidentiality or availability of an information asset.

Breach: An incident that results in the confirmed disclosure – not just potential exposure – of data to an unauthorized party. A distributed DoS (DDoS) attack, for instance, is most often an incident rather than a breach since data is rarely exfiltrated. However, we realize that doesn't make it any less serious.

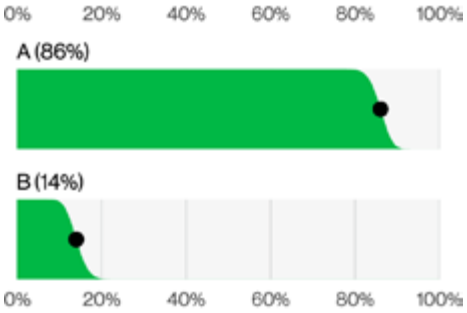

Figure 2. Example slanted bar chart (n=230)

Industry labels

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 Financial (52) is not indicative of 52 as a value. "52" is the NAICS code for the Financial and Insurance sector. The overall label of "Financial" is used for brevity within the figures. Detailed information on the codes and the classification system are available here: census.gov/naics.

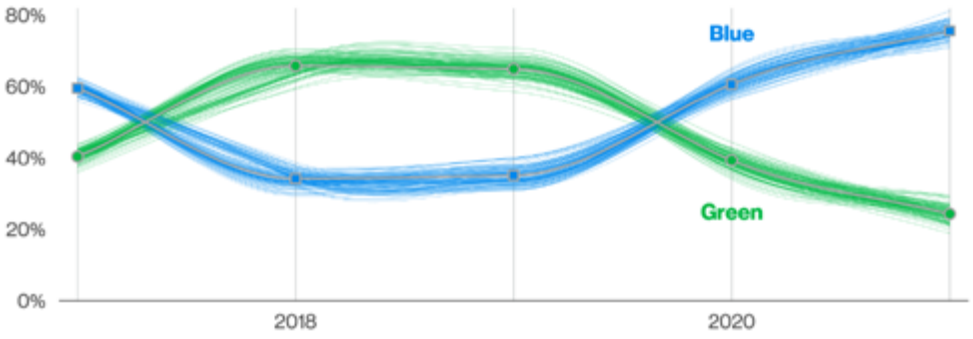

Figure 1. Example spaghetti chart

Being confident in our data

Starting in 2019 with slanted bar charts, the DBIR has tried to make the point that the only certain thing about information security is that nothing is certain. Even with all the data we have, we'll never know anything with absolute certainty. However, instead of throwing our hands up and complaining that it is impossible to measure anything in a data-poor environment or, worse yet, just plain making stuff up, we get to work. This year, you'll continue to see the team representing uncertainty throughout the report figures.

The examples shown in Figures 1, 2 and 3 all convey a range of realities that could credibly be true. Whether it be the slant of the bar chart, the threads of the spaghetti chart, the dots of the dot plot or the colors of the pictogram plot, all convey the uncertainty of the cybersecurity industry in their own special way.

The slanted bar chart will be familiar to returning readers. The slant on the bar chart represents the uncertainty of that data point to a 95% confidence level (which is a common standard for statistical testing). In layman's terms, if the slanted areas of two (or more) bars overlap, you can't really say one is bigger than the other without angering the math gods.

Much like the slanted bar chart, the spaghetti chart represents the same concept: the possible values that exist within the confidence interval. However, it's slightly more involved because we have the added element of time. The individual threads represent a sample of all possible connections between the points that exist within each observation's confidence interval.

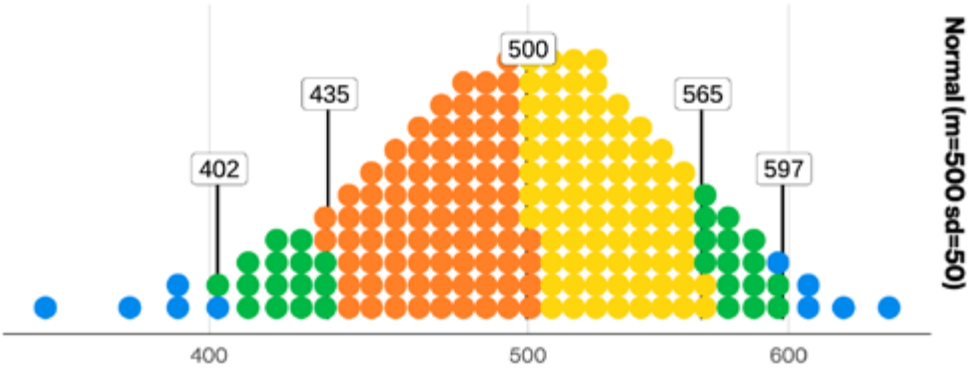

Figure 3. Example dot plot (n=10,000 – each dot is one event)
Orange: lower half of 80%; Yellow: upper half of 80%; Green: 80%–95%; Blue: Outliers, 95% of events: 402–597 80% of events: 435–565, Median: 500

As you can see, some of the threads are looser than others, indicating a wider confidence interval and a smaller sample size.

The dot plot is another returning champion, and the trick to understanding this chart is to remember that the dots represent a specific number of events, described in the figure caption. This is a much better way of understanding how something is distributed among organizations and provides considerably more information than an average or a median. We added more colors and callouts to those in an attempt to make them even more informative. In statistical terms, it's just a quantized density chart. In non-statistical terms, who doesn't love colored little dots?

Key topics and findings

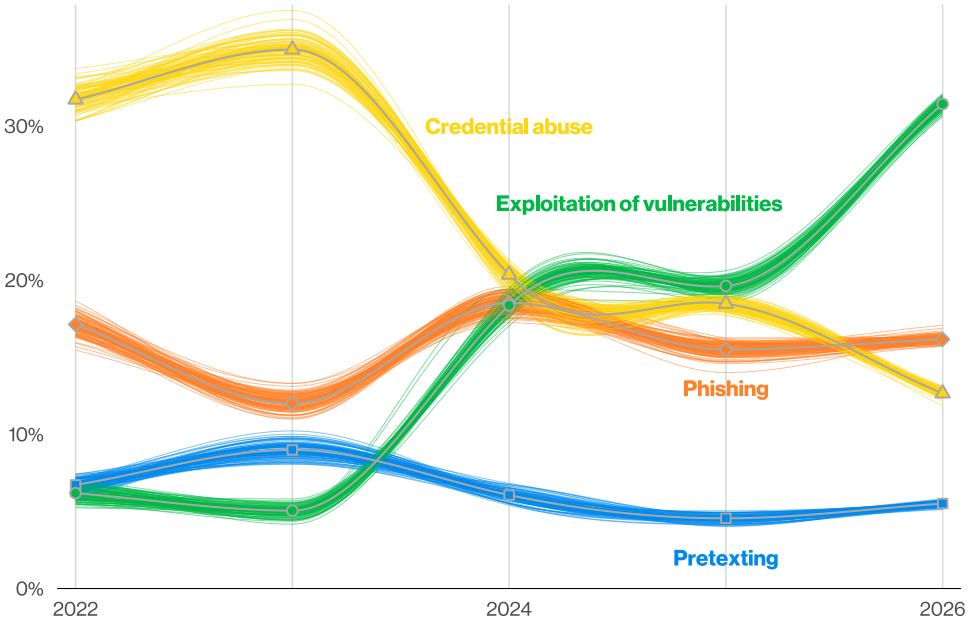

Figure 4. Known initial access vectors in non-Error, non-Misuse breaches over time (n for 2026 dataset=19,905)

Rise of vulnerability exploitation

Exploitation of vulnerabilities is now the most common initial access vector for breaches. It has risen to 31% in this year's reporting dataset, while credential abuse – the previous leader – is down to 13%.

Only 26% of critical vulnerabilities – defined as being in the Cybersecurity Infrastructure and Security Agency Known Exploited Vulnerabilities (CISA KEV) catalog – were fully remediated by organizations in 2025, a drop from the previous year's 38%.

The median time for full resolution went up to 43 days, almost two weeks more than the previous year's 32 days. In the median case, organizations had 50% more critical vulnerabilities to patch in this year's reporting dataset compared to the previous year.

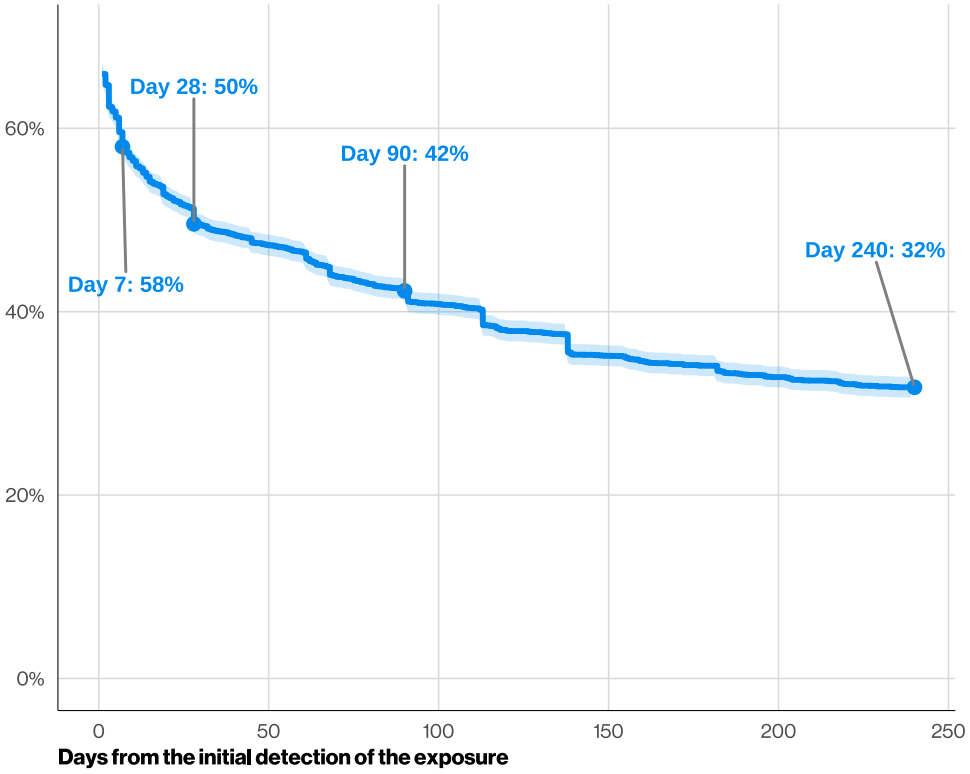

Figure 5. Survival analysis of third-party, cloud-based MFA exposures (n=7,513)

Growth in ransomware and third-party breaches continues.

Ransomware grew again to 48% of all breaches, up from 44% from the previous year. However, ransom payments have continued to decline among our dataset, as 69% of ransomware victims didn't pay. The median amount of ransom paid also continues a downward trend: $139,875 in this year's reporting dataset from $150,000 in the previous year.

As organizations increase their reliance on third parties for services and software, their exposure increases, as well, and breaches with third-party involvement have increased by 60% from last year's dataset, reaching 48% of total breaches.

Looking at remediation over time in third-party cloud exposure, only 23% of third-party organizations fully remediated missing or improperly secured multifactor authentication (MFA) on their cloud accounts, with 50% of all findings being resolved within a month.

For weak passwords and permission misconfigurations, the time to resolve 50% of all findings was much worse, reaching almost eight months.

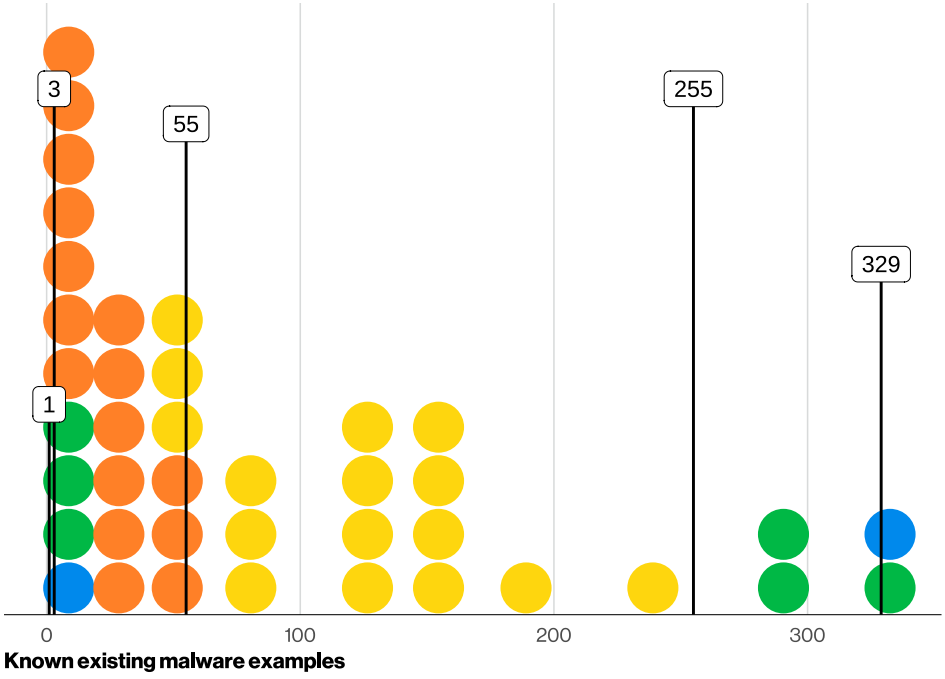

Figure 6. Distribution of known existing malware examples per ATT&CK technique observed (n=9,897—each dot is 247.43 observations)

Generative AI impacting the threat landscape

Threat actors are demonstrably using GenAI to help at different stages of attack, including targeting, initial access, and development of malware and other tools. The median threat actor researched or used AI assistance in 15 different documented techniques, with some Actors leveraging as many as 40 or 50.

Most AI-assisted development of malware and tooling was associated with well-known and defined attack techniques, with a median of 55 existing known malware examples performing the same functions.

Less than 2.5% of the AI-assisted malware observations involved less-common techniques with one or fewer known malware examples.

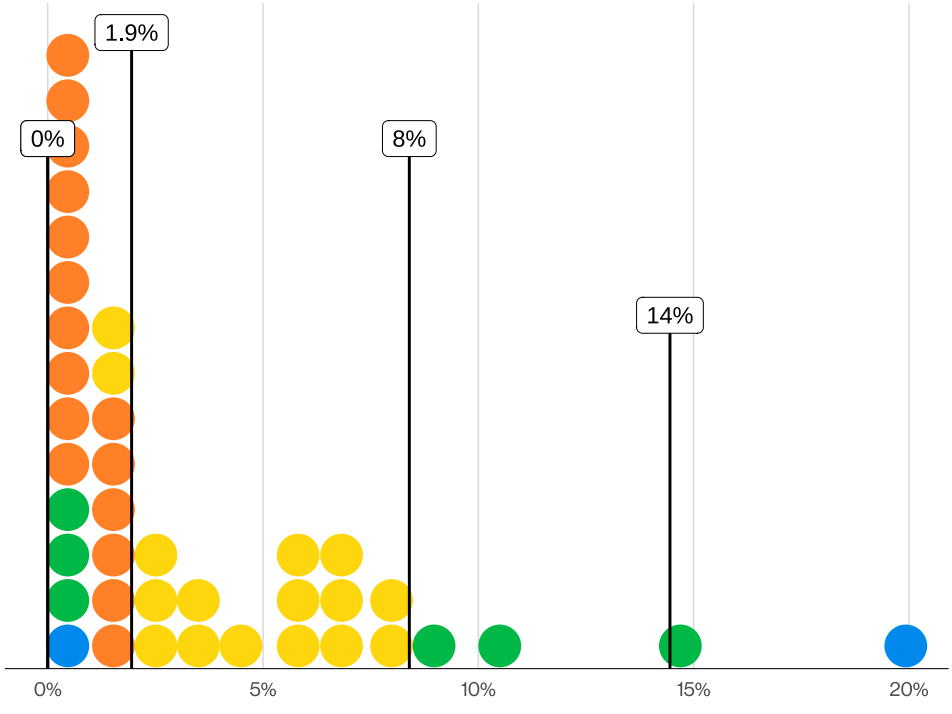

Figure 7. Distribution of success rate of non-Email vector-simulated social attack campaigns (n=35—each dot is 0.88 campaigns)

Mobile-centric Social Engineering

Human element was present in 62% of breaches, a slight increase from the previous year's 60%. Social Engineering was our third most common breach pattern, representing 16% of all breaches.

In phishing simulations, the median rate of successful "click" rates in mobile-centric vectors (such as voice and text messaging) is 40% higher than via email.

Pretexting has become a more common initial access vector to ransomware and extortion attacks. In all breaches, it reached 6%, while Phishing remained at 16% like the previous year. Pretexting is an attacker tactic in which a trusted relationship is built through concocted scenarios to trick the user into taking an action that unknowingly compromises the organization, frequently by voice communications but also seen via email or text messaging.

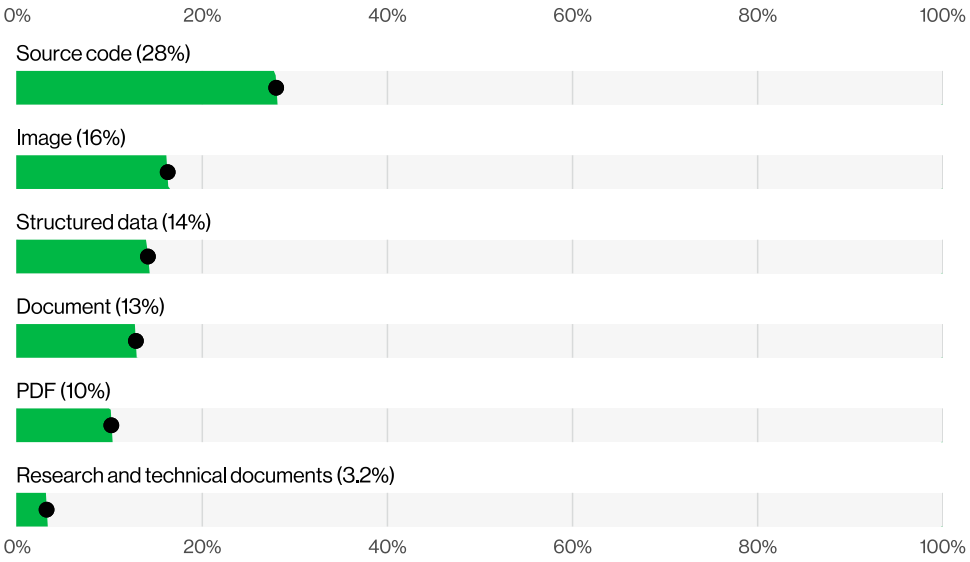

Figure 8. Select data types in untrusted DLP events targeting generative AI tools (n=858,440)

Shadow AI policy violations and malicious insiders

Regarding usage of unauthorized GenAI services ("Shadow AI"), 67% percent of users are using non-corporate accounts on their corporate devices to access AI services, a slight decrease from the previous year. However, 45% of employees are now considered regular users of AI (authorized or not) on their corporate devices, up from 15% in the previous year.

Shadow AI is now the third most common non-malicious insider action detected in our data loss prevention (DLP) dataset in 2025, a fourfold increase in percentage from the previous year.

The most common type submitted to external GenAI models was source code, followed by images and other types of structured data. In 3.2% of DLP policy violations, we even found research and technical documentation being uploaded to those unauthorized AI systems, which presents a risk of intellectual property exposure.

Retail NAICS 44–45

Summary

Retail organizations face persistent threats from external attackers exploiting vulnerabilities, stealing credentials and Phishing. These activities often lead to ransomware attacks and data theft, with third-party systems and internal corporate data becoming increasingly valuable targets.

What is the same?

The top three patterns remained the same, but their order of supremacy shifted a bit. The patterns have been the same consistently for many years now, but which is more prevalent in a given year changes.

Frequency	997 incidents, 806 with confirmed data disclosure
Top patterns	System Intrusion, Basic Web Application Attacks and Social Engineering represent 95% of breaches
Threat actors	External (99%), Internal (1%) (breaches)
Actor motives	Financial (85%), Espionage (19%) (breaches)
Data compromised	Internal (84%), Credentials (26%), Secrets (20%), Other (14%) (breaches)
Initial access vector breakdown	Exploitation of vulnerabilities (42%), Credential abuse (14%), Phishing (9%) (breaches)
Other metrics	Third-party (68%), Human element (58%) (breaches)

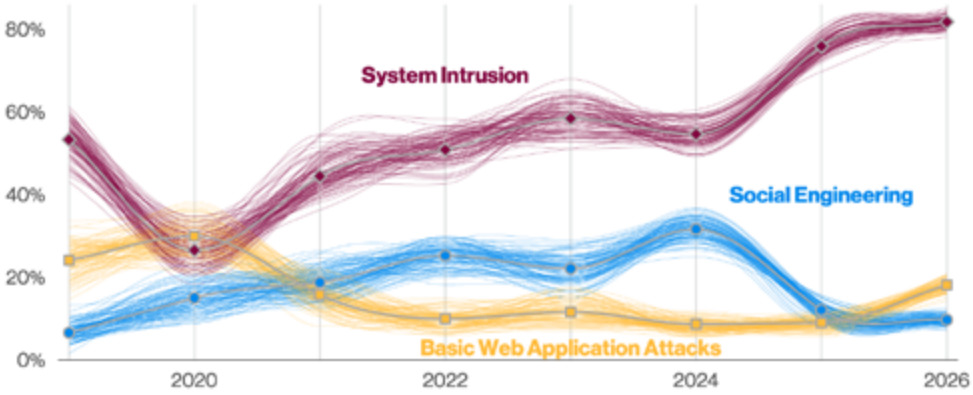

Figure 9. Top patterns in Retail breaches over time (n for 2026 dataset=806)

I have a coupon code.

Few shoppers can resist a good deal. This is also true of attackers, and they have been compromising systems like they were on final clearance.

This year, the number of incidents rose slightly, but the number of breaches nearly doubled. Despite that, the top three patterns essentially remain the same as last year, just in a different order. System Intrusion still leads, while Basic Web Application Attacks and Social Engineering continue to dance around each other.

As Figure 9 illustrates, it is not until you look all the way back to the 2020 DBIR that you see a change in the membership of the top three patterns. While they have shuffled about a bit on the stage, they have been close compatriots for several years. This consistency tells us that the same kinds of attacks are often being leveraged against this industry's infrastructure year after year – with a certain level of success. Case in point, this past year saw clothing retailer Hot Topic experiencing a breach affecting 57 million customers.[2] Clearly there remains significant incentive for attackers to target this sector, given the sheer volume of data up for grabs.

The unholy trio of Ransomware, Exploit vuln and Use of stolen creds figured prominently in the actions taken in this sector (Figure 10), and when combined with social attacks, you have accounted for the most prevalent ways in. Ransomware remains an ongoing problem across this industry and was the top malware action in breaches in this sector.

2. github.com/vz-risk/VCDB/issues/21205

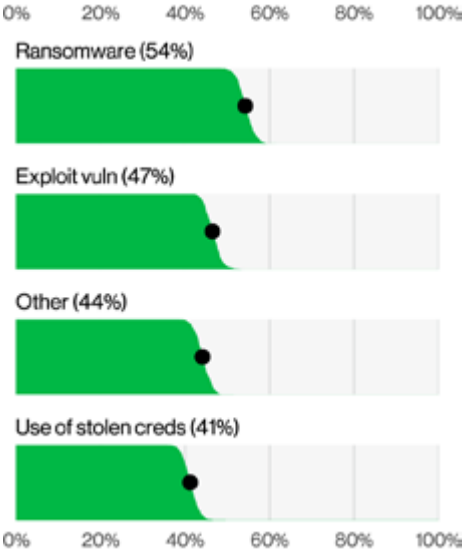

Figure 10. Top Action varieties in Retail breaches (n=719)

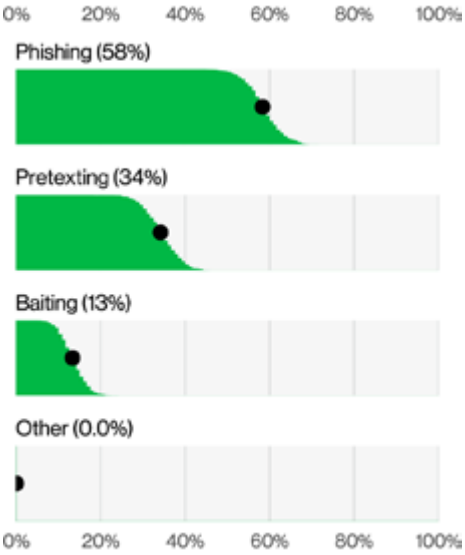

Figure 11. Top Social actions in Retail breaches (n=120)

The social varieties most commonly seen in these breaches have been Phishing and Pretexting, with the former almost twice as common as the latter, as seen in Figure 11. That makes some sense, since Phishing tends to be the lower-effort attack, where Pretexting tends to take a bit more time and skill to achieve a successful result (from the attacker's perspective). However, since both tactics have been quite successful for the attackers, it behooves organizations to have easy methods for people to report when they have become victims of these kinds of attacks.

Espionage-motivated actors increased again this year, rising from 9% to 19% of breaches where the motive was known. This suggests more sophisticated actors have taken notice of this sector and are turning their attention to what kinds of useful data their victims may have.

While this sector once saw primarily Payment card data compromised, threat actors have evolved and now target any data they can monetize, leading to a more diverse mix of data types being affected. Internal data, which can include plans, strategies and other information of value to Espionage-motivated attackers and ransomware actors looking for leverage rose from 65% last year to 84%. Figure 12 has the details.

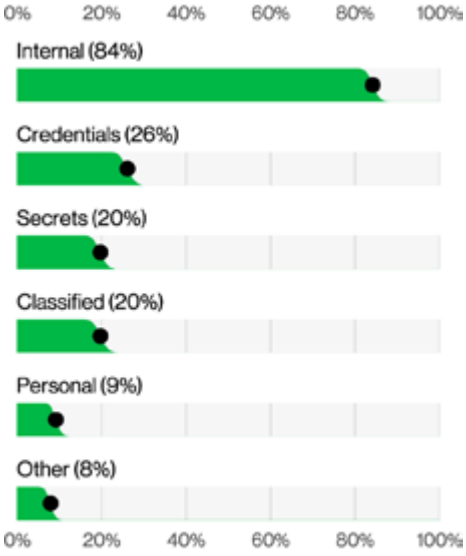

Figure 12. Top Data varieties compromised in Retail breaches (n=721)

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 2026 DBIR at verizon.com/dbir.

Want to make the world of cybersecurity a safer place?

If your organization aggregates incident or security data and you're interested in becoming a contributor or research partner to the annual Verizon DBIR (and we hope you are), the process is very easy and straightforward. Please email us at dbircontributor@verizon.com so we can discuss the details and make you a part of the DBIR research community.

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: github.com/vz-risk/veris.