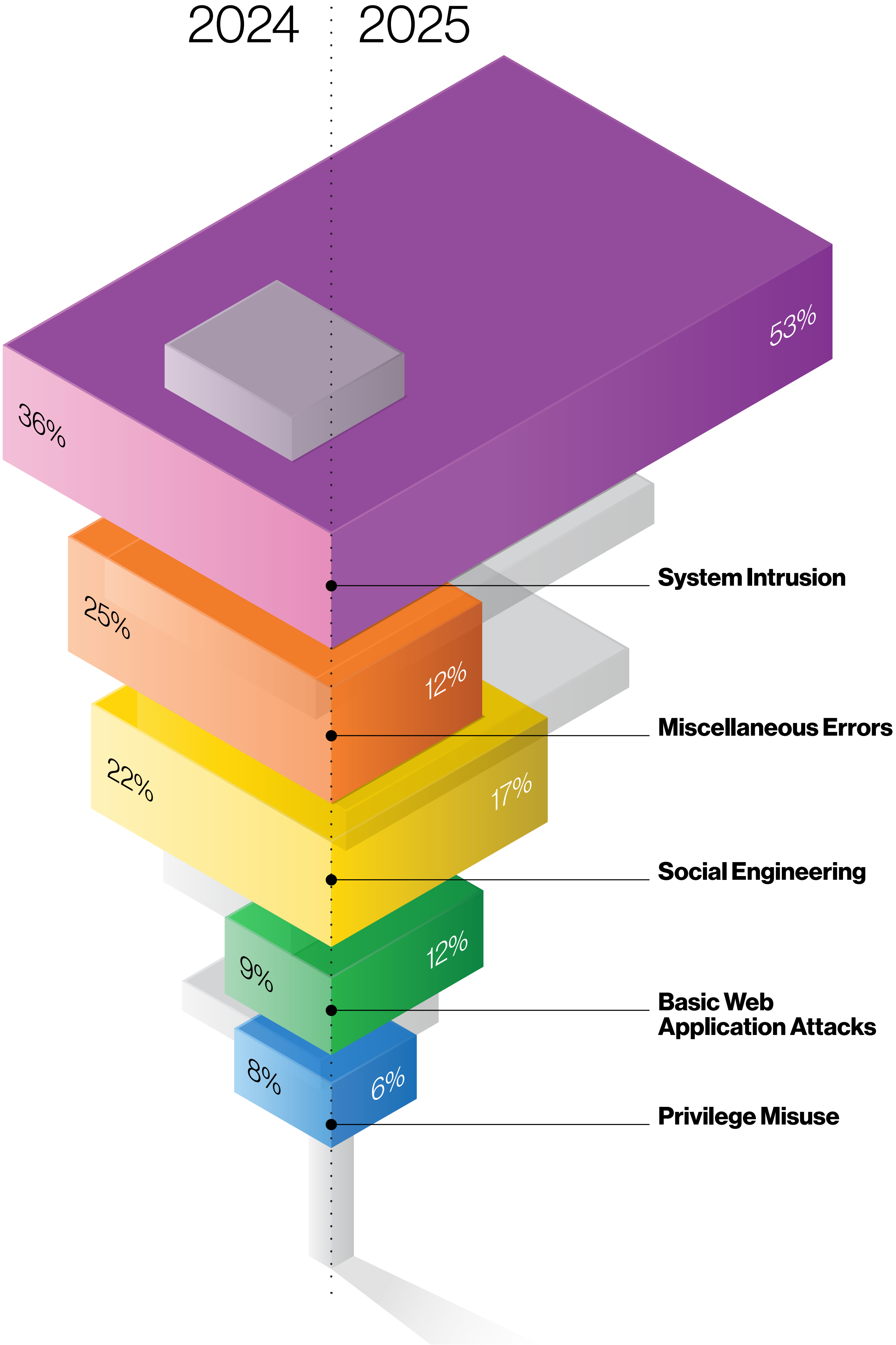
2025 Data Breach Investigations Report

Public Sector Snapshot

verizon


2024
2025
36%
53%
System Intrusion
25%
12%
Miscellaneous Errors
22%
17%
Social Engineering
9%
12%
Basic Web Application Attacks
8%
6%
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) Public Sector 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 organizations. 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 Public Administration (NAICS 92) sector—also known as the Public Sector—which includes establishments of federal, state and local government agencies as well as public safety agencies.

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 Public Sector (NAICS 92) is not indicative of 92 as a value. "92" is the code for the Public Administration 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

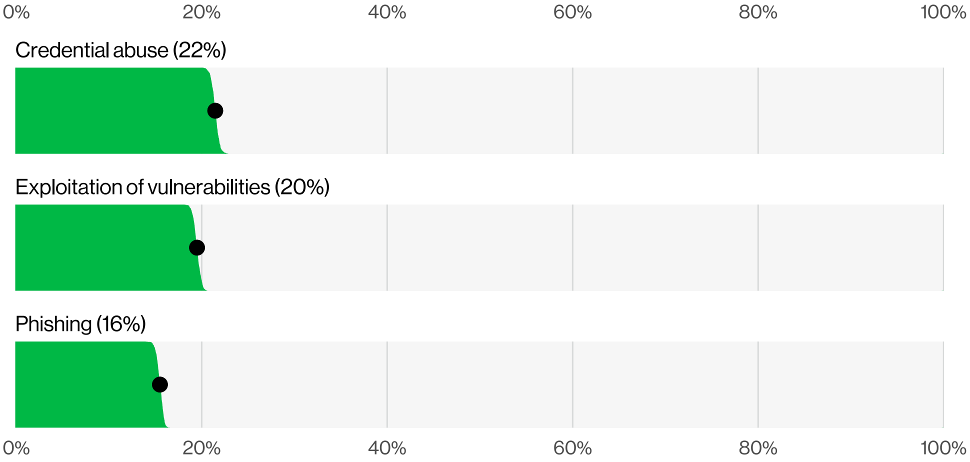


Figure 1. Known initial access vectors in non-Error, non-Misuse breaches (n=9,891)

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.

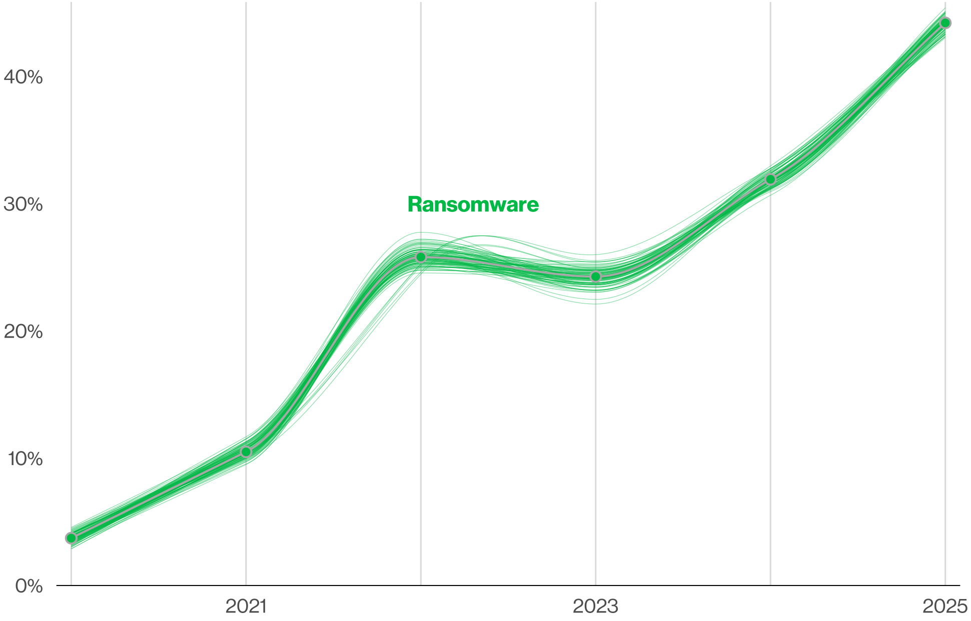


Figure 2. Ransomware action over time in breaches (n for 2025 dataset=10,747)

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.

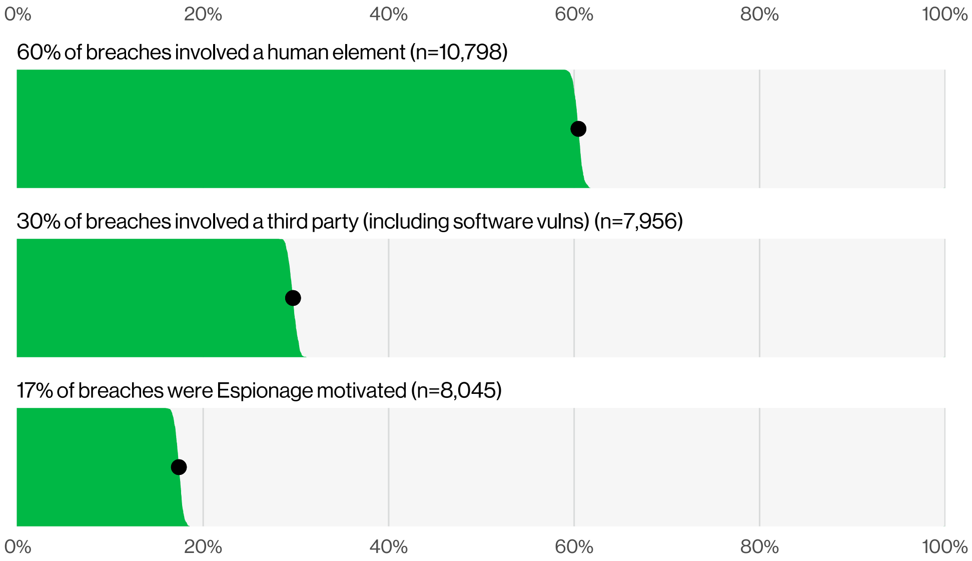


Figure 3. Select key enumerations in breaches

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.

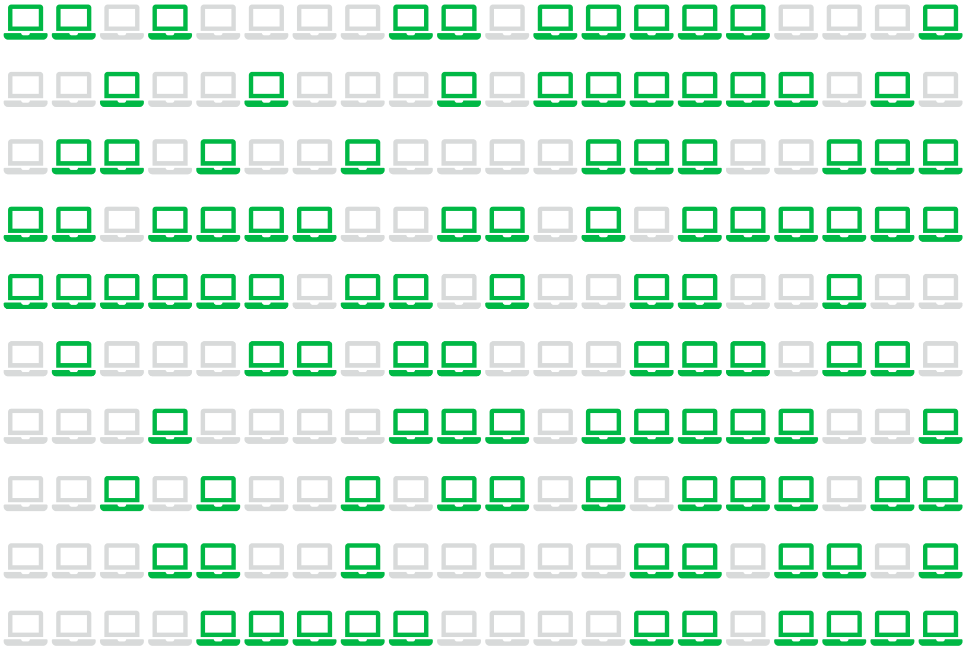


Figure 4. Percentage of non-managed devices with corporate logins in infostealer logs (each glyph is 0.5%)

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.

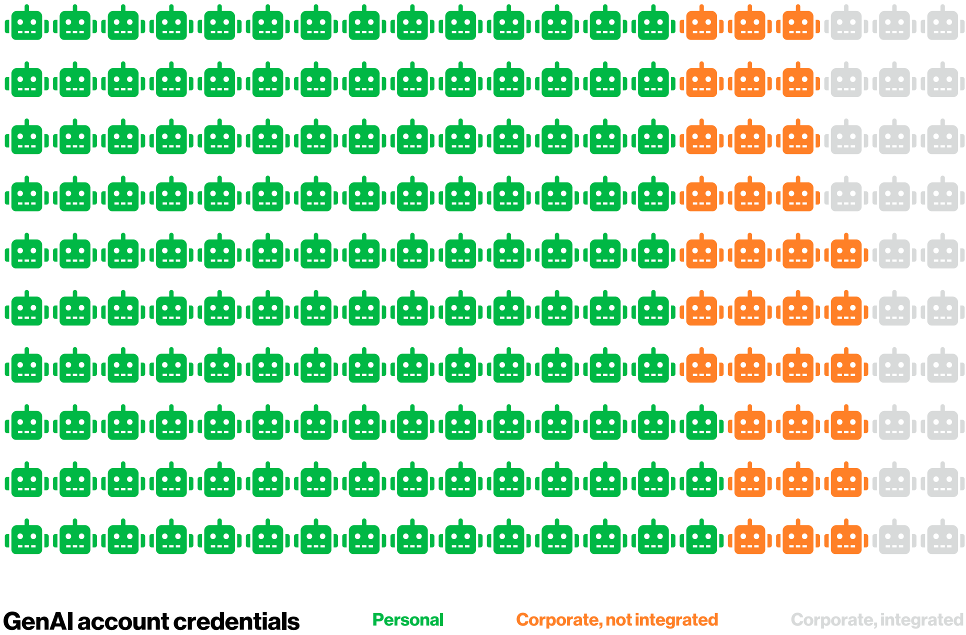


Figure 5. Percentage breakdown of GenAI service access account types (each glyph is 0.5%)

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.

Public Sector NAICS 92

Frequency	1,422 incidents, 946 with confirmed data disclosure
Top patterns	System Intrusion, Miscellaneous Errors and Basic Web Application Attacks represent 78% of breaches
Threat actors	External (67%), Internal (33%), Partner (1%) (breaches)
Actor motives	Financial (76%), Espionage (29%), Ideology (2%) (breaches)
Data compromised	Personal (47%), Internal (44%), Other (41%), Secrets (17%) (breaches)
What is the same?	This industry continues to be plagued by sophisticated attackers looking to gain access to the trove of data collected by governments about their constituents. Though the majority of breaches were from External actors, a significant number were from Internal actors making simple mistakes.

Summary

While we show a drop in reported incidents due to the makeup of contributors this year, the number of confirmed breaches remained steady. This means attackers are not easing up on government targets. Ransomware remains a major threat, hitting 30% of breaches across all levels of government. Errors remain a persistent issue, with Misdelivery in the lead.

Where have all the data points gone?

If you're a regular reader of this report, you may have noticed a significant change in the number of incidents being reported in this industry from prior years. This is largely due to one of our reliable data contributors not being able to participate this year.

Although we really hope to welcome them back next year, it is interesting to see that while the number of incidents (that violated one of the three tenants of the CIA Triad) is considerably lower, the number of confirmed breaches didn't change all that much. We've said before that we get the "what," but we do not always get the "why" in our data. One possible explanation for the number of breaches remaining close to last year's is simply that some of our other partners had sufficient visibility into breaches to keep us at or near previous levels.

Whatever the case, we assure you that the decreased number of incidents does not indicate that attackers are giving the government (of any country) a free pass.

Our top three patterns have seen a change from last year (Figure 6). In first place is the System Intrusion pattern, where all the complex attacks live (including everyone's favorite: Ransomware). Last year, people in the government making mistakes caused the most breaches, but this year, they're getting compromised through Basic Web Application Attacks instead, which almost everyone can agree is not an improvement.

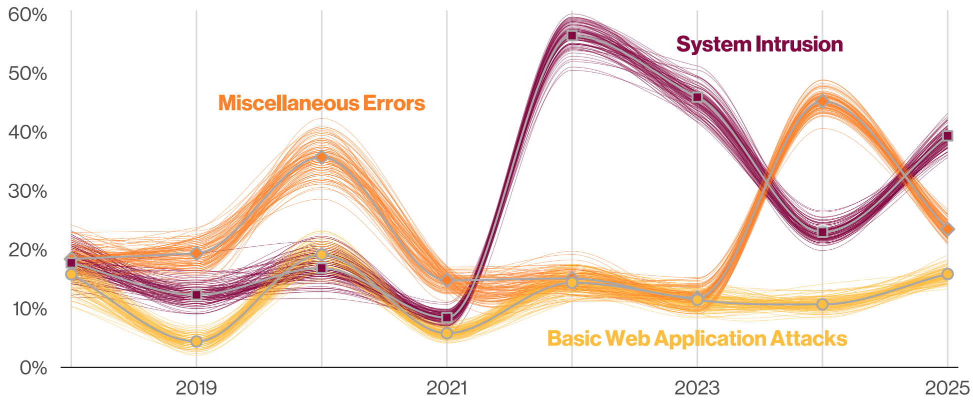


Figure 6. Top patterns over time in Public Sector breaches

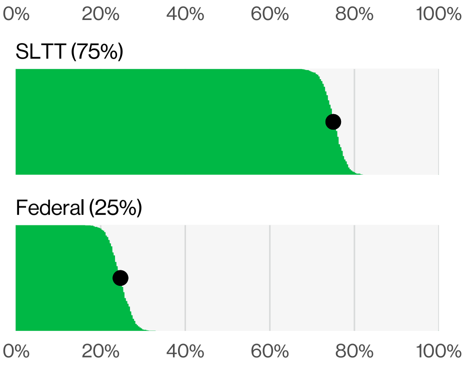


Figure 7. Ransomware victims by government level (n=312)

Speaking of Ransomware, it was present in 30% of breaches in this sector. When we look at our data in Figure 7, we see that Actors have been targeting government organizations large and small. We see that about 43% of Ransomware victims represent local governments in the U.S. in locations such as the Southeast and Midwest. Councils are also being targeted across the world, notably in Europe, Middle East and Africa (EMEA). Lest you think county-level governments (which fall into our Regional category) are immune, we have seen several examples of counties being victimized, as well. It continues at the state and federal levels, as well, and the real story here is that not only are these government entities being targeted, but they are also the favorite of certain ransomware gangs.

What we are saying here is that Ransomware is not a problem that is getting smaller in this sector. There is no real possibility of going unnoticed because your public entity is relatively obscure outside of your immediate area. These Actors are out there, and they are actively searching for soft targets they can monetize.

Mix up your errors— it keeps things interesting.

We had quite the shakeup in order of ascendance this year, and the pattern in the number two spot, Miscellaneous Errors, was at the top of the list in the 2024 report.

You can see in Figure 8 that the top error varieties are Misdelivery, Misconfiguration and Classification errors. Misdelivery is a particular problem for entities such as governments who do mass mailings to their constituents. When the contents and the envelopes get out of sync in such large deliveries, many people end up knowing more about strangers than they wanted. At least these kinds of breaches are less likely to result in subsequent fraud.

Misconfigured datasets are still being found by security researchers out on the internet without protective controls. It seems no matter how the vendors configure the defaults, some people will still manage to turn off the basics for convenience's sake.

A Classification error is when data is thought to be of low sensitivity and actually is not. We see this in cases in which data is marked as not being sensitive and, thus, not requiring such stringent controls, but in reality, the data was covered by laws requiring data breach notification, and so we find out about the breach. We understand, data classification can sometimes be seen as a very boring art, but it is necessary. People are making decisions on what uses to put the data to and how it should be handled based on how it is classified, so missteps can cause major issues for the organization.

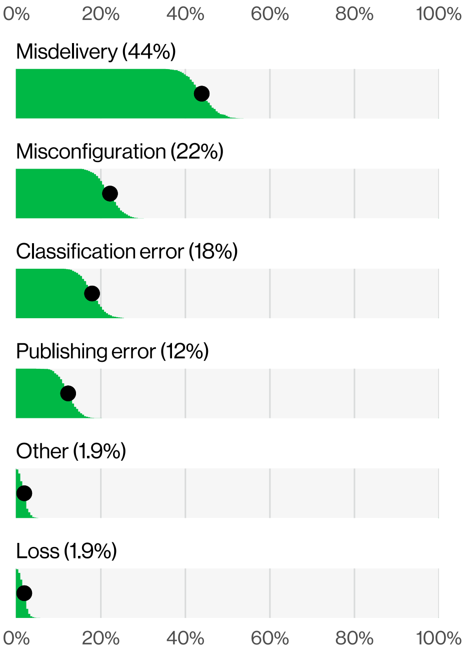


Figure 8. Top Error varieties in Public Sector breaches (n=212)

Last place brought a friend.

We had a bit of a surprise in the third place slot for patterns this year. The Social Engineering and Basic Web Application Attacks patterns were too close to call, so they will have to share the dubious distinction of third place. With regard to Social Engineering, Phishing is the tried-and-true favorite action variety, but we also saw Prompt bombing (Figure 9) newly rising in this year's data. If you're not familiar with the term, we only added it to VERIS in 2023, and it is the technique of sending annoying levels of authentication requests to users in the hopes they will just comply to make them go away. Is this a case of "if you track it, they will come"? We aren't sure, but we did see a number of cases in which this is the tactic that ultimately succeeded.

Not only do you have to worry about people reusing their passwords (which remains a huge problem), but they are also susceptible to this kind of attack on your multifactor authentication controls. Prompt bombing has been successful in more than 20% of Social attacks this year, so this would be a good thing to add to your training materials.

Basic Web Application Attacks feature several hacking varieties prominently: Use of stolen creds at 86%, Exploit misconfig at 45% and Brute force at 37%. These attacks frequently play out very quickly with few steps required for the attacker to gain access and abscond with their data prize.

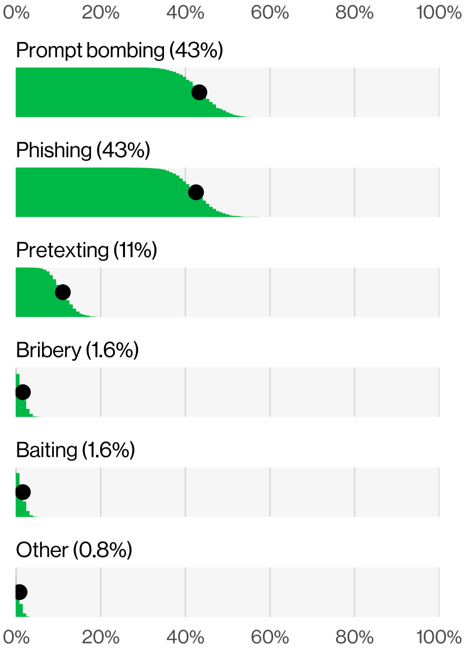


Figure 9. Top Social actions in Public Sector breaches (n=127)

The way we were: A five-year Public Sector retrospective

Some time ago—well, at least five years ago—we started breaking down the Public Sector data in our dataset by recording which level of government the victim belonged to—Federal versus State, Local, Territorial or Tribal (SLTT). By doing so, we now have enough data to look at how these different entity sizes are experiencing breaches. We have provided you with data from the past five years that shows not only how the different levels of government organizations experience breaches but also what kinds of Actors choose to target this space. Certainly we have seen both Federal- and SLTT-targeted attacks increase over time, with some very prominent ransomware cases wreaking havoc among multiple victims. Some of these Actors seem to prefer SLTT targets, in fact. However, the Federal level of government attracts its own threat actors, which means nobody is immune, and the most you can hope to achieve is to mitigate your most common actors and the actions they take. Read on for help in those areas.

Federal

Frequency	15,799 incidents, 848 with confirmed data disclosure
Top patterns	System Intrusion, Lost and Stolen Assets and Miscellaneous Errors represent 81% of breaches
Threat actors	External (66%), Internal (46%), Multiple (11%) (breaches)
Actor motives	Financial (63%), Espionage (33%), Ideology (5%) (breaches)
Data compromised	Personal (66%), Other (38%), Internal (34%), Secrets (13%) (breaches)

One finding that immediately jumped out at us is that we have fewer breaches at the Federal level than we do at the SLTT level. You may be looking at this data and wondering "Why is there so little if this is a five-year retrospective?" The answer is simply that sometimes our data comes without an indication of what government level the breached entity was, and because we don't get the victim organization's name (except from the publicly disclosed sources), we can't make that determination. Another factor is that there are far fewer entities at the Federal level than there are at the regional levels and below. We in the U.S. have our federal government, which is huge with all its various branches, but then you have to factor in the state, county and city levels. The further down the ladder you go, the more targets there are.

Figure 10 is showing the cases where we did know the government level of the victim, and these were at the Federal level.

Also keep in mind that these do not exclude the breaches of non-U.S. governments—while the dataset is dominated by the Northern American regional breaches, it includes breaches reported from any country.

We also noticed that the top three patterns for both organizational sizes were not only identical in makeup but also in ranked order. Now contrast this finding with the same graphic for the full Public Sector dataset for this year's report (Figure 6 on page 12). Although it does show the same top two patterns this year, it was not the case when you look backwards in time. In a retrospective view, you can see other patterns gain ascendancy for a time and then fall back down. This is expected variation between this smaller subset of known Federal-level breaches as compared to all government sector data.

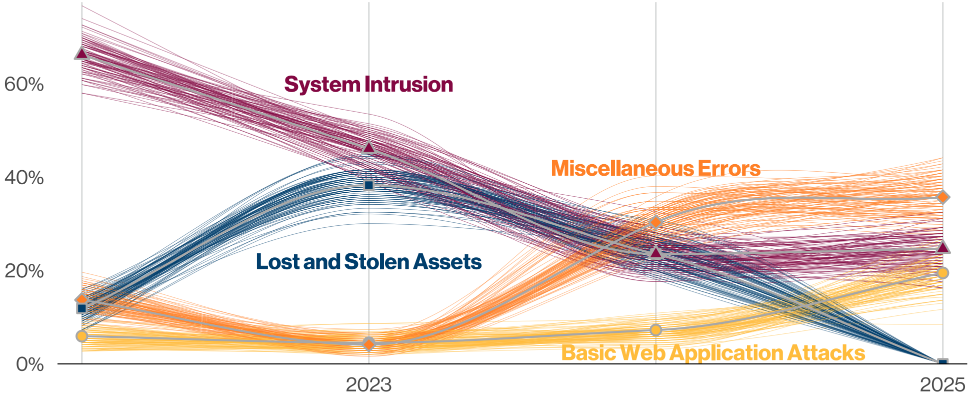


Figure 10. Top patterns over time in Federal Public Sector breaches

State, Local, Territorial and Tribal (SLTT)

Frequency	2,101 incidents, 1,341 with confirmed data disclosure
Top patterns	Miscellaneous Errors, System Intrusion and Basic Web Application Attacks represent 79% of breaches
Threat actors	External (55%), Internal (45%), Partner (1%) (breaches)
Actor motives	Financial (96%), Espionage (1%), Ideology (1%), Convenience (1%) (breaches)
Data compromised	Personal (83%), Other (29%), Internal (21%), Credentials (12%) (breaches)

While the top three patterns in the SLTT breaches are similar in makeup,[1] we did have more variation in the earlier years, as shown by the fuzziness of the potential lines in Figure 11. If you aren't familiar with how to read a spaghetti chart, each line represents a potential path the data took, and the tighter the grouping of lines, the higher the confidence. Back in 2019 and 2020, there were wider pathways than there are as we approach the present day, so the data has become easier to estimate with a higher confidence as to accuracy. Contrast that with the pathways in the Federal breaches, and you see there was a tighter configuration of the data even early on in the recording.

The true takeaway in this is that even when we break out the data based on how large the attacked entity was, we still see the same top three patterns over time. This highlights the need to have your controls (both protective and detective) in place for these three patterns as a critical path to helping your organization take care of the data entrusted to it by the constituents it represents.

The Multi-State Information Sharing and Analysis Center (MS-ISAC) is a trusted cybersecurity resource for more than 18,000 U.S. SLTT governmental organizations and has been around since the early 2000s. Part of the cybersecurity resources provided to MS-ISAC members is the Nationwide Cybersecurity Review (NCSR), which helps organizations assess their overall cybersecurity posture based on the NIST Cybersecurity Framework. As part of this assessment, the MS-ISAC found that 70% of NCSR respondents selected "Lack of sufficient funding" as a top security concern and that 80% of NCSR respondents had security staffing of fewer than five. Considering the frequent opportunistic and targeted attacks impacting SLTT, the limitations in staffing and budget to defend against attacks can affect all of our private data.

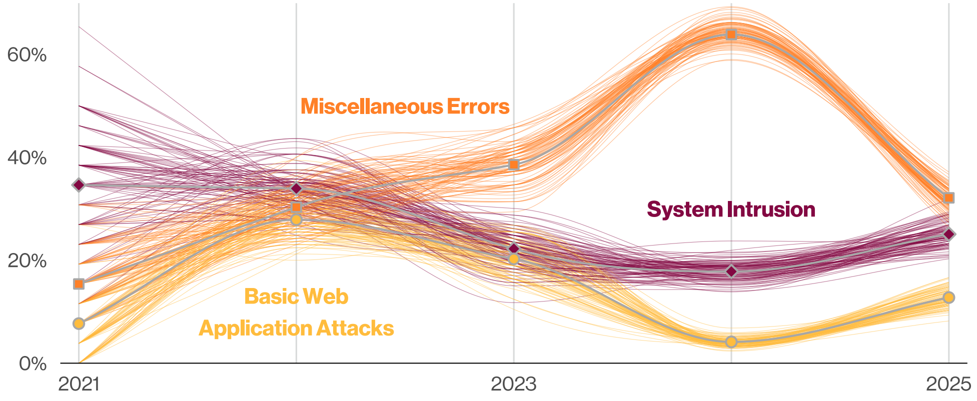


Figure 11. Top patterns over time in SLTT Public Sector breaches

[1] https://www.cisecurity.org/ms-isac

Comparative analysis

Figure 12 shows the breakdown of the action varieties between Federal and SLTT over the past five years. You can see that the Use of stolen credentials is one of the overall favorite initial access vectors for both levels of government, but as we go into the lower bars of the graph, we do start to see some differences. Several of these overlap sufficiently to make it clear they are all favored tools in the attackers' collections.

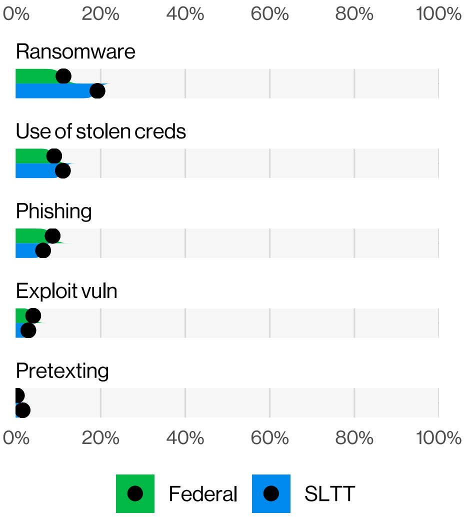


Figure 12. Top Action varieties in breaches by government level (2020–2025) (n=544)

We have some more marked differences looking at the patterns for the same time period (Figure 13). While System Intrusion is a clear favorite for Federal, Miscellaneous Errors was equally popular in the SLTT segment. The contrast between assets being lost and stolen in the different segments was also pronounced.

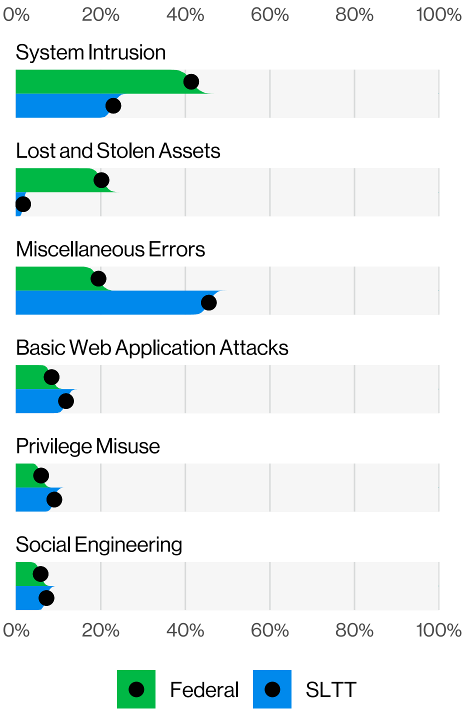


Figure 13. Top patterns in breaches by government level (2020–2025) (n=2,189)

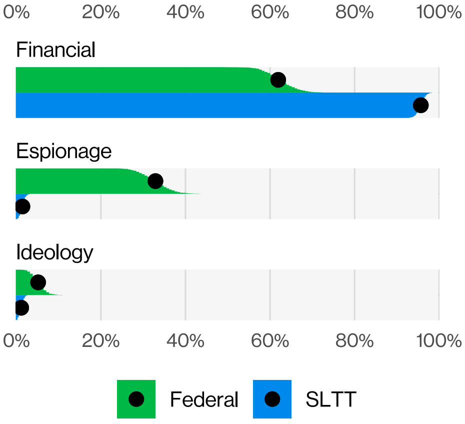


Figure 14. Top Actor motives in breaches by goverment level (2020–2025) (n=501)

Finally, take a look at Figure 14, where we show the motivations of the attackers. Though we expect Financial to be the top motive, the prevalence of Espionage-motivated actors targeting the Federal level was significant, as well. It stands to reason that the Actors would be targeting the highest level of government more frequently than the regional or local entities. These actors, if not directly state-sponsored, are usually at least somewhat supported or condoned in their goals of gaining access to sensitive government data. Targeting smaller organizations would be less likely to gain them access to the types of data they prefer—namely those data points useful for espionage on a grander scale. As mentioned in previous sections, the uptick in Espionage-motivated breaches is likely (at least in part) due to our increased visibility with the data contributor mix.

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.