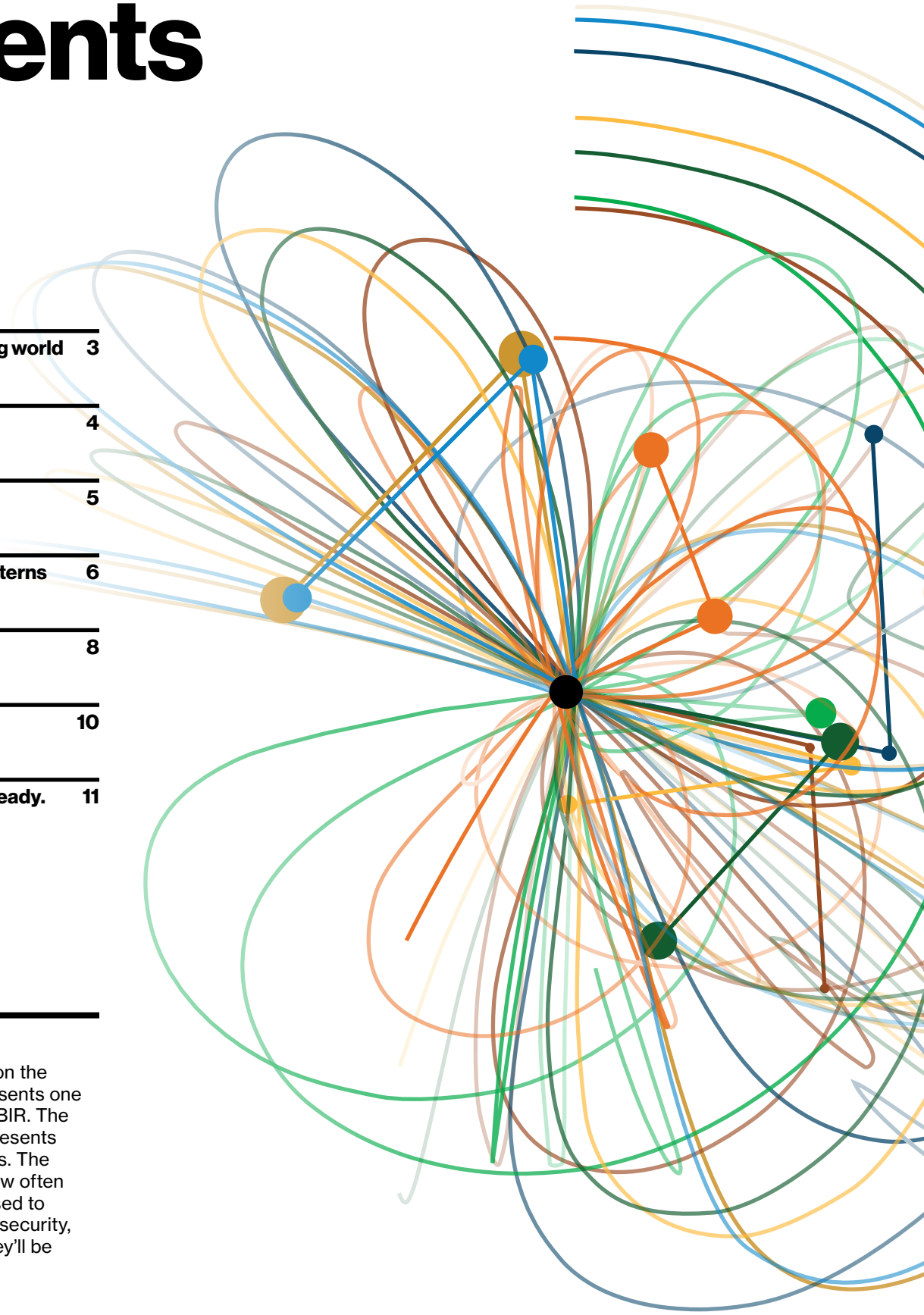
DBIR

2021 Data Breach Investigations Report

Public Sector snapshot

verizon

Table of contents



About the cover

There are eight pendulums on the cover. Each pendulum represents one of the new patterns in the DBIR. The weight of the pendulum represents how often the pattern occurs. The length of the pendulum is how often they are breaches, as opposed to simply incidents. Just like in security, it's hard to predict where they'll be in the future.

Staying ready in a changing world

Changes in the real world often occur rapidly, and they rarely give advanced notice of their arrival. Organizations are forced to react quickly and to make decisions on their security stance accordingly. The wisest decisions are informed decisions. While no one can accurately predict the threats organizations may have to face next month or next year, they can discern what eventualities are most probable and prepare for those. That is why we create the Verizon Data Breach Investigations Report (DBIR). This year's report is the 14th iteration and is powered by 83 contributing organizations—the highest number yet. The DBIR team analyzed 29,207 real-world security incidents, of which 5,258 were confirmed breaches, to create the 2021 DBIR.

This year we have updated the DBIR patterns (now seven in number) using machine learning clustering. This resulted in the creation of two completely new patterns—Social Engineering and System Intrusion—along with an overhaul of Basic Web Application Attacks and the recalibration of Denial of Service, Lost and Stolen Assets, Miscellaneous Errors, and Privilege Misuse, plus Everything Else. We continue to highlight specific industries (12 of them), including the public sector.

Read on for public sector and overall report highlights. Please pass this summary along to colleagues and download the full report at verizon.com/dbir for a more detailed view of the threat landscape in 2021.

Getting better all the time

The DBIR team continues to work to expand and simplify the Vocabulary for Event Recording and Incident Sharing (VERIS) framework to classify and analyze incidents and breaches. We have developed an updated mapping to the latest version of the Center for Internet Security (CIS) Controls®, which were released earlier this year. We provide the top recommended CIS Controls from Implementation Group 1 (IG1) in each industry section to provide additional guidance on how to most effectively mitigate the risks faced by each vertical. We also used the mappings to boost our analysis and have made them available for use by the larger security community as well.

29,207

The DBIR team analyzed 29,207 incidents, of which 5,258 were confirmed breaches.

Industry labels

This snapshot highlights important takeaways for the Public Administration (NAICS 92) 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. Detailed information on the codes and classification system is available at

https://www.census.gov/naics/?58967?yearbck=2012

Summary of findings

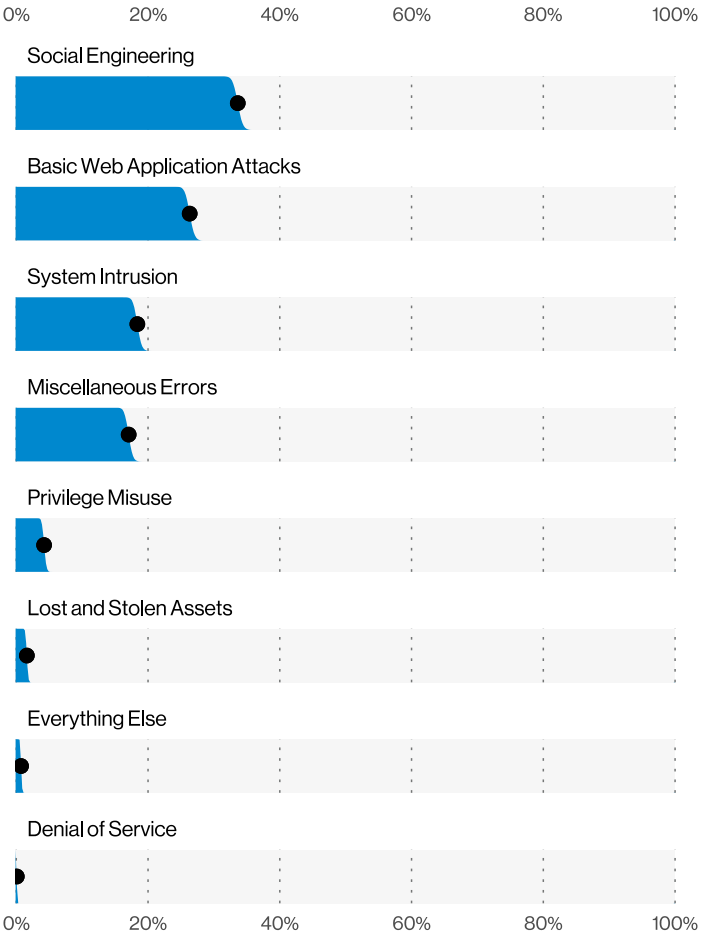


Figure 1. Patterns in breaches (n=5,275)

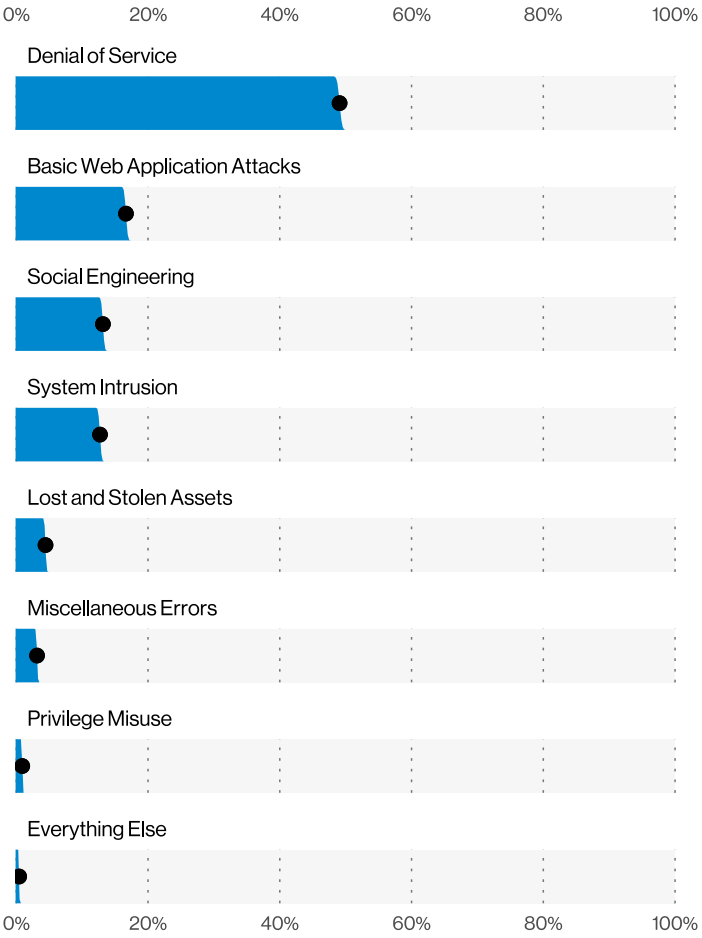


Figure 2. Patterns in incidents (n=29,206)

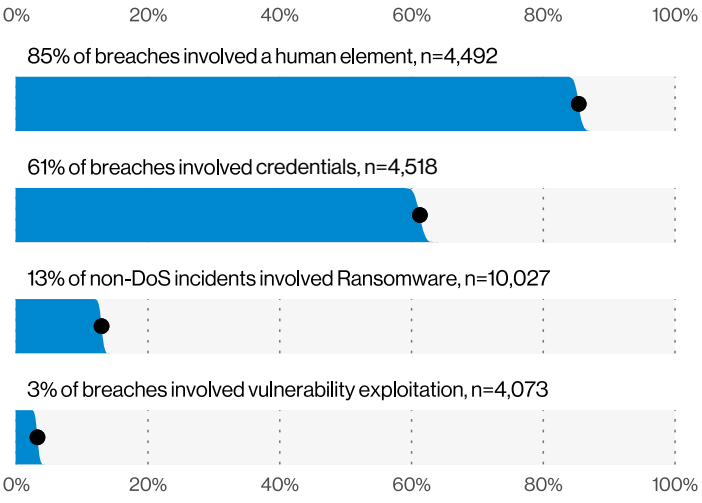


Figure 3. Select action varieties (n=4,073)

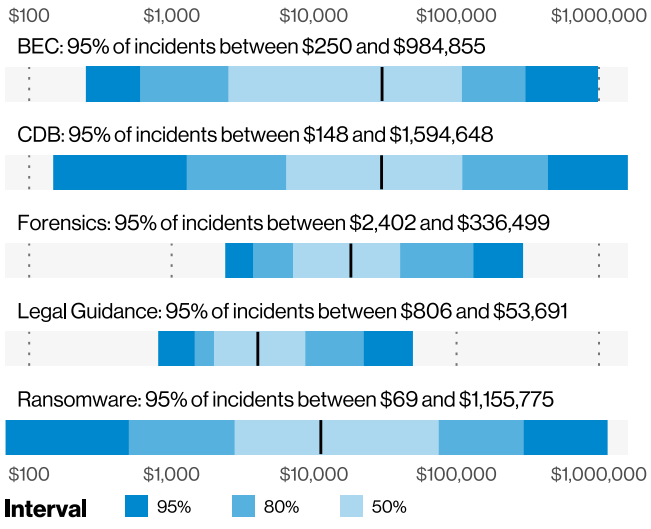


Figure 4. Select impacts of incidents

Key takeaways

Ransomware is still on the rise.

Ransomware appears in 10% of breaches—more than double the frequency from last year. This upward move was influenced by new tactics, where some ransomware perpetrators now steal the data as they encrypt it. That puts Ransomware now in third place among actions causing breaches.

Vox populi...(might have said too much).

Eighty-five percent of breaches involved the human element. Phishing was present in 36% of breaches in our dataset, up from 25% last year. Business Email Compromises (BECs) were the second most common form of Social Engineering. This reflects the rise of Misrepresentation, which was 15 times higher than last year.

Errors were (slightly) less of a problem.

Errors decreased last year as a percentage of breaches (from 22% to 17%), although they increased in absolute terms from 883 to 905 breaches. This breaks a three-year streak in Errors percentage either growing or remaining consistent.

Attackers still like your web apps.

Attacks on web applications continue to be high. They are the main attack vector in Hacking actions, with more than 80% of breaches. In addition, Desktop sharing has moved into second place in Hacking vectors.

Mostly cloudy

Compromised external cloud assets were more common than on-premises assets in both incidents and breaches. Conversely, there was a decline of user devices (desktops and laptops) being compromised. This makes sense when we consider that breaches are moving toward Social and Web application vectors, such as gathering credentials and using them against cloud-based email systems.

What's the password?

Some things never seem to change: Breaches, as always, continue to be mostly due to external, financially motivated actors. And 61% of breaches involved credential data.

That was quite a year.

In August 2020, we speculated that COVID-19 would lead to an increase in Phishing, Ransomware, Errors and Use of stolen credentials on web applications. In the 2021 DBIR we found we were partially correct: Phishing increased by 11% and Ransomware increased by 6%. But the Use of stolen creds and publishing errors stayed consistent with last year (1% and -0.5% respectively), while Misconfiguration and Misdelivery decreased as a percentage of errors (-2% and -6% respectively).

Breaches have price tags.

This year we attempted a deeper analysis of the impact of breaches on organizations. Using loss data, insurance cost data and stock price data, we have modeled the range of losses due to incidents.

The good news? Fourteen percent of simulated breaches had no impact. But don't count on that for your organization's security plan. The median for incidents with an impact was $21,659 with 95% of incidents falling between $826 and $653,587.

Incident Classification Patterns

The DBIR first introduced the Incident Classification Patterns in 2014 as a useful shorthand for scenarios that occurred very frequently. The threat landscape has changed a bit since then, so this year we are excited to introduce a refresh of the DBIR patterns.

The new patterns are based on an elegant machine learning clustering process. These new patterns better capture complex interaction rules that the old ones were unlikely to handle, and they are much more focused on what happens during the breach. That makes them better suited for control recommendations, too.

The updated patterns explain 95.8% of analyzed breaches and 99.7% of analyzed incidents over all time.

Here are our key findings from each pattern.

Social Engineering	Psychological compromise of a person, which alters their behavior into taking an action or breaching confidentiality	Social attacks as a pattern have continued to increase since 2017, with Business Email Compromise (BEC) breaches doubling again since last year. Web-based email is a favorite target. • More than 80% of breaches are discovered by external parties • Phishing templates have a wide range of click rates, from no clicks to click rates over 50% • In a sample of 1,148 people who received real and simulated phishes, none of them clicked the simulated phish, but 2.5% clicked the real phishing email
Basic Web Application Attacks	Simple web application attacks with a small number of steps or additional actions after the initial web application compromise	We redesigned the Basic Web Application Attacks pattern to capture what had been hiding in web application-focused errors, social engineering and system intrusions. The attacks were largely against cloud-based servers that were hacked via the Use of stolen credentials or brute force attacks. • 95% of organizations suffering credential stuffing attacks had between 637 and 3.3 billion malicious login attempts throughout the year • The Information industry overtook the Finance industry as the most common target of botnet attacks on customers this year

System Intrusion	System Intrusion captures the complex attacks that leverage Malware and/or Hacking to achieve their objectives, including deploying ransomware.	The creation of this new pattern and its placement (tied with Miscellaneous Errors in breaches at the number three spot, behind Social Engineering and Basic Web Application Attacks) provides clarity to organizations trying to understand how much to invest in preventing advanced threats. • More than 70% of cases in this pattern involved Malware and 40% involved Hacking actions • 99% of Ransomware cases fell into this pattern
Miscellaneous Errors	Incidents where unintentional actions directly compromised a security attribute of an information asset. This does not include lost devices, which is grouped with theft instead.	Miscellaneous Errors decreased as a percentage of breaches. This was not due to a decrease in Errors, however, but because of an increase in other types of breaches. • Misconfiguration was by far the most common form of error (approximately 52%) • The vast majority of the time, when known, Security researchers (80%) were responsible for discovery • Personal data was the most commonly exposed data type in this pattern
Privilege Misuse	Incidents predominantly driven by unapproved or malicious use of legitimate privileges	Privilege Misuse continues to decrease as a percentage of breaches, thus underscoring the lower incidence of malicious insider threats compared to other patterns. • 70% of breaches in this pattern were due to Privilege abuse • More than 30% of incidents take months or years to discover
Lost and Stolen Assets	Any incident where an information asset went missing, whether through misplacement or malice	Error (in the form of loss of an asset) is more common than theft of assets, and employees discovering issues is the most common way incidents come to light. Increasingly, people lose devices rather than documents or other media.
Denial of Service	Attacks intended to compromise the availability of networks and systems. Includes both network and application layer attacks.	Distributed Denial of Service (DDos) attacks are highly unevenly distributed (spikey), making them difficult to predict. Instead, this requires organizations to plan for the percentage of DDoS attacks they want to be able to handle (50%, 80%, 95% or more).
Everything Else	This last pattern isn't really a pattern at all. Instead, it covers all incidents that don't fit within the orderly confines of the other patterns.	The former Payment Card Skimmer pattern ended up here. There were only 20 skimming incidents (all confirmed breaches) in the dataset this year. • This year, three of the rarely seen Environmental-caused breaches were added and are included in this pattern given their relative rarity • The reclustering of the patterns allowed us to explain an additional 18% of breaches that would have otherwise fallen into this pattern

Public Administration

Summary

What follows is a summary of our findings in the public sector. By far the biggest threat in this sector is the Social Engineer. Actors who can craft a credible Phishing email are absconding with Credentials at an alarming rate.

Frequency	3,236 incidents, 885 with confirmed data disclosure
Top Patterns	Social Engineering, Miscellaneous Errors and System Intrusion represent 92% of breaches
Threat Actors	External (83%), Internal (17%) (breaches)
Actor Motives	Financial (96%), Espionage (4%) (breaches)
Data Compromised	Credentials (80%), Personal (18%), Other (6%), Medical (4%) (breaches)
Top IG1 Protective Controls	Security Awareness and Skills Training (14), Access Control Management (6), Account Management (5)

The Social Engineering pattern was responsible for more than 69% of breaches in this sector (Figure 5). Clearly, Public Administration is a favorite among the phishing fiends. The Social actions were almost exclusively Phishing, with email as the vector (Figure 6). Pretexting was rarely leveraged at all, and why should they go to all the work of inventing a scenario when a straight-up phish gets the job done?

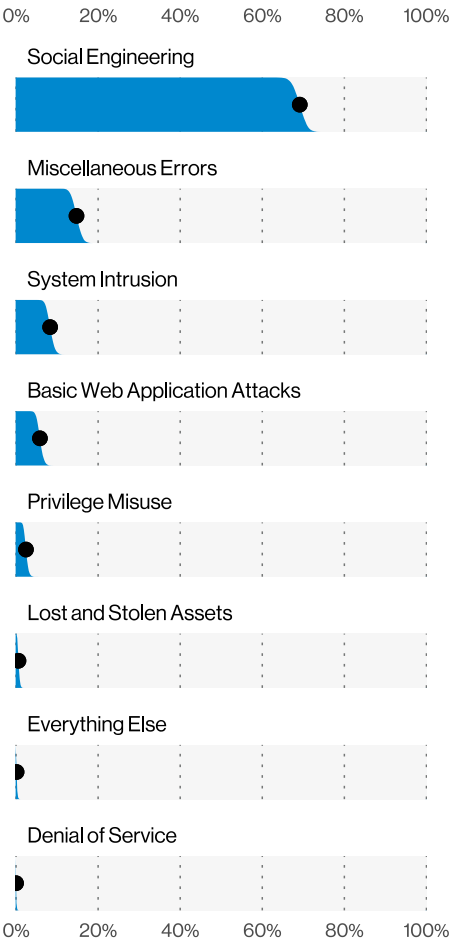


Figure 5. Patterns in Public Administration breaches (n=885)

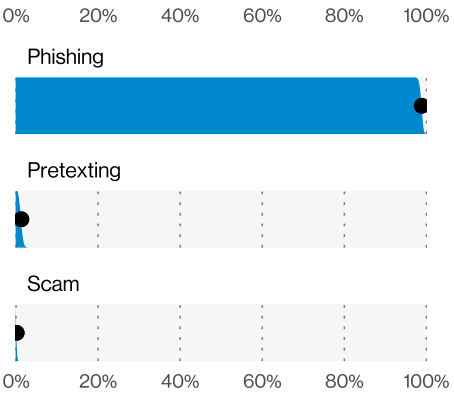


Figure 6. Social varieties in Public Administration breaches (n=611)

The Miscellaneous Errors pattern was a far distant second and consisted of Misconfiguration (although not usually found by Security researchers—which was a surprise, as that is the most common pairing) and Misdelivery (Figure 7). Certainly, government entities are responsible for a lot of mass mailings, and paper documents were the second most common assets that were delivered to the wrong recipient, with good old-fashioned emails taking first place.

The System Intrusion pattern rounds out our top three and is a combination of Hacking and Malware actions. We found the Use of stolen credentials followed by dropping Malware with either C2 or Ransomware capabilities to be the most common story in this pattern.

The most frequently stolen data type is Credentials, which are then used to further the attacker's presence in the victim's network and systems (Figure 8). After Credentials, Personal information is the top data type compromised where breaches were confirmed in this sector.

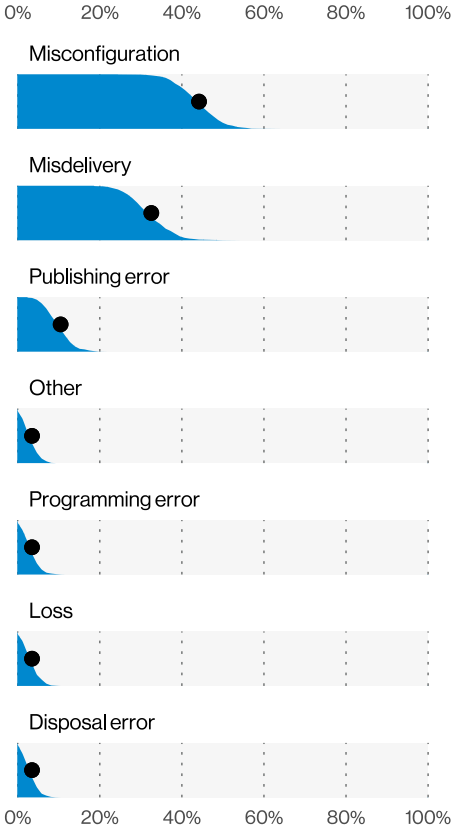


Figure 7. Top Error varieties in Public Administration breaches (n=86)

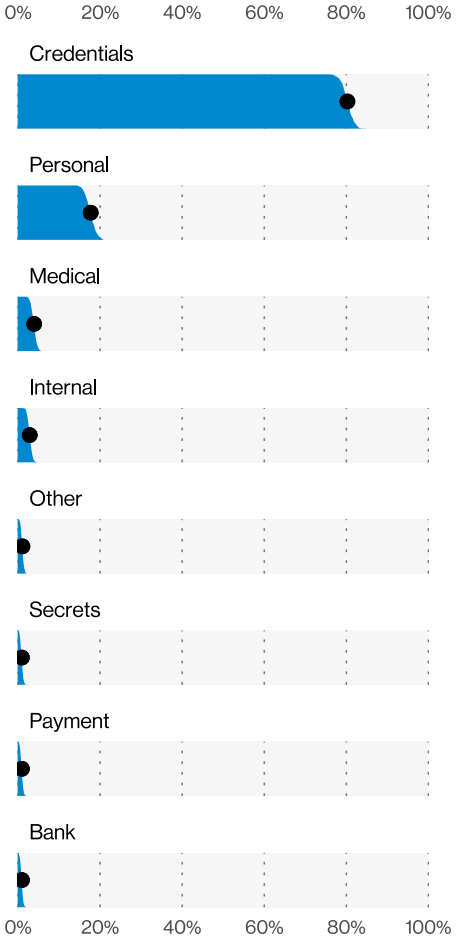


Figure 8. Top Data varieties in Public Administration breaches (n=841)

Best practices

This year we combined the newly updated CIS Controls with our own newly updated patterns to identify the core set of Controls that every organization should consider implementing regardless of size and budget.

Control 4: Secure Configuration of Enterprise Assets and Software

This Control is not only a mouthful, but it also contains many safeguards focused on engineering solutions that are secure from the outset rather than tacking security on later. Implementing this Control will help to reduce Error-based breaches such as Misconfiguration and Loss of assets through enforcing remote wipe abilities on portable devices.

Control 5: Account Management

While this is technically a new version 8 Control, it should be extremely familiar, as the subcontrols are simply a centralization of the previous account management practices that were found in a few of the previous Controls (e.g., Boundary Protect and Account Monitoring and Control). This control is very much targeted at helping organizations manage access to accounts and is useful against Brute force and credential stuffing attacks.

Control 6: Access Control

This Control is directly related to Control 5. Rather than simply looking at user accounts and managing access to those, you are also managing the rights and privileges. It calls for enforcing multifactor authentication on key components of the environment, which is a useful tactic against the Use of stolen credentials.

Control 14: Security Awareness and Skills Training

This control is a classic and hopefully doesn't need a great deal of explanation. Considering the high prevalence of Errors and Social Engineering, it is obvious that awareness and technical training is a smart place to invest some money to help support your team against a world full of cognitive hazards.

Stay informed and threat ready.

Successfully navigating through the cyberthreats facing government agencies today requires intelligence from a source you can trust. The full DBIR contains real-world details on the actors, actions and patterns that can help you to prepare your defenses and educate employees. Get the data-based insights you need to protect your organization.

Read the full 2021 DBIR at verizon.com/dbir

Want to make the world a better place?

The DBIR relies on contributions from dozens of organizations, and we'd love to have you. Become a contributor to next year's report, or provide us feedback for improving the DBIR at dbir@verizon.com, tweet us @VZDBIR and check out the VERIS GitHub page: https://github.com/vz-risk/veris

verizon