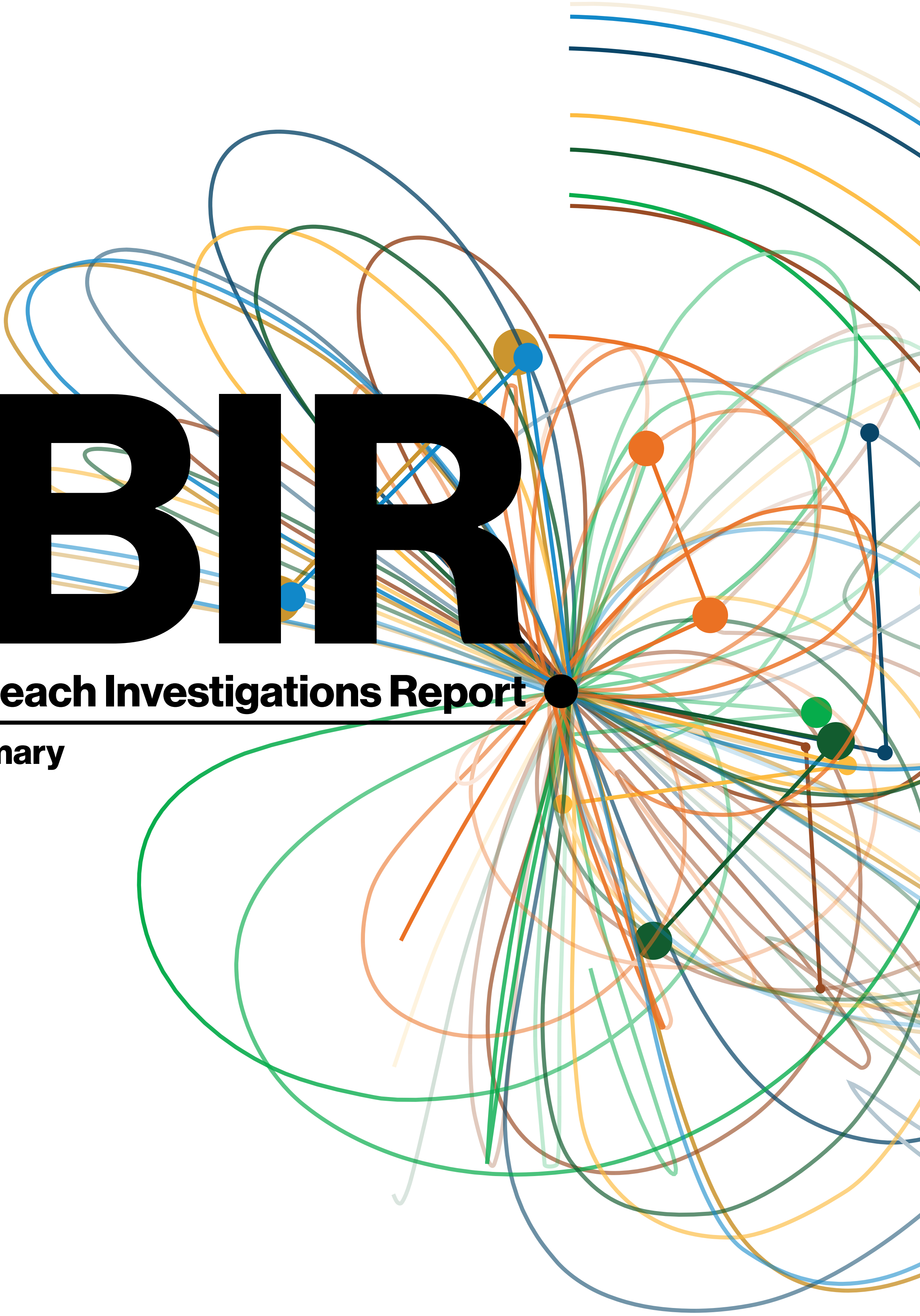
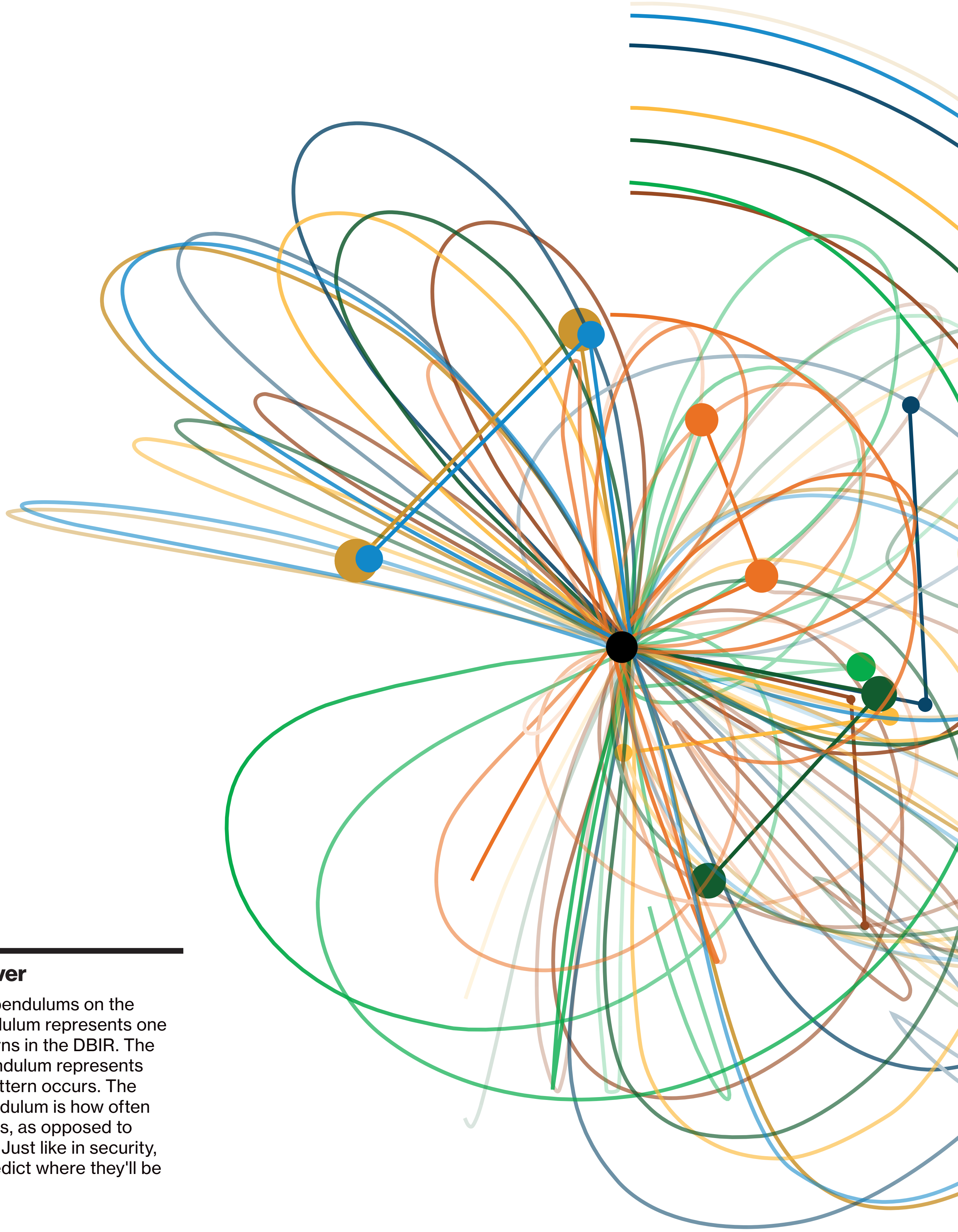
# DBIR

## 2021 Data Breach Investigations Report

### Executive Summary



verizon



## 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 difficult to predict where they'll be in the future.

# Table of contents

# 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 regarding 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, Privilege Misuse, plus Everything Else. We once again explore various parts of the globe in order to provide a regional analysis of breach trends. We continue to highlight specific industries (12 of them), and we also provide a glimpse into how small and medium-sized businesses (SMBs) compare and contrast with large enterprises with regard to threats.

Read on for 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.

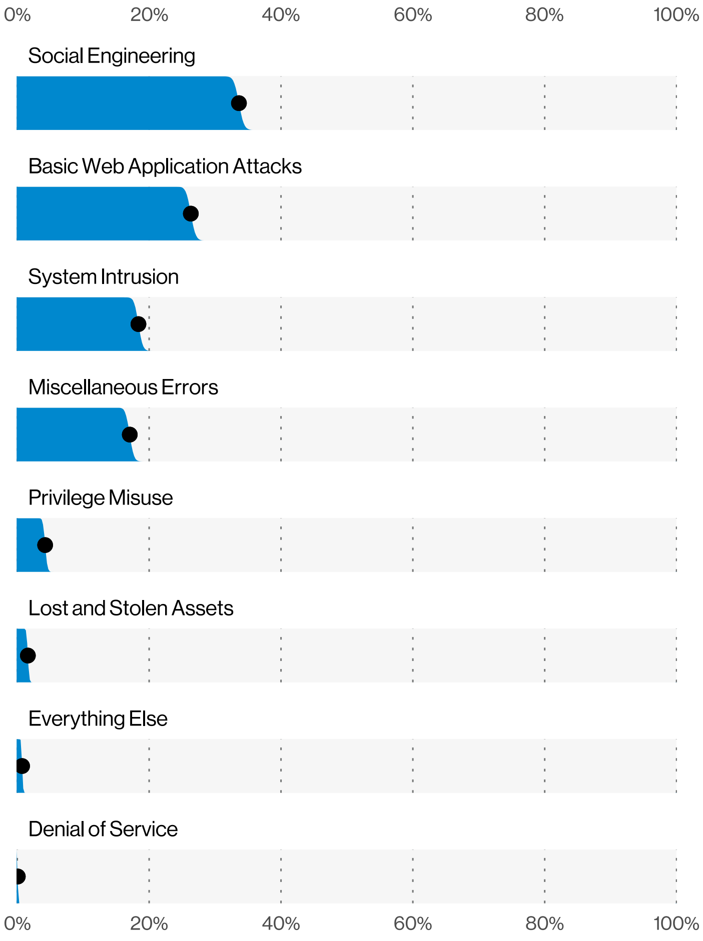
**29,207**

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

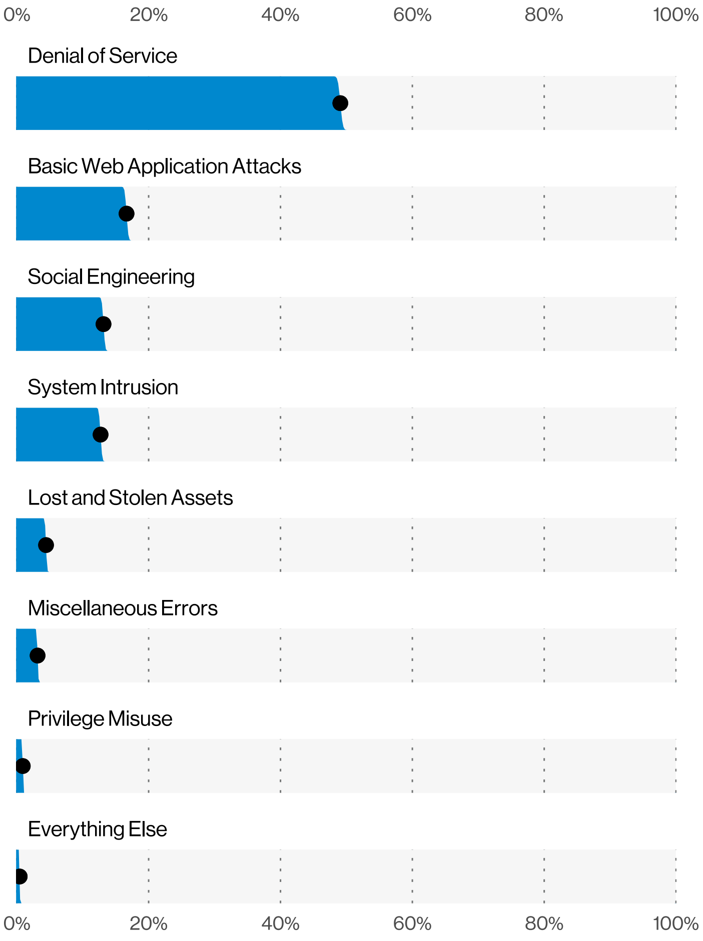
### Getting better all the time

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.

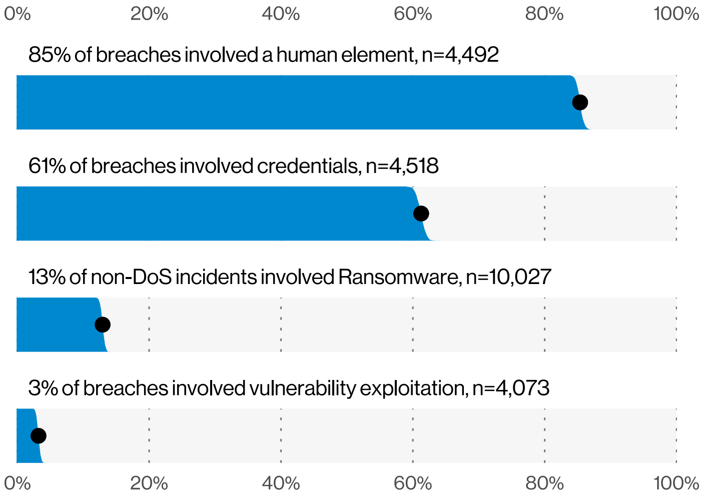
# Summary of findings



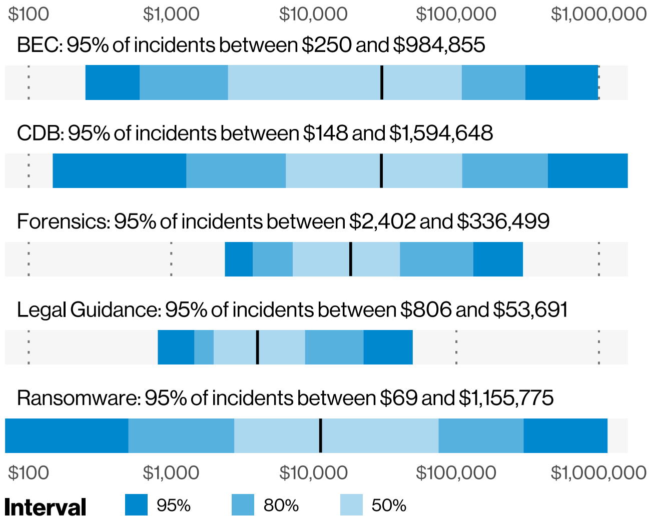
Patterns in breaches (n=5,275)



Patterns in incidents (n=29,206)



Select action varieties (n=4,073)



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 now steals 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 over 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 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.<br>• Over 80% of breaches are discovered by external parties<br>• Phishing templates have a wide range of click rates, from no clicks to click rates over 50%<br>• 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.<br>• Ninety-five percent of organizations suffering credential stuffing attacks had between 637 and 3.3 billion malicious login attempts through the year<br>• 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 at the #3 spot in breaches with Miscellaneous Error and behind Social Engineering and Basic Web Application Attacks) provides clarity to organizations trying to understand how much to invest in preventing advanced threats.<br>• Over 70% of cases in this pattern involved malware and 40% involved hacking actions<br>• Ninety-nine percent 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.<br>• Misconfiguration was by far the most common form of error (approximately 52%)<br>• The vast majority of the time, when known, security researchers (80%) were responsible for discovery<br>• 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.<br>• Seventy percent of breaches in this pattern were due to privilege abuse<br>• Over 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 (spiky), 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.<br>• This year, three of the rarely seen Environmental-caused breaches were added and are included in this pattern given their relative rarity<br>• The reclustering of the patterns allowed us to explain an additional 18% of breaches that would have otherwise fallen into this pattern |

# Industry highlights

**Organizations, regardless of size or industry, always face some risk of cyberattack. However, the type of attack they are most likely to face often varies among verticals. To deploy defenses effectively and efficiently, and thereby make the most of your security budget, it is important to understand how attacks commonly play out in your industry. We classify organizations using North American Industry Classification System (NAICS) codes.**

## Accommodation and Food Services (NAICS 72)

The Accommodation and Food Services industry is experiencing Hacking, Social and Malware attacks with close to equal frequency.

| | |
|---|---|
| **Frequency** | 69 incidents, 40 with confirmed data disclosure |
| **Top Patterns** | System Intrusion, Social Engineering and Basic Web Application Attacks represent 85% of breaches |
| **Threat Actors** | External (90%), Internal (10%) (breaches) |
| **Actor Motives** | Financial (86%-100%), Espionage (0%-14%) (breaches) |
| **Data Compromised** | Personal (51%), Credentials (49%), Payment (33%), Other (15%) (breaches) |
| **Top IG1 Protective Controls** | Security Awareness and Skills Training (14), Access Control Management (6), Secure Configuration of Enterprise Assets and Software (4) |

## Arts, Entertainment and Recreation (NAICS 71)

The Use of stolen credentials, Phishing and Ransomware continue to play large roles in this industry. Compromised medical information (from athletic programs) was seen at an unexpectedly high level as well.

| | |
|---|---|
| **Frequency** | 7,065 incidents, 109 with confirmed data disclosure |
| **Top Patterns** | System Intrusion, Basic Web Application Attacks and Miscellaneous Errors represent 83% of breaches |
| **Threat Actors** | External (70%), Internal (31%), Multiple (1%) (breaches) |
| **Actor Motives** | Financial (100%) (breaches) |
| **Data Compromised** | Personal (83%), Credentials (32%), Medical (26%), Other (18%) (breaches) |
| **Top IG1 Protective Controls** | Security Awareness and Skills Training (14), Secure Configuration of Enterprise Assets and Software (4), Access Control Management (6) |

## Education Services (NAICS 61)

The Education vertical has an unusually large percentage of Social Engineering attacks in which Pretexting is the variety. These are typically carried out with a view toward instigating a fraudulent transfer of funds. Miscellaneous Errors and System Intrusion are both still enrolled as well and are taking a full course load.

| | |
|---|---|
| **Frequency** | 1,332 incidents, 344 with confirmed data disclosure |
| **Top Patterns** | Social Engineering, Miscellaneous Errors and System Intrusion represent 86% of breaches |
| **Threat Actors** | External (80%), Internal (20%), Multiple (1%) (breaches) |
| **Actor Motives** | Financial (96%), Espionage (3%), Fun (1%), Convenience (1%), Grudge (1%) (breaches) |
| **Data Compromised** | Personal (61%), Credentials (51%), Other (12%), Medical (7%) (breaches) |
| **Top IG1 Protective Controls** | Security Awareness and Skills Training (14), Access Control Management (6), Secure Configuration of Enterprise Assets and Software (4) |

## Financial and Insurance (NAICS 52)

Misdelivery represented 55% of Financial sector errors. The Financial sector frequently faces credential and Ransomware attacks from External actors.

| | |
|---|---|
| **Frequency** | 721 incidents, 467 with confirmed data disclosure |
| **Top Patterns** | Miscellaneous Errors, Basic Web Application Attacks and Social Engineering represent 81% of breaches |
| **Threat Actors** | External (56%), Internal (44%), Multiple (1%), Partner (1%) (breaches) |
| **Actor Motives** | Financial (96%), Espionage (3%), Grudge (2%), Fun (1%), Ideology (1%) (breaches) |
| **Data Compromised** | Personal (83%), Bank (33%), Credentials (32%), Other (21%) (breaches) |
| **Top IG1 Protective Controls** | Security Awareness and Skills Training (14), Secure Configuration of Enterprise Assets and Software (4), Access Control Management (6) |

## Healthcare (NAICS 62)

Basic human error continues to beset this industry as it has for the past several years. The most common Error continues to be Misdelivery (36%), whether electronic or of paper documents. Malicious internal actions, however, have dropped from the top three for the second year in a row. Financially motivated organized criminal groups continue to target this sector, with the deployment of Ransomware remaining a favored tactic.

| | |
|---|---|
| **Frequency** | 655 incidents, 472 with confirmed data disclosure |
| **Top Patterns** | Miscellaneous Errors, Basic Web Application Attacks and System Intrusion represent 86% of breaches |
| **Threat Actors** | External (61%), Internal (39%) (breaches) |
| **Actor Motives** | Financial (91%), Fun (5%), Espionage (4%), Grudge (1%) (breaches) |
| **Data Compromised** | Personal (66%), Medical (55%), Credentials (32%), Other (20%), (breaches) |
| **Top IG1 Protective Controls** | Security Awareness and Skills Training (14), Secure Configuration of Enterprise Assets and Software (4), Access Control Management (6) |

## Information (NAICS 51)

This industry faces a distinct problem with Errors, and Misconfiguration is leading the way. From an incident perspective, DoS attacks accounted for the vast majority of attacks. Information has overtaken Finance as the main target of botnet breaches for the first time.

| | |
|---|---|
| **Frequency** | 2,935 incidents, 381 with confirmed data disclosure |
| **Top Patterns** | Basic Web Application Attacks, Miscellaneous Errors and System Intrusion represent 83% of breaches |
| **Threat Actors** | External (66%), Internal (37%), Multiple (4%), Partner (1%) (breaches) |
| **Actor Motives** | Financial (88%), Espionage (9%), Grudge (2%), Convenience (1%), Fun (1%) (breaches) |
| **Data Compromised** | Personal (70%), Credentials (32%), Other (27%), Internal (12%) (breaches) |
| **Top IG1 Protective Controls** | Security Awareness and Skills Training (14), Secure Configuration of Enterprise Assets and Software (4), Access Control Management (6) |

## Manufacturing (NAICS 31-33)

This industry, like many others, is beset by Social Engineering attacks. Manufacturing also saw a marked rise in Ransomware-related breaches.

| | |
|---|---|
| **Frequency** | 585 incidents, 270 with confirmed data disclosure |
| **Top Patterns** | System Intrusion, Social Engineering and Basic Web Application Attacks represent 82% of breaches |
| **Threat Actors** | External (82%), Internal (19%), Multiple (1%) (breaches) |
| **Actor Motives** | Financial (92%), Espionage (6%), Convenience (1%), Grudge (1%), Secondary (1%) (breaches) |
| **Data Compromised** | Personal (66%), Credentials (42%), Other (36%), Payment (19%) (breaches) |
| **Top IG1 Protective Controls** | Security Awareness and Skills Training (14), Access Control Management (6), Secure Configuration of Enterprise Assets and Software (4) |

## Mining, Quarrying and Oil & Gas Extraction + Utilities (NAICS 21 + 22)

These two industries suffered from Social Engineering attacks this year. Credentials, Personal and Internal data are the most commonly lost data varieties. Ransomware is also a major threat for these verticals.

| | |
|---|---|
| **Frequency** | 546 incidents, 355 with confirmed data disclosure |
| **Top Patterns** | Social Engineering, System Intrusion and Basic Web Application Attacks represent 98% of breaches |
| **Threat Actors** | External (98%), Internal (2%) (breaches) |
| **Actor Motives** | Financial (78%-100%), Espionage (0%-33%) (breaches) |
| **Data Compromised** | Credentials (94%), Personal (7%), Internal (3%), Other (3%) (breaches) |
| **Top IG1 Protective Controls** | Security Awareness and Skills Training (14), Access Control Management (6), Account Management (5) |

## Professional, Scientific and Technical Services (NAICS 54)

The combination of the System Intrusion and Social Engineering patterns account for the majority of cases in this sector. The Use of stolen credentials is widespread, and employees have a definite tendency to fall for Social tactics.

| | |
|---|---|
| **Frequency** | 1,892 Incidents, 630 with confirmed data disclosure |
| **Top Patterns** | System Intrusion, Social Engineering and Basic Web Application Attacks represent 81% of breaches |
| **Threat Actors** | External (74%), Internal (26%) (breaches) |
| **Actor Motives** | Financial (97%), Espionage (2%), Grudge (1%) (breaches) |
| **Data Compromised** | Credentials (63%), Personal (49%), Other (21%), Bank (9%) (breaches) |
| **Top IG1 Protective Controls** | Security Awareness and Skills Training (14), Access Control Management (6), Secure Configuration of Enterprise Assets and Software (4) |

## Public Administration (NAICS 92)

By far the biggest threat in this vector is the social engineer. Actors who can craft a credible phishing email are absconding with Credentials at an alarming rate in this sector.

| | |
|---|---|
| **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) |

# Retail (NAICS 44-45)

The Retail industry continues to be a target for financially motivated criminals looking to cash in on the combination of Payment cards and Personal information this sector is known for. Social tactics include Pretexting and Phishing, with the former commonly resulting in fraudulent money transfers.

| | |
|---|---|
| **Frequency** | 725 incidents, 165 with confirmed data disclosure |
| **Top Patterns** | System Intrusion, Social Engineering and Basic Web Application Attacks represent 77% of breaches |
| **Threat Actors** | External (84%), Internal (17%), Multiple (2%), Partner (1%) (breaches) |
| **Actor Motives** | Financial (99%), Espionage (1%) (breaches) |
| **Data Compromised** | Payment (42%), Personal (41%), Credentials (33%), Other (16%) (breaches) |
| **Top IG1 Protective Controls** | Security Awareness and Skills Training (14), Secure Configuration of Enterprise Assets and Software (4), Access Control Management (6) |

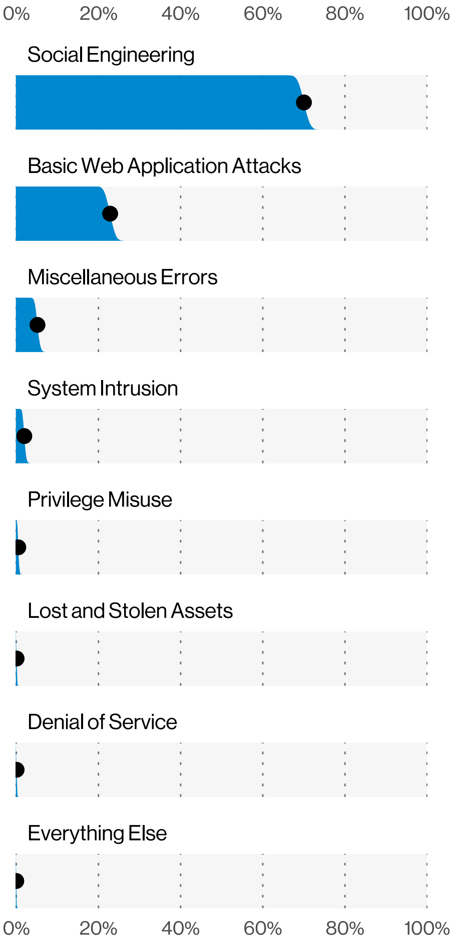
# SMB deep dive

**The gap between the number of breaches seen by small and large organizations has become much less pronounced this year, and the top patterns have also aligned. For the first time since we began to look at breaches and incidents from an organizational size point of view, we're close to a "one size fits all" situation. Both are being targeted by financially motivated organized crime actors.**

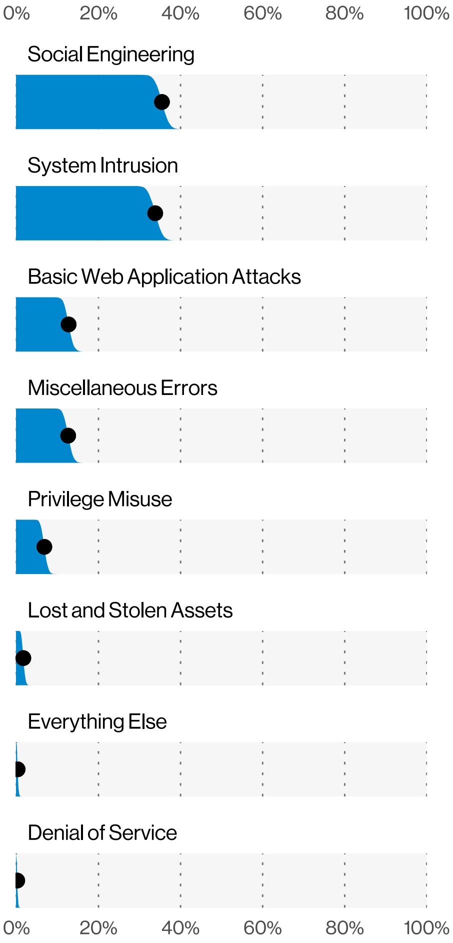
**Last year, we reported that smaller organizations seemed to be doing better in terms of discovering breaches more quickly. This year's data shows that large organizations have made a shift to finding breaches within days or faster in over half of the cases (55%), while small organizations fared less positively at 47%.**

| | **Small (fewer than 1,000 employees)** | **Large (more than 1,000 employees)** |
|---|---|---|
| **Frequency** | 1,037 incidents, 263 with confirmed data disclosure | 819 incidents, 307 with confirmed data disclosure |
| **Top Patterns** | System Intrusion, Miscellaneous Errors and Basic Web Application Attacks represent 80% of breaches | System Intrusion, Miscellaneous Errors and Basic Web Application Attacks represent 74% of breaches |
| **Threat Actors** | External (57%), Internal (44%), Multiple (1%), Partner (0%) (breaches) | External (64%), Internal (36%), Partner (1%), Multiple (1%) (breaches) |
| **Actor Motives** | Financial (93%), Espionage (3%), Fun (2%), Convenience (1%), Grudge (1%), Other (1%) (breaches) | Financial (87%), Fun (7%), Espionage (5%), Convenience (2%), Grudge (2%), Secondary (1%) (breaches) |
| **Data Compromised** | Credentials (44%), Personal (39%), Other (34%), Medical (17%) (breaches) | Credentials (42%), Personal (38%), Other (34%), Internal (17%) (breaches) |

# Regional findings



Patterns in APAC breaches (n=1,495)

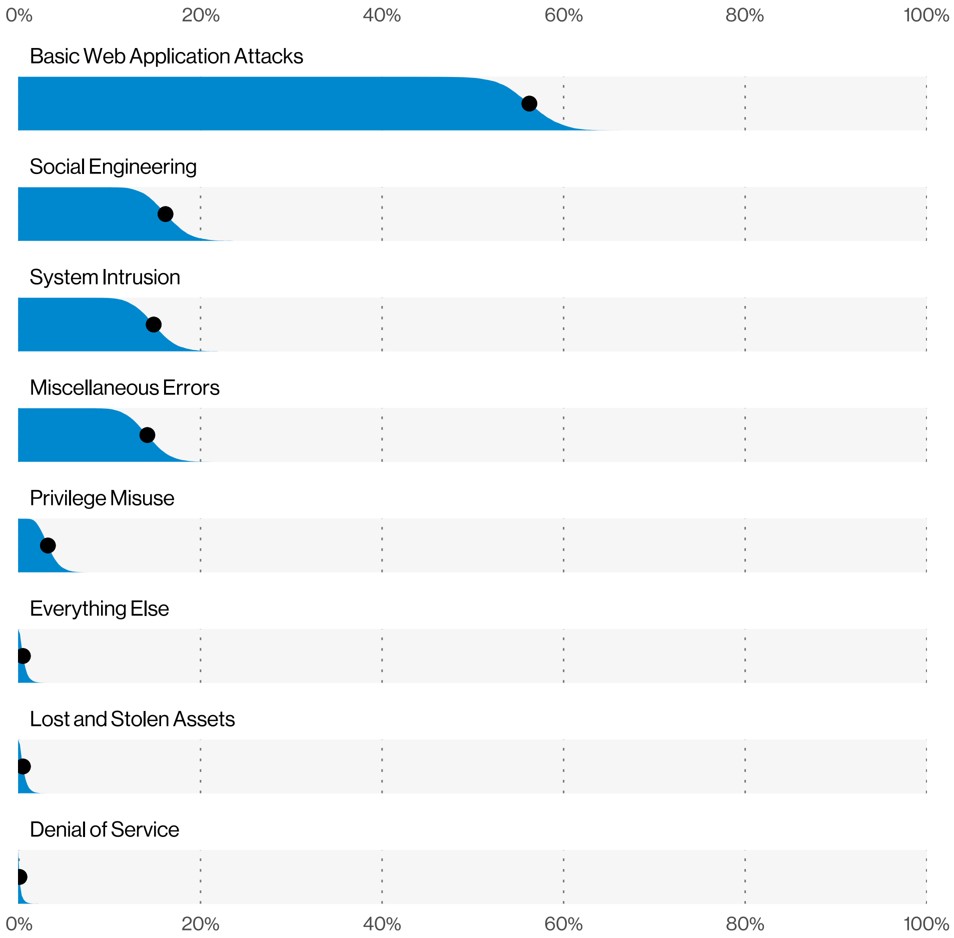


Patterns in Northern American breaches (n=1,080)

**Financially motivated attacks in APAC and Northern America**

Many of breaches that took place in the Asia-Pacific (APAC) were caused by financially motivated attackers Phishing employees for creds, and then using those stolen creds to gain access to mail accounts and web application servers.

Northern America (NA) also was often the target of financially motivated actors searching for money or easily monetizable data. Social Engineering, Hacking and Malware continue to be the favored tools utilized by these.



Patterns in EMEA breaches (N=293)

### Some of the usual suspects in EMEA

Europe, the Middle East and Africa (EMEA) continues to be beset by Basic Web Application Attacks, System Intrusion and Social Engineering.

# 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 industry 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 with 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✓