DBIR

2020 Data Breach Investigations Report

Executive Summary

verizon

3,950 breaches

That is what you are seeing. Each of these squares is organized by the 16 different industries and four world regions we cover in this year's report. Each square represents roughly one breach (1.04 to be more exact), for a total of 4,675 squares since breaches can be displayed in both their industry and region.

We also analyzed a record total of 157,525 incidents, 32,002 of which met our quality standards. The data coverage this year is so comprehensive that it shines through the monochromatic front cover, reinforcing the mission of the DBIR as being a data-driven resource. Turn the page to dig into the findings.

Table of contents

Data and insights to stay threat ready

The more you know about the threats you face, the better your chances of keeping your data secure and your name out of the headlines. That is why we create the *Verizon Data Breach Investigations Report* (DBIR). This year's report is the 13th iteration and is powered by 81 contributing organizations—the highest number yet. The DBIR team analyzed 32,002 security incidents, of which 3,950 were confirmed breaches, to create the 2020 DBIR. We have included spotlights on more industries than ever before and added new geographical breakouts of our data.

Read on for report highlights, pass this summary to colleagues and download the full report for a detailed view of the threats you face today.

32,002

The DBIR team analyzed 32,002 security incidents, of which 3,950 were confirmed breaches

Getting better all the time

The DBIR team continues to expand the Vocabulary for Event Recording and Incident Sharing (VERIS) framework to classify and analyze incidents and breaches. This year, we developed mappings with MITRE ATT&CK® and the Center for Internet Security's Critical Security Controls (CIS CSCs). We used the mappings to boost our analysis and have made them available for use by the larger security community too.

Summary of findings

Figure 1. Who are the victims?

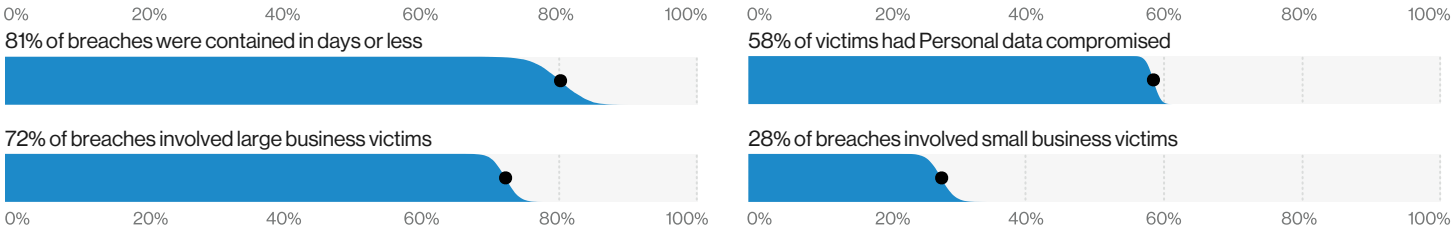


Figure 2. Who's behind the breaches?

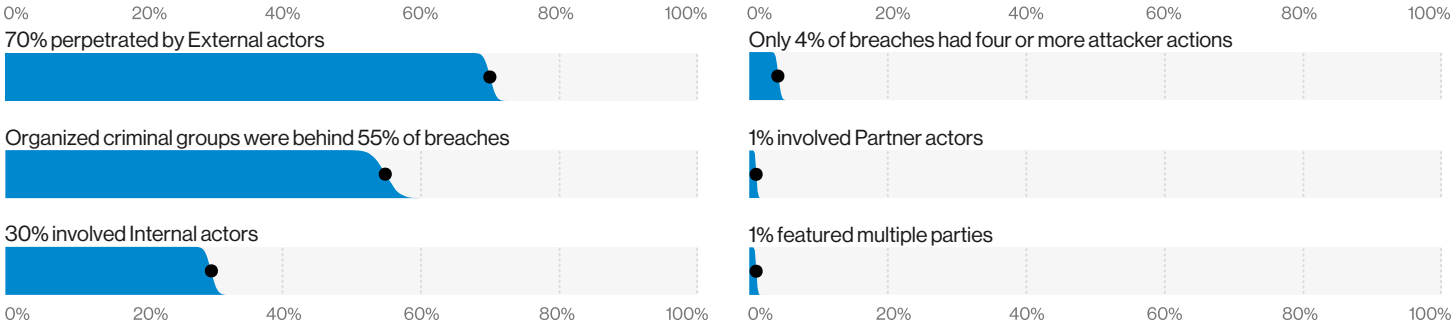
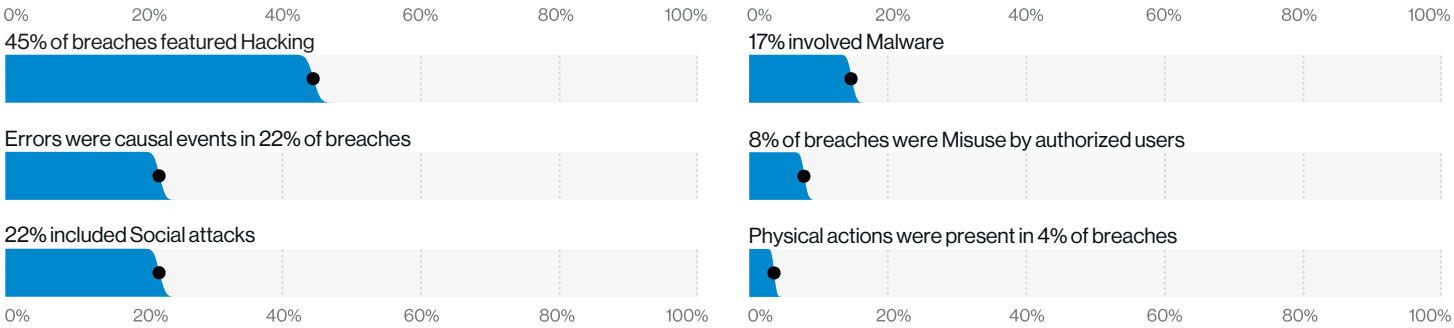


Figure 3. What tactics are utilized? (Actions)



Key takeaways

Correcting myths

On the outside looking in

Many believe shady Internal actors to be the most common cause of breaches, but the DBIR data continues to show that External actors are—and always have been—more common. In fact, 70% of breaches this year were caused by outsiders.

Money is the root of most breaches.

Espionage gets the headlines but accounts for just 10% of breaches in this year's data. The majority (86% of breaches) continue to be financially motivated. Advanced threats—which also get lots of buzz—represent only 4% of breaches.

Shining a light on attackers and their methods

The times, they aren't a'changing.

Credential theft, social attacks (i.e., phishing and business email compromise) and errors cause the majority of breaches (67% or more). These tactics prove effective for attackers, so they return to them time and again. For most organizations, these three tactics should be the focus of the bulk of security efforts.

Ransomware is everywhere.

Ransomware now accounts for 27% of Malware incidents, and 18% of organizations blocked at least one piece of ransomware. No organization can afford to ignore it.

Oh, what a tangled web application

Attacks on web apps were a part of 43% of breaches, more than double the results from last year. As workflows move to cloud services, it makes sense for attackers to follow. The most common methods of attacking web apps are using stolen or brute-forced credentials (over 80%) or exploiting vulnerabilities (less than 20%) in the web application to gain access to sensitive information.

Up-close and personal data

Personal data is getting swiped more often—or those thefts are being reported more often due to disclosure regulations. Either way, Personal data was involved in 58% of breaches, nearly twice the percentage in last year's data. This includes email addresses, names, phone numbers, physical addresses and other types of data that one might find hiding in an email or stored in a misconfigured database.

Do as I say, not as I do.

This year's DBIR saw a high number of internal-error-related breaches (881, versus last year's 424). While people are certainly still far from perfect, this increase is likely due to improved reporting requirements because of new legislation and changes in existing law rather than insiders making more frequent mistakes.

Providing much-needed good news

Block party

Security tools are getting better at blocking common malware. The DBIR data shows that Trojan-type malware peaked at just under 50% of all breaches in 2016 and has since dropped to just 6.5%. Malware sampling indicates that 45% of malware is either droppers, backdoors or keyloggers. Although this kind of threat is still plentiful, much of it is being blocked successfully.

Patch things up.

Less than 5% of breaches involved exploitation of a vulnerability. In our dataset, we do not see attackers attempting these kinds of attacks that often; only 2.5% of security information and event management (SIEM) events involved exploiting a vulnerability. This finding suggests that most organizations are doing a good job at patching—so keep it up.

However, while patching does seem to be working, poor asset management can hide big problems. Most organizations we see have internet-facing assets spread across five or more networks. It's the forgotten assets that never get patched that can create dangerous holes in your defenses.

27%

Ransomware now accounts for 27% of Malware incidents.

Credential theft, errors and social attacks are the three most common culprits in breaches. Employees working from home could be particularly vulnerable to these attacks. In these uncertain times, it makes sense to focus prevention efforts here.

Industry highlights

Organizations, regardless of size or industry, are at risk of cyberattack—yet the type of attack they are most likely to face often varies. To deploy defenses efficiently and make the most of your security budget, you need to see both the big picture and how attacks commonly play out in your industry. This year we've expanded the set of industries to 16, and we have also included an analysis of how threats differ between small and large organizations. We classify organizations using North American Industry Classification System (NAICS) codes.

Accommodation and Food Services (NAICS 72)

Point of Sale (PoS)-related attacks no longer dominate breaches in Accommodation and Food Services as they have in years past. Instead, responsibility is spread relatively evenly among several different action types such as malware, error and hacking via stolen credentials. Financially motivated attackers continue to target this industry for the payment card data it holds.

Frequency	125 incidents, 92 with confirmed data disclosure
Top Patterns	Crimeware, Web Applications and Point of Sale represent 61% of data breaches.
Threat Actors	External (79%), Internal (22%), Multiple (2%), Partner (1%) (breaches)
Actor Motives	Financial (98%), Secondary (2%) (breaches)
Data Compromised	Payment (68%), Personal (44%), Credentials (14%), Other (10%) (breaches)
Top Controls	Limitation and Control of Network Ports, Protocols, and Services (CSC 9), Boundary Defense (CSC 12), Data Protection (CSC 13)

Arts, Entertainment and Recreation (NAICS 71)

Web application attacks led to many breaches in this sector. Denial of Service attacks had higher bits per second volume in this industry than in the overall dataset. Social engineering attacks and errors also figure prominently in this vertical.

Frequency	194 incidents, 98 with confirmed data disclosure
Top Patterns	Web Applications, Miscellaneous Errors and Everything Else represent 68% of data breaches.
Threat Actors	External (67%), Internal (33%), Partner (1%), Multiple (1%) (breaches)
Actor Motives	Financial (94%), Convenience (6%) (breaches)
Data Compromised	Personal (84%), Medical (31%), Other (26%), Payment (25%) (breaches)
Top Controls	Boundary Defense (CSC 12), Secure Configurations (CSC 5, CSC 11), Implement a Security Awareness and Training Program (CSC 17)

Construction (NAICS 23)

This industry suffers from Web Applications attacks and social engineering, and the Use of stolen credentials remains a problem. However, it boasts a low submit rate for phishing and exhibits a surprisingly low number of employee errors.

Frequency	37 incidents, 25 with confirmed data disclosure
Top Patterns	Everything Else, Web Applications and Crimeware represent 95% of all incidents.
Threat Actors	External (95%), Internal (5%) (incidents)
Actor Motives	Financial (84% to 100%), Grudge (0% to 16%) (incidents)[1]
Data Compromised	Personal and Credentials
Top Controls	Secure Configurations (CSC 5, CSC 11), Boundary Defense (CSC 12), Account Monitoring and Control (CSC 16)

Education Services (NAICS 61)

This industry saw phishing attacks in 28% of breaches and hacking via stolen credentials in 23% of breaches. In incident data, Ransomware accounts for approximately 80% of Malware infections in this vertical. Education Services performed poorly in terms of reporting phishing attacks, thus losing critical response time for the victim organizations.

Frequency	819 incidents, 228 with confirmed data disclosure
Top Patterns	Everything Else, Miscellaneous Errors and Web Applications represent 81% of breaches.
Threat Actors	External (67%), Internal (33%), Partner (1%), Multiple (1%) (breaches)
Actor Motives	Financial (92%), Fun (5%), Convenience (3%), Espionage (3%), Secondary (2%) (breaches)
Data Compromised	Personal (75%), Credentials (30%), Other (23%), Internal (13%) (breaches)
Top Controls	Implement a Security Awareness and Training Program (CSC 17), Boundary Defense (CSC 12), Secure Configurations (CSC 5, CSC 11)

Financial and Insurance (NAICS 52)

The attacks in this sector are perpetrated by External actors who are financially motivated to get easily monetized data (63%), Internal financially motivated actors (18%) and Internal actors committing errors (9%). Web Application attacks that leverage the Use of stolen credentials also continue to affect this industry. Breaches caused by Internal actors have shifted from malicious actions to benign errors, although both are still damaging.

Frequency	1,509 incidents, 448 with confirmed data disclosure
Top Patterns	Web Applications, Miscellaneous Errors and Everything Else represent 81% of breaches .
Threat Actors	External (64%), Internal (35%), Partner (2%), Multiple (1%) (breaches)
Actor Motives	Financial (91%), Espionage (3%), Grudge (3%) (breaches)
Data Compromised	Personal (77%), Other (35%), Credentials (35%), Bank (32%) (breaches)
Top Controls	Implement a Security Awareness and Training Program (CSC 17), Boundary Defense (CSC 12), Secure Configurations (CSC 5, CSC 11)

Healthcare (NAICS 62)

Financially motivated criminal groups continue to target this industry via ransomware attacks. Lost and stolen assets also remain a problem in our incident dataset. Basic human error is alive and well in this vertical. Misdelivery grabbed the top spot among Error action types, while internal Misuse has decreased.

Frequency	798 incidents, 521 with confirmed data disclosure
Top Patterns	Miscellaneous Errors, Web Applications and Everything Else represent 72% of breaches.
Threat Actors	External (51%), Internal (48%), Partner (2%), Multiple (1%) (breaches)
Actor Motives	Financial (88%), Fun (4%), Convenience (3%) (breaches)
Data Compromised	Personal (77%), Medical (67%), Other (18%), Credentials (18%) (breaches)
Top Controls	Implement a Security Awareness and Training Program (CSC 17), Boundary Defense (CSC 12), Data Protection (CSC 13)

Information (NAICS 51)

Web Application attacks via vulnerability exploits and the Use of stolen credentials are prevalent in this industry. Errors continue to be a significant factor and are primarily made up of the Misconfiguration of databases. Growth in Denial of Service attacks also remains a problem for the Information sector.

Frequency	5,741 incidents, 360 with confirmed data disclosure
Top Patterns	Web Applications, Miscellaneous Errors and Everything Else represent 88% of data breaches.
Threat Actors	External (67%), Internal (34%), Multiple (2%), Partner (1%) (breaches)
Actor Motives	Financial (88%), Espionage (7%), Fun (2%), Grudge (2%), Other (1%) (breaches)
Data Compromised	Personal (69%), Credentials (41%), Other (34%), Internal (16%) (breaches)
Top Controls	Secure Configurations (CSC 5, CSC 11), Continuous Vulnerability Management (CSC 3), Implement a Security Awareness and Training Program (CSC 17)

Manufacturing (NAICS 31-33)

Manufacturing is beset by External actors using password-dumper malware and stolen credentials to hack into systems and steal data. While the majority of attacks are financially motivated, there was a respectable showing of cyber-espionage motivated attacks in this industry as well. Internal employees misusing their access to abscond with data also remains a concern for this vertical.

Frequency	922 incidents, 381 with confirmed data disclosure
Top Patterns	Crimeware, Web Applications and Privilege Misuse represent 64% of breaches.
Threat Actors	External (75%), Internal (25%), Partner (1%) (breaches)
Actor Motives	Financial (73%), Espionage (27%) (breaches)
Data Compromised	Credentials (55%), Personal (49%), Other (25%), Payment (20%) (breaches)
Top Controls	Boundary Defense (CSC 12), Implement a Security Awareness and Training Program (CSC 17), Data Protection (CSC 13)

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

Breaches are composed of a variety of actions, but Social attacks such as Phishing and Pretexting dominate incident data (no confirmation of data disclosure). Cyber-Espionage motivated attacks and incidents involving operational technology (OT) assets are also concerns for these industries.

Frequency	194 incidents, 43 with confirmed data disclosure
Top Patterns	Everything Else, Web Applications and Cyber-Espionage represent 74% of breaches.
Threat Actors	External (75%), Internal (28%), Multiple (2%) (breaches)
Actor Motives	Financial (63% to 95%), Espionage (8% to 43%), Convenience/Other/Secondary (0% to 17% each), Fear/Fun/Grudge/Ideology (0% to 9% each) (breaches)[1]
Data Compromised	Credentials (41%), Personal (41%), Other (35%), Internal (19%) (breaches)
Top Controls	Secure Configurations (CSC 5, CSC 11), Boundary Defense (CSC 12), Implement a Security Awareness and Training Program (CSC 17)

Other Services (NAICS 81)

Other Services covers a variety of business types, ranging from personal and repair services to nonprofit religious and social benefit organizations. Financially motivated External actors are the highest motive, with Web Applications accounting for 39% of breaches. Error among employees is another issue for this sector, particularly with regard to Misconfiguration and Misdelivery. While Credentials are a desirable target, it is Personal data that is most frequently stolen here.

Frequency	107 incidents, 66 with confirmed data disclosure
Top Patterns	Web Applications, Miscellaneous Errors and Everything Else represent 83% of breaches.
Threat Actors	External (68%), Internal (33%), Multiple (2%) (breaches)
Actor Motives	Financial (60% to 98%), Espionage (0% to 28%), Convenience/Fear/Fun/Grudge/Other/Secondary (0% to 15% each) (breaches)[1]
Data Compromised	Personal (81%), Other (42%), Credentials (36%), Internal (25%) (breaches)
Top Controls	Boundary Defense (CSC 12), Implement a Security Awareness and Training Program (CSC 17), Secure Configurations (CSC 5, CSC 11)

Professional, Technical and Scientific Services (NAICS 54)

Financially motivated attackers continue to steal credentials and leverage them against web application infrastructure. Social engineering in the form of phishing and pretexting are common tactics used to gain access. This industry also suffers from Denial of Service attacks regularly.

Frequency	7,463 incidents, 326 with confirmed data disclosure
Top Patterns	Web Applications, Everything Else and Miscellaneous Errors represent 79% of breaches.
Threat Actors	External (75%), Internal (22%), Partner (3%), Multiple (1%) (breaches)
Actor Motives	Financial (93%), Espionage (8%), Ideology (1%) (breaches)
Data Compromised	Personal (75%), Credentials (45%), Other (32%), Internal (27%) (breaches)
Top Controls	Secure Configurations (CSC 5, CSC 11), Implement a Security Awareness and Training Program (CSC 17), Boundary Defense (CSC 12)

Public Administration (NAICS 92)

Ransomware is a problem for this sector, with financially motivated attackers utilizing it to target a wide array of government entities. Misdelivery and Misconfiguration errors also persist in this sector.

Frequency	6,843 incidents, 346 with confirmed data disclosure
Top Patterns	Miscellaneous Errors, Web Applications and Everything Else represent 73% of breaches.
Threat Actors	External (59%), Internal (43%), Multiple (2%), Partner (1%) (breaches)
Actor Motives	Financial (75%), Espionage (19%), Fun (3%) (breaches)
Data Compromised	Personal (51%), Other (34%), Credentials (33%), Internal (14%) (breaches)
Top Controls	Implement a Security Awareness and Training Program (CSC 17), Boundary Defense (CSC 12), Secure Configurations (CSC 5, CSC 11)

Real Estate and Rental and Leasing (NAICS 53)

Web Applications attacks utilizing stolen credentials are rife in this vertical. Social engineering attacks in which adversaries insert themselves into the transfer-of-property process and attempt to direct fund transfers to attacker-owned bank accounts are also prevalent. Like many other industries, misconfigurations are impacting this sector.

Frequency	37 incidents, 33 with confirmed data disclosure
Top Patterns	Web Applications, Everything Else and Miscellaneous Errors represent 88% of data breaches.
Threat Actors	External (73%), Internal (27%) (breaches)
Actor Motives	Financial (45% to 97%), Convenience/Espionage (0% to 40% each), Fear/Fun/Grudge/Ideology/Other/Secondary (0% to 21% each) (breaches)[1]
Data Compromised	Personal (83%), Internal (43%), Other (43%), Credentials (40%) (breaches)
Top Controls	Secure Configurations (CSC 5, CSC 11), Implement a Security Awareness and Training Program (CSC 17), Boundary Defense (CSC 12)

Retail (NAICS 44-45)

Attacks against e-commerce applications are by far the leading cause of breaches in this industry. As organizations continue to move their primary operations to the web, the criminals migrate along with them. Consequently, PoS-related breaches, which were for many years the dominant concern for this vertical, continue at the low levels of 2019's DBIR. While Payment is a commonly lost data type, Personal and Credentials also continue to be highly sought after in this sector.

Frequency	287 incidents, 146 with confirmed data disclosure
Top Patterns	Web Applications, Everything Else and Miscellaneous Errors represent 72% of breaches.
Threat Actors	External (75%), Internal (25%), Partner (1%), Multiple (1%) (breaches)
Actor Motives	Financial (99%), Espionage (1%) (breaches)
Data Compromised	Personal (49%), Payment (47%), Credentials (27%), Other (25%) (breaches)
Top Controls	Boundary Defense (CSC 12), Secure Configurations (CSC 5, CSC 11), Continuous Vulnerability Management (CSC3)

Transportation and Warehousing (NAICS 48-49)

Financially motivated organized criminals utilizing attacks against web applications have their sights set on this industry. But employee errors such as standing up large databases without controls are also a recurring problem. These, combined with social engineering in the forms of phishing and pretexting attacks, are responsible for the majority of breaches in this industry.

Frequency	112 incidents, 67 with confirmed data disclosure
Top Patterns	Everything Else, Web Applications and Miscellaneous Errors represent 69% of breaches .
Threat Actors	External (68%), Internal (32%) (breaches)
Actor Motives	Financial (74% to 98%), Espionage (1% to 21%), Convenience (0% to 15%) (breaches)[1]
Data Compromised	Personal (64%), Credentials (34%), Other (23%) (breaches)
Top Controls	Boundary Defense (CSC 12), Implement a Security Awareness and Training Program (CSC 17), Secure Configurations (CSC 5, CSC 11)

SMB deep dive

While differences between small and medium-sized businesses (SMBs) and large organizations remain, the movement toward the cloud and its myriad web-based tools, along with the continued rise of social attacks, has narrowed the dividing line between the two. As SMBs have adjusted their business models, the criminals have adapted their actions to keep in step and select the quickest and easiest path to their victims.

	Small (fewer than 1,000 employees)	Large (more than 1,000 employees)
Frequency	407 incidents, 221 with confirmed data disclosure	8,666 incidents, 576 with confirmed data disclosure
Top Patterns	Web Applications, Everything Else and Miscellaneous Errors represent 70% of breaches.	Everything Else, Crimeware and Privilege Misuse represent 70% of breaches.
Threat Actors	External (74%), Internal (26%), Partner (1%), Multiple (1%) (breaches)	External (79%), Internal (21%), Partner (1%), Multiple (1%) (breaches)
Actor Motives	Financial (83%), Espionage (8%), Fun (3%), Grudge (3%) (breaches)	Financial (79%), Espionage (14%), Fun (2%), Grudge (2%) (breaches)
Data Compromised	Credentials (52%), Personal (30%), Other (20%), Internal (14%), Medical (14%) (breaches)	Credentials (64%), Other (26%), Personal (19%), Internal (12%) (breaches)

Regional findings

For the first time, this year's DBIR provides a breakdown of data by region.

Figure 4. Northern America

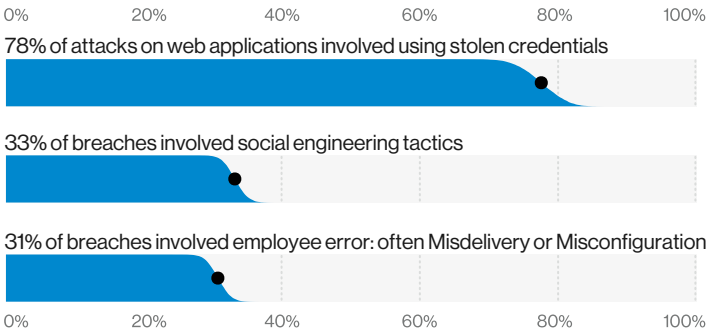


Figure 5. Europe, Middle East and Africa

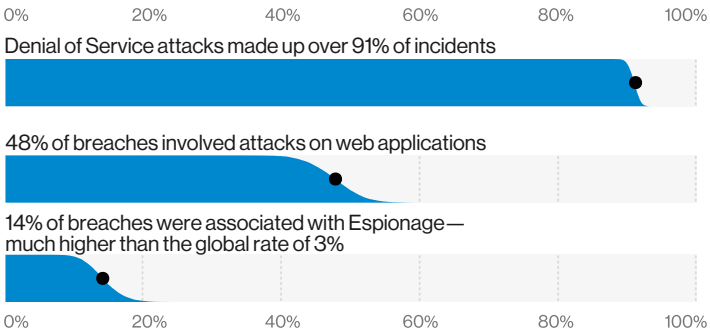


Figure 6. Asia-Pacific

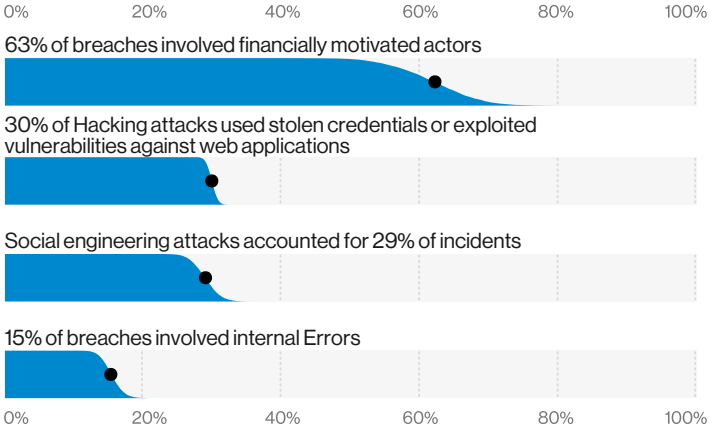
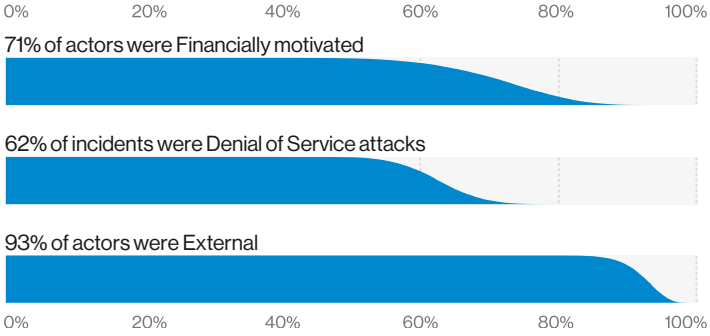


Figure 7. Latin America and the Caribbean



Best practices

This year, we've aligned our findings with the Center for Internet Security Critical Security Controls to provide you with a way to translate DBIR data into your security efforts. Here are the top controls that our data suggests will be worthwhile for most organizations.

Continuous Vulnerability Management (CSC 3)

Use this method to find and remediate things like code-based vulnerabilities; also great for finding misconfigurations.

Secure Configurations (CSC 5, CSC 11)

Ensure and verify that systems are configured with only the services and access needed to achieve their function.

Email and Web Browser Protection (CSC 7)

Lock down browsers and email clients to give your users a fighting chance when facing the Wild West that we call the internet.

Limitation and Control of Network Ports, Protocols and Services (CSC 9)

Understand what services and ports should be exposed on your systems, and limit access to those.

Boundary Protection (CSC 12)

Go beyond firewalls to consider things like network monitoring, proxies and multifactor authentication.

Data Protection (CSC 13)

Control access to sensitive information by maintaining an inventory of sensitive information, encrypting sensitive data and limiting access to authorized cloud and email providers.

Account Monitoring (CSC 16)

Lock down user accounts across the organization to keep bad guys from using stolen credentials. Use of multifactor authentication also fits in this category.

Implement a Security Awareness and Training Program (CSC 17)

Educate your users on malicious attackers and on accidental breaches.

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 protect your organization.

Read the full 2020 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.

1 We had a relatively small sample here, so we have used a range of percentages to make sure we are very clear about the broad margin of confidence we have in respect to this section. See the full report for more details on this approach.