2022 DBIR: Healthcare

Snapshot

(NAICS 62)

Welcome to the Healthcare snapshot from the 15th annual Verizon Data Breach Investigations Report (DBIR). It is truly hard to believe that it has been 15 years since our inaugural report.

The DBIR examines common types of cybersecurity attacks and offers insights into how organizations can protect themselves. This year, we looked at 23,896 incidents. Healthcare saw 849 of those incidents, 571 of which had confirmed data disclosure. This data represents real-world breaches and incidents investigated by the Verizon Threat Research Advisory Center (VTRAC) or provided to us by our 87 global contributors.

We hope that you can use this report and the information it contains to increase your awareness of the most common tactics used against Healthcare and to help prepare your organization.

Read on for report highlights related to Healthcare. Also, 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 2022.

For all industry labels in the DBIR report, we align with the North American Industry Classification System (NAICS) standard to categorize the victim organization. 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. Detailed information on the codes and the classification system is available here: census.gov/naics/?58967?yearbck=2012

Incident Classification Patterns

The DBIR first introduced the Incident Classification Patterns in 2014 as a useful shorthand for scenarios that occurred very frequently. Last year, due to changes in attack type and the threat landscape, we revamped and enhanced those patterns, moving from nine to the eight you see in this report.

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.

Social Engineering

Psychological compromise of a person that alters their behavior into taking an action or breaching confidentiality.

The human element continues to be a key driver of 82% of breaches, and this pattern captures a large percentage of those breaches. Additionally, malware and stolen credentials provide a great second step after a social attack gets the actor in the door, which emphasizes the importance of having a strong security awareness program.

- Fifty-nine percent of Social Engineering breaches compromised credentials, and 31% used stolen credentials. Credential compromise was three times more likely in Social Engineering breaches than in the rest of the patterns
- Phishing is more than twice as likely as Pretexting in the Social Engineering pattern
- A Financial motive is eight times more common than an Espionage motive in Social Engineering breaches

Basic Web Application Attacks

Simple web application attacks with a small number of steps or additional actions after the initial web application compromise.

This pattern continues to largely be dominated by attackers using stolen credentials to access an organization's internet-facing infrastructure, like web servers and email servers.

- Four out of every five web app attacks involved stolen credentials. This finding underlies the importance of password safeguards
- Espionage is four times more likely in Basic Web Application Attack (BWAA) breaches than in the rest of the patterns, indicating that Nation-states don't necessarily have to pursue complex attacks to leverage established and effective attacks to achieve their objectives
- Use of stolen credentials is six times more likely than Exploiting a vulnerability in BWAA breaches

System Intrusion

System Intrusion captures the complex attacks that leverage Malware and/or Hacking to achieve their objectives, including deploying ransomware.

This pattern consists of more complex breaches and attacks that leverage a combination of several different actions, such as Social, Malware and Hacking, and is where we find Supply Chain breaches and Ransomware, both of which increased dramatically this year.

- Ninety-two percent of System Intrusion breaches are Financially motivated
- Use of stolen credentials is four times more likely than Exploiting vulnerabilities in System Intrusion breaches

Miscellaneous Errors

Incidents where unintentional actions directly compromised a security attribute of an information asset. This does not include lost devices, which are grouped with theft instead.

This year's data shows it is all about your employees. Misdelivery and Misconfiguration are the top two varieties. Misconfiguration is frequently paired with the discovery method of "Security researcher."

- Misconfigured servers accidentally exposed to the internet or Misdelivery actions in which users send emails to the wrong recipient represent 13% of total breaches
- External cloud assets have decreased 83% since last year in Miscellaneous Errors breaches, potentially indicating a shift in technologies leveraging a secure-by-default approach
- Eighty-five percent of Miscellaneous Error breaches involved servers

Privilege Misuse

Incidents predominantly driven by unapproved or malicious use of legitimate privileges.

Most of these incidents result in successful data breaches. These actors are still motivated by greed (financial gain) and are stealing Personal data because it is easy to monetize.

- Documents are three times more likely in Privilege Misuse than in the rest of the patterns

Lost and Stolen Assets

Any incident where an information asset went missing, whether through misplacement or malice.

The prevalence of theft is driven by the Financial motive—we believe many of the perpetrators of theft are committing the crime with the intention of an immediate payoff by selling the stolen asset.

- The type of data affected by these incidents is the same (almost exactly) as last year. External actors typically perpetrate the thefts, while employees are responsible for losing track of their assets
- Unaffiliated actors are 14 times more likely in Lost and Stolen Assets incidents than in the rest of the patterns

Denial of Service

Attacks intended to compromise the availability of networks and systems. Includes both network- and application-layer attacks.

Large organizations are twice as common in Denial of Service (DoS) incidents than the rest of the patterns. While these attacks are a nuisance impacting a large range of organizations, some face these attacks on a regular basis, which may potentially affect their function.

Everything Else

Everything else isn't really a pattern at all. Instead, it covers all incidents that don't fit within the orderly confines of the other patterns.

Healthcare

Basic Web Application Attacks have overtaken the Miscellaneous Errors in causing breaches in this sector. Errors are still a significant problem.

Patterns in years	5-year difference	3-year difference	Difference with peers
Basic Web Application Attacks	Greater	Greater	Greater
System Intrusion	Greater	Greater	Less
Miscellaneous Errors	Less	Less	Greater

Frequency	849 incidents, 571 with confirmed data disclosure
Top patterns	Basic Web Application Attacks, Miscellaneous Errors and System Intrusion represent 76% of breaches
Threat actors	External (61%), Internal (39%) (breaches)
Actor motives	Financial (95%), Espionage (4%), Convenience (1%), Grudge (1%) (breaches)
Data compromised	Personal (58%), Medical (46%), Credentials (29%), Other (29%) (breaches)
Top IG1 protective Controls	Security Awareness and Skills Training (CSC 14), Secure Configuration of Enterprise Assets and Software (CSC 4), Access Control Management (CSC 6)
What is the same?	The top three patterns are the same, but the order is not. The threat actors were exactly the same as last year (down to the percentage point).

Healthcare is the industry where the internal actor has figured prominently in breaches since we first began collecting and reporting data. While the make-up of the insider breach has moved from being largely malicious Misuse incidents to the more benign (but no less reportable) Miscellaneous Errors, we have always been able to rely on this industry to tell the insider threat story. With the rise of the Basic Web Application Attacks pattern in this vertical, those inside actors no longer hold sway. Move over Insiders, the big dogs are here.

Make no mistake (no pun intended), your employees are still causing breaches, but they are more than 2.5 times more likely to make an error than to maliciously misuse their access. Misdelivery and Loss are the most common errors (and they are so close, we'd need a photo finish to determine a winner).

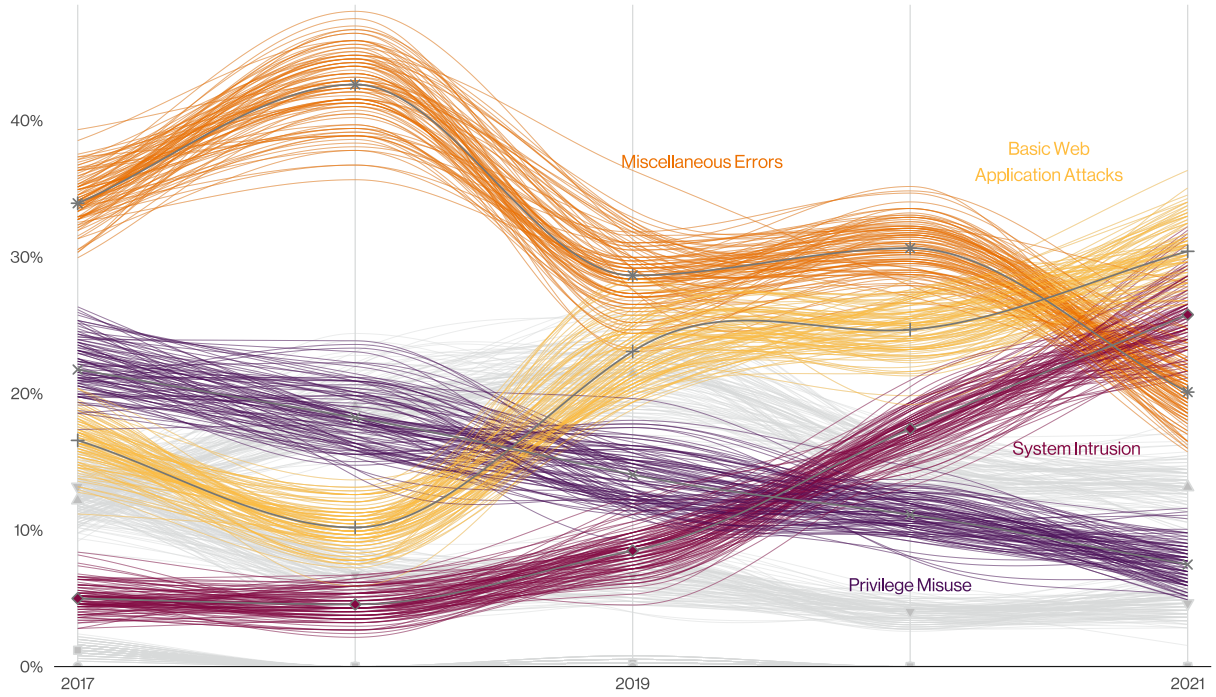

Figure 1. Patterns over time in Healthcare industry breaches

Figure 1 illustrates the change over time in patterns for Healthcare. Back in 2015, the top pattern was Privilege Misuse, followed by Miscellaneous Errors. It wasn't until 2019 that we started to see the rise of Basic Web Application Attacks, and they have clearly become a serious problem for everyone, not just this industry. Healthcare has increasingly become a target of run-of-the-mill hacking attacks and the more impactful ransomware campaigns (both from the System Intrusion pattern, which came in third). With the increase in ransomware, comes the associated increase of the discovery method of Actor Disclosure. It is a bad day when that ransom note pops up after the encryption has been triggered, providing convenient methods of payment for these customer service-focused threat groups. (And really, who doesn't want to make it easy for their "customers" to pay them?)

For the second year, Personal data is compromised more often than Medical. Do we consider this the norm now for the one industry with a plethora of medical data? Is this because the actors are just getting in and getting their encryption game on without regard to the type of records they are rendering inaccessible? Only those in the industry know for certain if they have increased their controls around their Medical data but left Personal data in the waiting room.

Being confident in our data

Starting in 2019 with slanted bar charts, the DBIR has tried to make the point that the only certain thing about information security is that nothing is certain.

The slant on the slanted bar chart represents the uncertainty of that data point to a 95% confidence level (which is standard for statistical testing).

Spaghetti charts, and our relative newcomer, pictogram plots, attempt to capture uncertainty in a similar way to slanted bar charts but are more suited for a single proportion.

Stay informed and threat ready.

Successfully navigating through the cyberthreats facing Healthcare 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.

Read the full 2022 DBIR at verizon.com/dbir