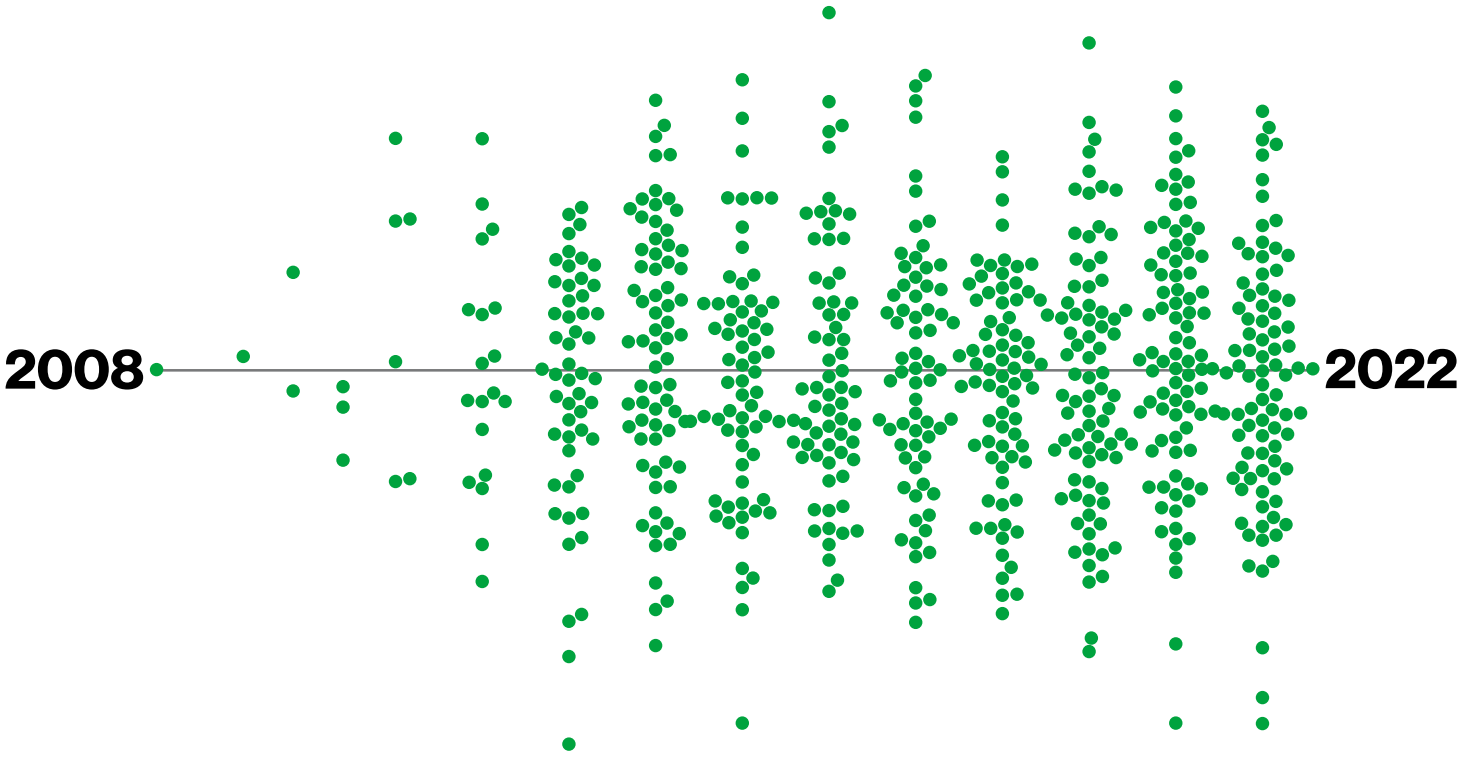
DBIR

2022 Data Breach Investigations Report

Public Sector snapshot



About the cover

Our long-time readers may recall that the cover for our inaugural report back in 2008 depicted an empty chair in a server room. It was intended to convey the fact that many organizations are not properly minding their assets and data. The 2022 cover is a throwback to that report, both for purposes of nostalgia and to convey that many organizations continue to struggle with keeping an eye on their people and their systems. The overlay of the timeline with the dot plot illustrates the number of global contributors that have joined us over the 15-year history of the report (broken out by year).

Table of contents

15 years of data research: The evolving threat environment

Welcome to the 15th annual Verizon Data Breach Investigations Report (DBIR). It is truly hard to believe that it has been 15 years since our inaugural installment of this document. Thank you to our contributors for your continued willingness to share your data, insight and vast experience in a selfless effort to improve this industry.

The past year has been extraordinary in a number of ways, but it was certainly memorable with regard to the murky world of cybercrime. From very well-publicized critical infrastructure attacks to massive supply chain breaches, the financially motivated criminals and nefarious Nation-state actors have rarely, if ever, come out swinging the way they did over the past 12 months.

As in past years, we will examine what our data has to tell us about these and other common action types used against enterprises. This year, we looked at 23,896 incidents, 5,212 of which were confirmed breaches. This data represents actual real-world breaches and incidents investigated by the Verizon Threat Research Advisory Center (VTRAC) or provided to us by our 87 global contributors, without whose generous help this document could not be produced. We hope that 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 against your specific industry, and what you can do to protect your organization and its assets.

Read on for report highlights related to Public Administration, 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.

23,896

The DBIR team analyzed 23,896 incidents, of which 5,212 were confirmed data 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 here:

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

Summary of findings

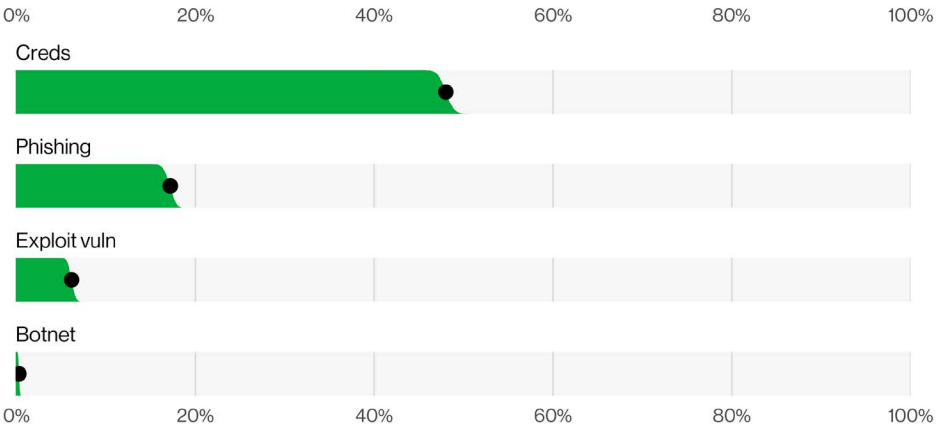


Figure 1. Select enumerations in non-Error, non-Misuse breaches (n=4,250)

There are four key paths leading to your estate: Credentials, Phishing, Exploit vulnerabilities and Botnets. These four pervade all areas of the DBIR, and no organization is safe without a plan to handle them all.

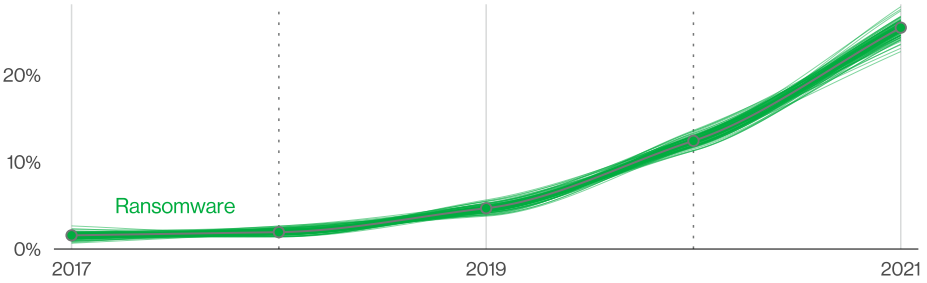


Figure 2. Ransomware over time in breaches

This year, Ransomware has continued its upward trend with an almost 13% increase (for a total of 25% of breaches)—a rise as big as the last five years combined. It's important to remember that ransomware by itself is really just a model of monetizing an organization's access. Blocking the four key paths helps to block Ransomware.

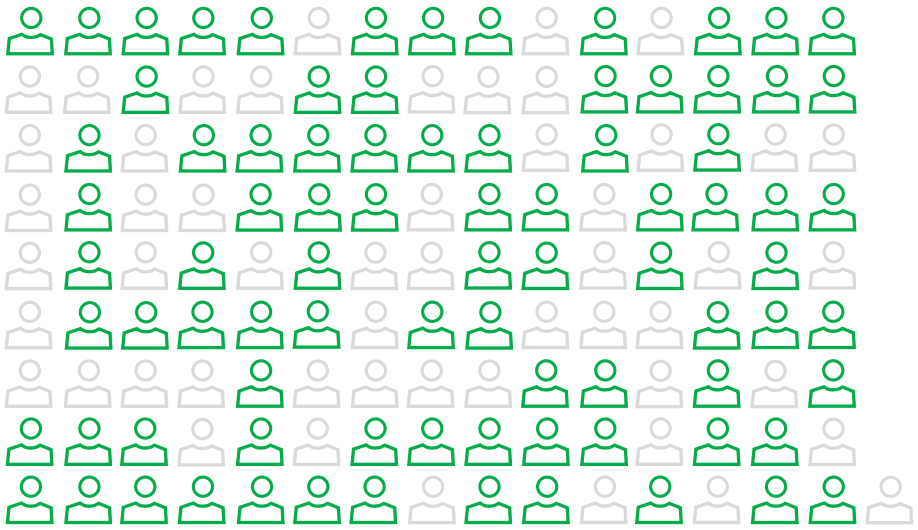


Figure 3. Partner vector in Systems Intrusion incidents (n=3,403)
Each glyph represents 25 incidents.

2021 illustrated how one key supply chain breach can lead to wide-ranging consequences. Compromising the right partner is a force multiplier for threat actors. Unlike a financially motivated actor, Nation-state threat actors may skip the breach and keep the access.

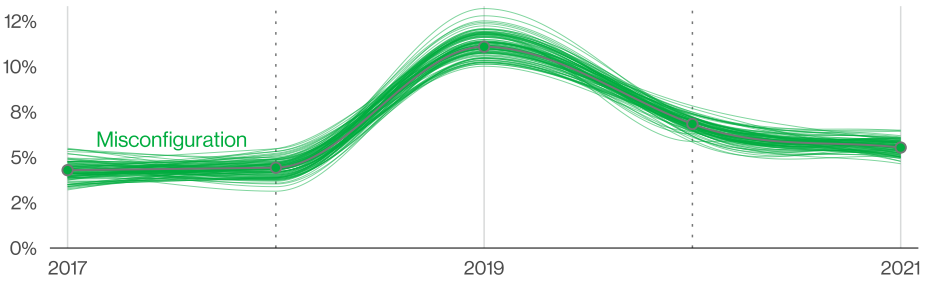


Figure 4. Misconfiguration over time in breaches

Error continues to be a dominant trend, and is heavily influenced by misconfigured cloud storage. While this is the second year in a row that we have seen a slight leveling out for this pattern, the fallibility of employees should not be discounted.

Figure 5. The human element in breaches (n=4,110)
Each glyph represents 25 breaches.

The human element continues to drive breaches. This year, 82% of breaches involved the human element. Whether it is the Use of stolen credentials, Phishing or simply an Error, people continue to play a large part in incidents and breaches alike.

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.

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 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. • 59% of Social Engineering breaches compromised creds, and 31% used stolen credentials. Credential compromise was 3x more likely in Social Engineering breaches than in the rest of the patterns • Phishing is more than 2x as likely as Pretexting in the Social Engineering pattern • A Financial motive is 8x more common than an Espionage motive in Social Engineering breaches
Basic Web Application Attacks (BWAA)	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. • 4 out of every 5 web app attacks involved stolen creds. This finding underlies the importance of password safeguards • Espionage is 4x more likely in 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 6x 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. • 92% of System Intrusion breaches are Financially motivated • Use of stolen credentials is 4x 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 • 85% 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 3x 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 14x 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 2x more common in Denial of Service 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.

Key takeaways

Attacks on all fronts

There are four key paths leading to your estate: Credentials, Phishing, Exploit vulnerabilities and Botnets. All four pervade all areas of the DBIR, and no organization is safe without a way to handle them all.

Ransomware remains a key issue.

Ransomware has increased 13% in breaches, greater than the last five years combined. Ransomware has provided actors a potential way to monetize access to a wider range of victims than was possible in the past.

Keep your supply chain close ...

2021 illustrated how one key supply chain breach can lead to wide-ranging consequences. Compromising the right partner is a force multiplier for threat actors.

And your partners even closer.

Unlike a Financially motivated actor, Nation-state threat actors may skip the breach and keep the access to leverage it at a future (and possibly more critical) date. Partners accounted for the vector in 62% of incidents discussed in the System Intrusion pattern—although this was mostly due to a single supply chain breach.

Errors are still a concern.

Error continues to be a dominant trend and is heavily driven by misconfigured cloud storage. While this is the second year in a row that we have seen a slight leveling out for this pattern, the fallibility of employees should not be discounted. Breaches due to Misconfiguration errors appear to have peaked in 2019 at 11% of breaches, while they represent 6% of breaches currently.

Social attackers target the human element.

The human element was involved in 82% of breaches, and consists of Social attacks, Error and Misuse; but Social attacks such as Phishing and Pretexting were responsible for the majority.

Public Administration

Frequency	2,792 incidents, 537 with confirmed data disclosure
Top patterns	System Intrusion, Miscellaneous Errors and Basic Web Application Attacks represent 81% of breaches.
Threat actors	External (78%), Internal (22%) (breaches)
Actor motives	Financial (80%), Espionage (18%), Ideology (1%), Grudge (1%) (breaches)
Data compromised	Personal (46%), Credentials (34%), Other (28%), Internal (28%) (breaches)
Top IG1[1] protective controls	Security Awareness and Skills Training (CSC 14), Access Control Management (CSC 6), Account Management (CSC 5)
What is the same?	Miscellaneous Errors remain in the top three patterns in the same place as last year.

Government agencies and other organizations in the Public Sector have emerged as targets in general over the last few years, but this year bad actors increasingly targeted this sector for potential financial gain. Much like corporations have had to protect their financial assets against attacks, agencies are also now on high alert for guarding their financial information.

This year, the System Intrusion pattern kicked the Social Engineering pattern right out of the "top three" club, as Financially motivated attacks rose among government and other Public Sector organizations. This was quite the coup, considering the Social Engineering pattern was in the top spot last year. In part, this may be attributed to some prominent and far-reaching supply chain breaches that came to light last year.

As the Social Engineering pattern fell, the Basic Web Application Attacks stepped in to fill the vacuum. Miscellaneous Errors remained in the middle spot, with the trio of Misconfiguration, Misdelivery and Loss nearly tied for what caused the most error-based breaches in this sector.

The occurrence of errors in this sector accounts for the prevalence of breaches caused by the Internal actor. While there was a smattering of Misuse breaches in this sector, internal actors are about seven times more likely to make a mistake that causes a breach than they are to do something malicious.

We have said before how popular Credentials are as a data type to be raided. However, this year's data showed a drop from 2021's report, when it was 80% in this sector. Personal was only 18% last year but has now catapulted into the top spot.

In honor of our 15-year anniversary, we wanted to take a look back in time at what has changed in this sector. Just three years ago, the top motive was Espionage, at 66% of breaches. Five years ago, it was 64%, which illustrates that it has been a persistent challenge for Government entities. This makes sense, when you consider that regardless of which Government entity we are talking about, someone wants to know what they're up to. Speaking of malicious, we found that the Espionage motive is up 4% from last year to 18% this year. Internal breaches also increased from last year, and we have the motive of Grudge popping up in our list for a change.

Patterns in years	5-year difference	3-year difference	Difference with peers
Basic Web Application Attacks	No change	Greater	Less
Miscellaneous Errors	No change	Less	Less
System Intrusion	Greater	Greater	Greater

1 The Implementation Group 1 (IG1) Controls are taken from the CIS Critical Security Controls.

Figure 6 illustrates the change in the Espionage-motivated actors in this industry since 2017. As you can see, when the Espionage motive fell, the Financially motivated attacks rose. It appears that the Public Administration sector has joined the rest of us in being targeted by criminals looking to make a buck.

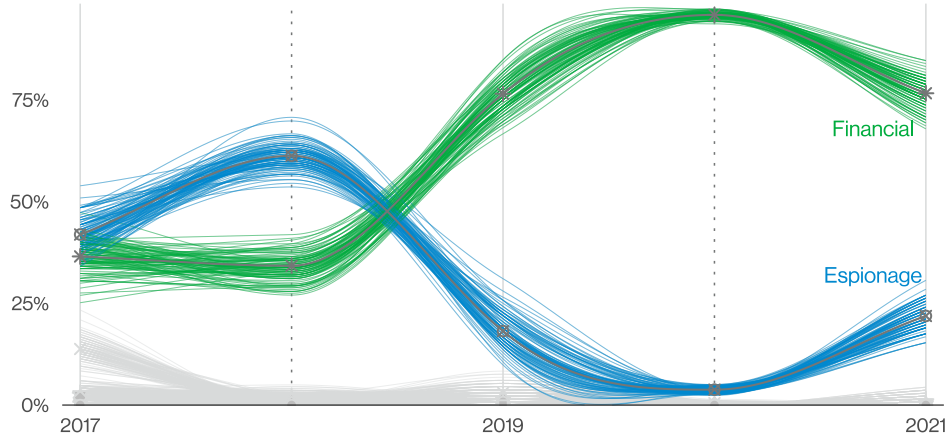


Figure 6. Actor motives over time in Public Administration breaches

CIS Critical Security Controls

The CIS Critical Security Controls (CIS CSC) is a community-built, prioritized list of cybersecurity best practices that help organizations of different maturity levels protect themselves against threats. Since 2019 we've published a mapping document that can help organizations crosswalk the patterns that are most concerning to them with the Safeguards that can protect them from the attacks within those patterns.

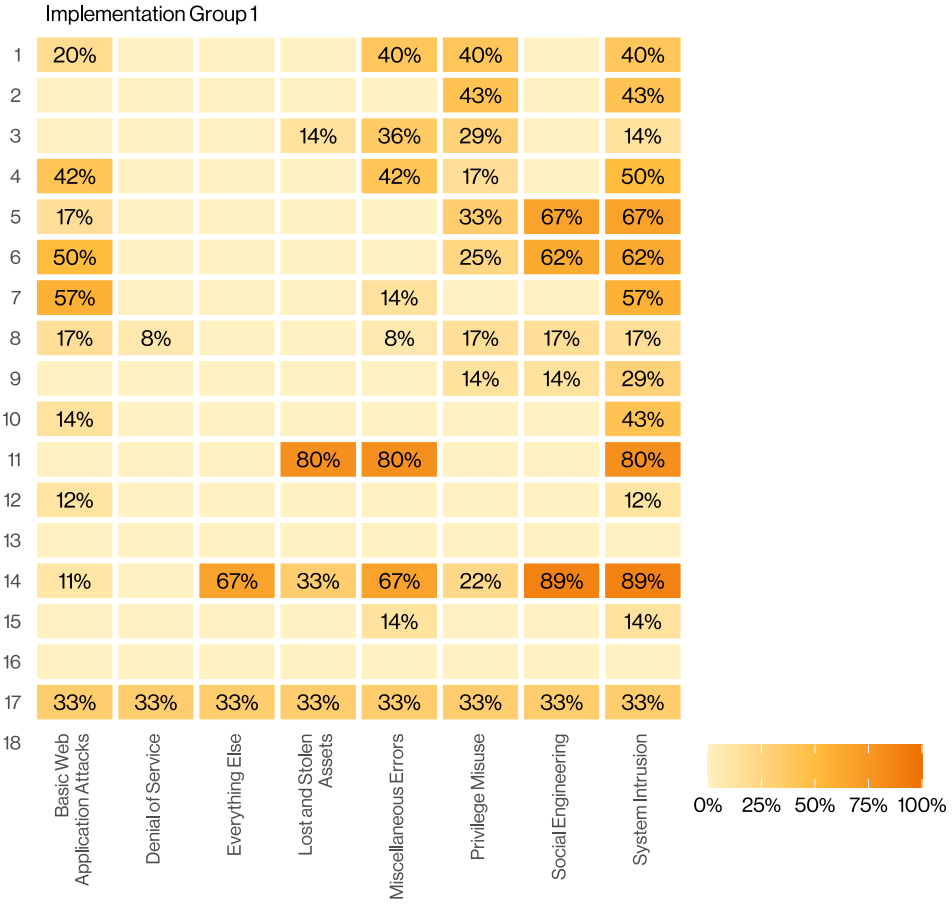


Figure 7. CIS to pattern mapping

Stay informed and threat ready.

As always, it is our hope that you have found the information herein to be informative, actionable and enjoyable to read. While we do our best to bring the occasional smile to our readers, we assure you that we take cybercrime seriously indeed. The five of us on the DBIR team feel truly fortunate to be in this fight alongside each and every one of you. We will do our best to keep providing you with whatever insight we can from our data, and we wish all of you the greatest success. Here is to a brighter tomorrow! We hope to see you all again next year. We will close with a line from a former report that we feel is particularly apropos.

"Be well, be prosperous and be prepared for anything."

Read the full 2022 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