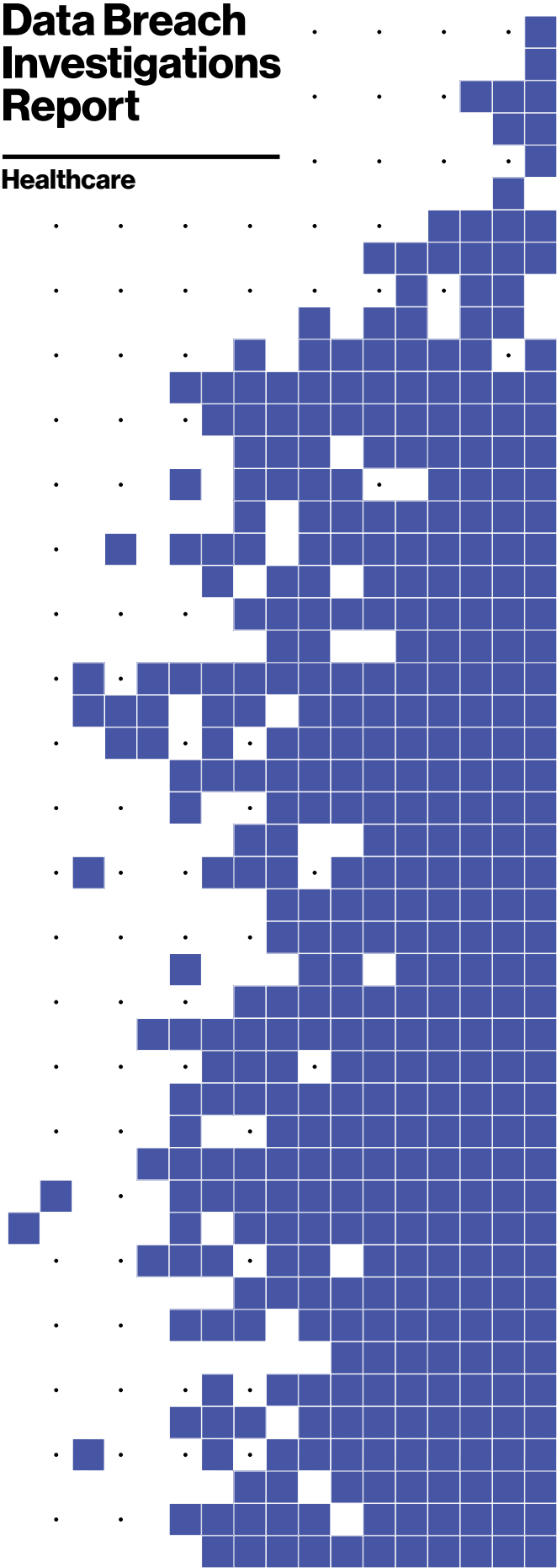
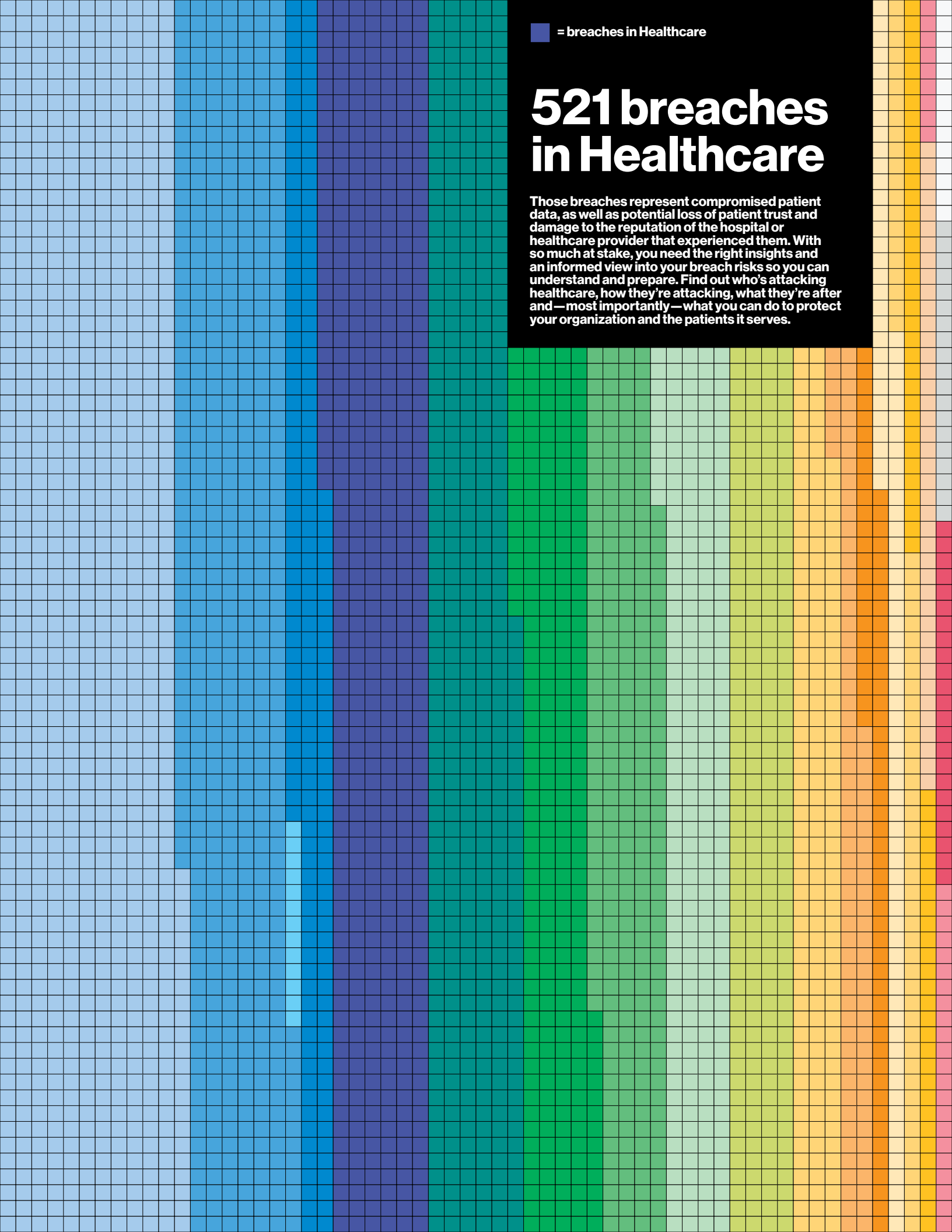
DBIR

2020 Data Breach Investigations Report

Healthcare



verizon


= breaches in Healthcare
521 breaches in Healthcare
Those breaches represent compromised patient data, as well as potential loss of patient trust and damage to the reputation of the hospital or healthcare provider that experienced them. With so much at stake, you need the right insights and an informed view into your breach risks so you can understand and prepare. Find out who's attacking healthcare, how they're attacking, what they're after and—most importantly—what you can do to protect your organization and the patients it serves.

Introduction to Healthcare

If there's one constant in our technology-driven world, it's that data breaches remain as ubiquitous as ever. Not surprisingly, as our world becomes more connected, each connection point represents a new entryway for would-be attackers.

Perhaps the best way to keep out of an attacker's crosshairs is to stay informed. The better you understand how attack trends are evolving and what threats you're likely to face, the more focused you can be in your security planning.

The *2020 Data Breach Investigations Report* (DBIR) offers critical insights into today's cybersecurity landscape. Findings are based on extensive data—the DBIR team analyzed 32,002 security incidents, including 3,950 confirmed breaches, from 81 countries around the world.

This snapshot highlights important takeaways for the Healthcare sector.

32,002

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

Healthcare snapshot

Key findings

Data from this past year reveals that financially motivated criminal groups continue to target the Healthcare 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)

Reading the charts

This year, we saw a substantial increase in the number of breaches and incidents reported in our overall dataset, and that rise is reflected within the Healthcare vertical. In fact, the number of confirmed data breaches in this sector came in at 521 versus 304 in last year's report. Since this is the *Data Breach Investigations Report*, we tend to put more focus on actual confirmed breaches. But in Healthcare, given the Department of Health and Human Services (HHS) guidance on ransomware cases for example, the incidents hold higher relevance than they might in a different vertical despite the data being simply "at-risk" rather than a confirmed compromise.

Figure 1 shows the breakdown of the patterns for incidents in Healthcare. The Crimeware pattern includes Ransomware incidents, and as one might expect, that pattern accounts for a large portion of the incidents in this sector. If we drop further down the list in this chart, we see that one pattern that tends to get lost in the shuffle is Lost and Stolen Assets. Because the asset is not available, proving whether the data was accessed or not is no simple matter. Therefore, we code these as incidents with data being "at-risk" rather than as a confirmed compromise. Our caution to the reader is not to assume that because the attacks aren't showing up as confirmed breaches in our dataset, you won't have to declare a breach according to the rules that govern your industry.

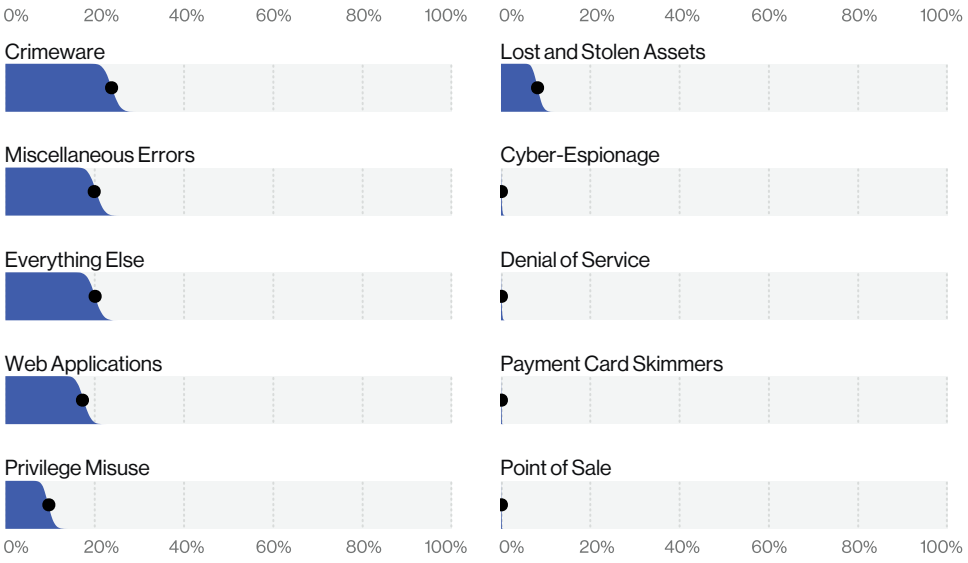


Figure 1. Patterns in Healthcare industry incidents (n = 798)

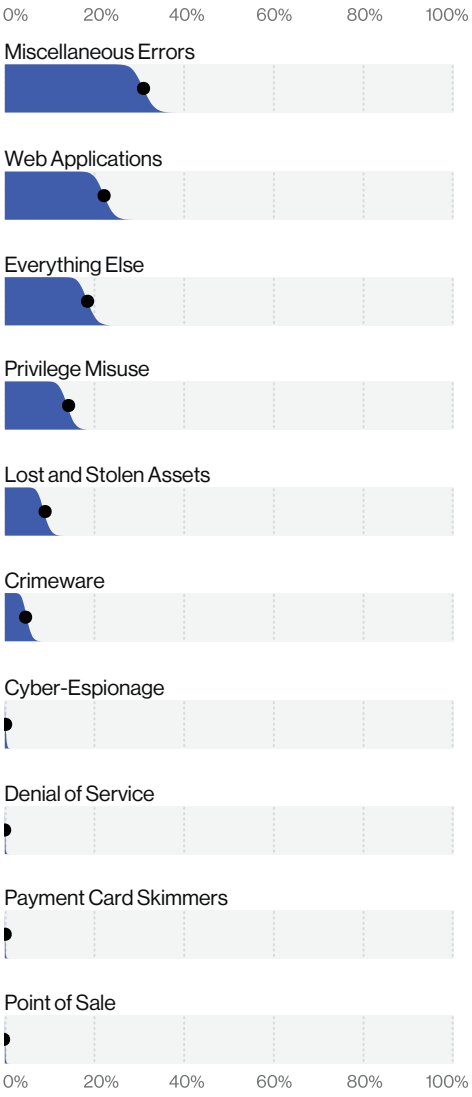


Figure 2. Patterns in Healthcare industry breaches (n = 521)

Take three patterns and call me in the morning.

If you've been following the Healthcare section for some time, you may notice a big change in the breach pattern rankings on Figure 2. This is the first year that the Privilege Misuse pattern is not in the top three. However, this pattern saw a significant proportional drop in our dataset overall—not just in the Healthcare vertical. In the 2019 report, we showed Privilege Misuse at 23% of attacks, while in 2020, it has dropped to just 8.7%. Does that indicate that insiders are no longer committing malicious actions with the access granted to them to accomplish their jobs? Well, we wouldn't go quite that far. However, it will be interesting to see if this continues as a trend when next year's data comes in.

Another change that goes along with decreased insider misuse breaches is the corresponding drop in multiple actor breaches. The Healthcare sector has typically been the leader in this type of breach—which usually occurs when External and Internal actors combine forces to abscond with data that is then used for financial fraud. The multiple actor breaches last year were at 4%, and this year we see a drop to 1%. The 2019 DBIR reported a first in that the Healthcare vertical had Internal actor breaches (59%) exceeding those perpetrated by External actors (42%). This year, External actor breaches are slightly more common at 51%, while breaches perpetrated by Internal actors fall to 48%. However, this is a small percentage, and Healthcare remains the industry with the highest amount of internal bad actors.

As with many things in life, as one attack grows more prevalent, others begin to decrease. So the story goes with the Miscellaneous Errors pattern. While it has frequently graced the top three patterns in this sector, it took the gold this year. In case you are curious, the top mistake within Healthcare is our old friend, Misdelivery.

This Error tends to fall into two major categories:

- Someone is sending an email and addresses it to the wrong (and frequently wider) distribution—it's an added bonus if a file containing sensitive data was attached
- An organization is sending out a mass mailing (paper documents) and the envelopes with the addresses become out of sync with the contents of the envelope. If sampling is not done periodically throughout the mailing process to ensure that they remain *NSYNC, then it's bye, bye, bye to your patients' sensitive information

When thinking of the Healthcare vertical, one naturally thinks of Medical data. And, unsurprisingly, this is the industry in which that type of data is the most commonly breached. However, we also see quite a lot of both Personal data (which can be anything from basic demographic information to other covered data elements) and Credentials stolen in these attacks. The second most common pattern for Healthcare is the Web Applications attack. As more and more organizations open patient portals and create new and innovative ways of interacting with their patients, they create additional lucrative attack surfaces.

Finally, we see a good deal of the Everything Else pattern, which is not unlike a lost and found for attacks that do not fit the criteria of any other attack pattern. It is within this pattern that the business email compromise resides. If you're not familiar with this attack, it is typically a phishing attack with the aim of leveraging a pretext (an invented scenario to give a reason for the victim to do what the attacker wants) to successfully transfer money (by wire transfer, gift cards or any other means). Although these are common attack types across the dataset, it is a good reminder to Healthcare organizations that it isn't only patient medical data that is being targeted.

Learn more about Verizon solutions that can help you secure, innovate and grow your business.

View Verizon solutions for Healthcare here: enterprise.verizon.com/solutions/industry/healthcare/

When did you first notice these symptoms?

The time required to compromise and exfiltrate data has been getting smaller in our overall dataset. Unfortunately, the time required for an organization to notice that they have been breached is not keeping pace. There is a discrepancy there somewhat akin to how long it takes you to earn your wages vs how long it takes for them to be taxed. Some attacks, by their very nature, will both happen quickly and be detected quickly. A good example is a stolen laptop—how long does it take someone to smash a car window and make off with the loot? (That is a rhetorical question, so don't mail in answers; there is no prize for getting it right.) Likewise, it also doesn't take much time for the owner to come back to their car and see the break-in.

Both of these will have a short duration due to the nature of the crime. In contrast, an insider who has decided to abuse their access to copy a small amount of data each week and sell it to their buddy who in turn utilizes it for financial fraud may not be caught for a very long time.

Recommended best practices

This year we've aligned our findings with the Center for Internet Security Critical Security Controls (CSCs) 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 Configuration (CSC 5 and 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 Defense (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, both 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 2020 DBIR contains details on the actors, actions and patterns that can help you prepare your defenses. Get the intelligence you need to protect your organization.

Read the full 2020 DBIR at verizon.com/dbir

Take our free Security Readiness Assessment to see how your security stacks up.