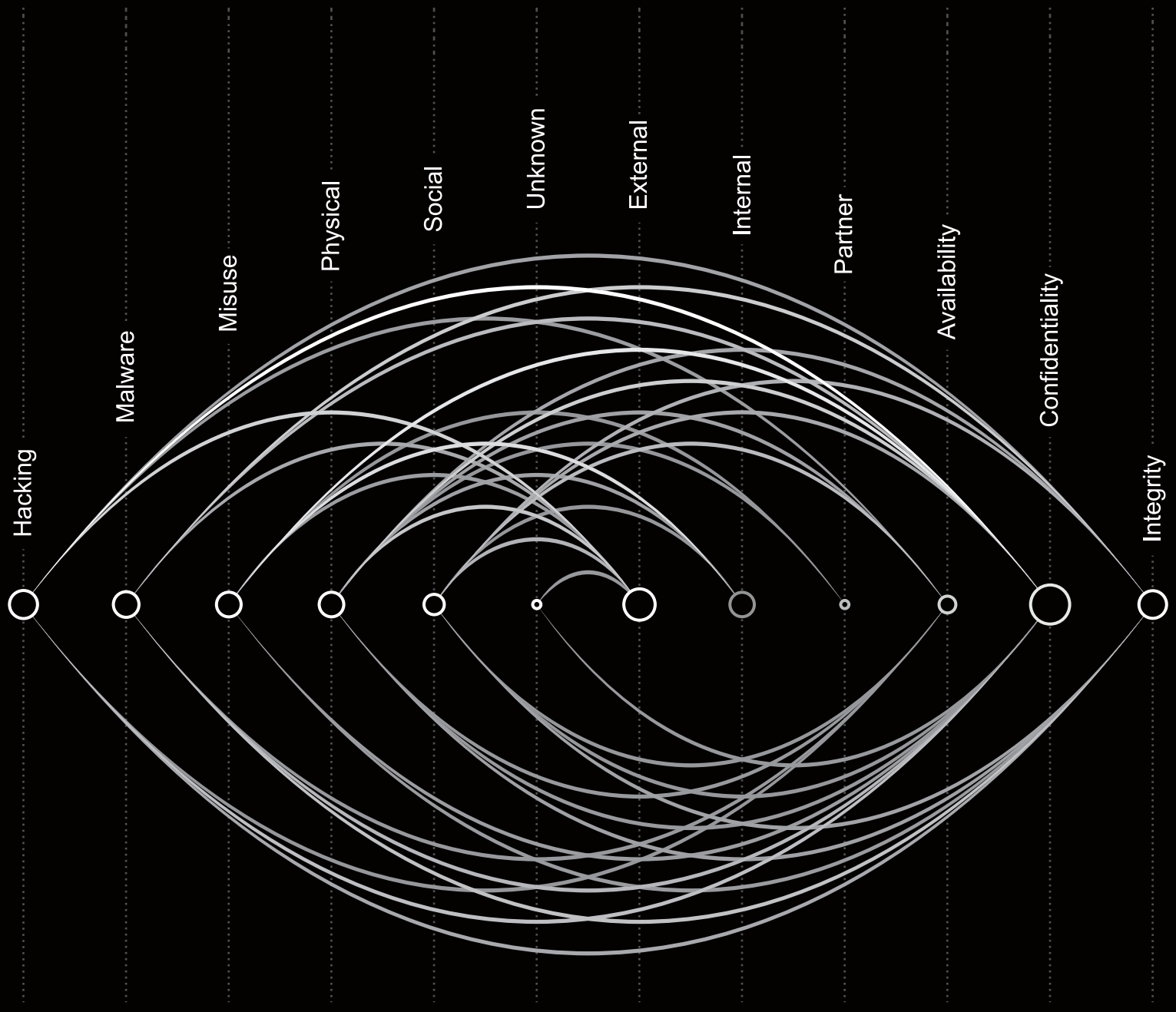
Executive summary

2018 Data Breach Investigations Report



verizon

verizon

Your organization's security depends on you.

Data breaches aren't just a problem for security professionals. The impact is felt across the whole business – from your legal team, embroiled in litigation, to your frontline employees, who can't access the tools they need to do their jobs. Everyone needs to play their part in managing the risks. But first you need to understand what you're up against.

You need confidence in your security if you're going to get the most from the latest digital innovations. That's why, every year, we publish the Data Breach Investigations Report (DBIR) – this is our 11th edition. Each report is based on analysis of thousands of real-world incidents – over 53,000 this year, including 2,216 confirmed data breaches.

53,308 security incidents, 2,216 data breaches, 65 countries, 67 contributors.

This year we saw, yet again, that cybercriminals are still finding success with the same tried and tested techniques, and their victims are still making the same mistakes.

Let's start you on the path to improved security by examining who has you in their sights, what they're after and how they plan to get their hands on it.

It will probably be you one day

Most cybercriminals are motivated by cold, hard cash. If there's some way they can make money out of you, they will. That could mean stealing payment card data, personally identifiable information or your intellectual property.

And they don't care who they take it from. Ignore the stereotype of sophisticated cybercriminals targeting billion-dollar businesses. Most attacks are opportunistic and target not the wealthy or famous, but the unprepared.

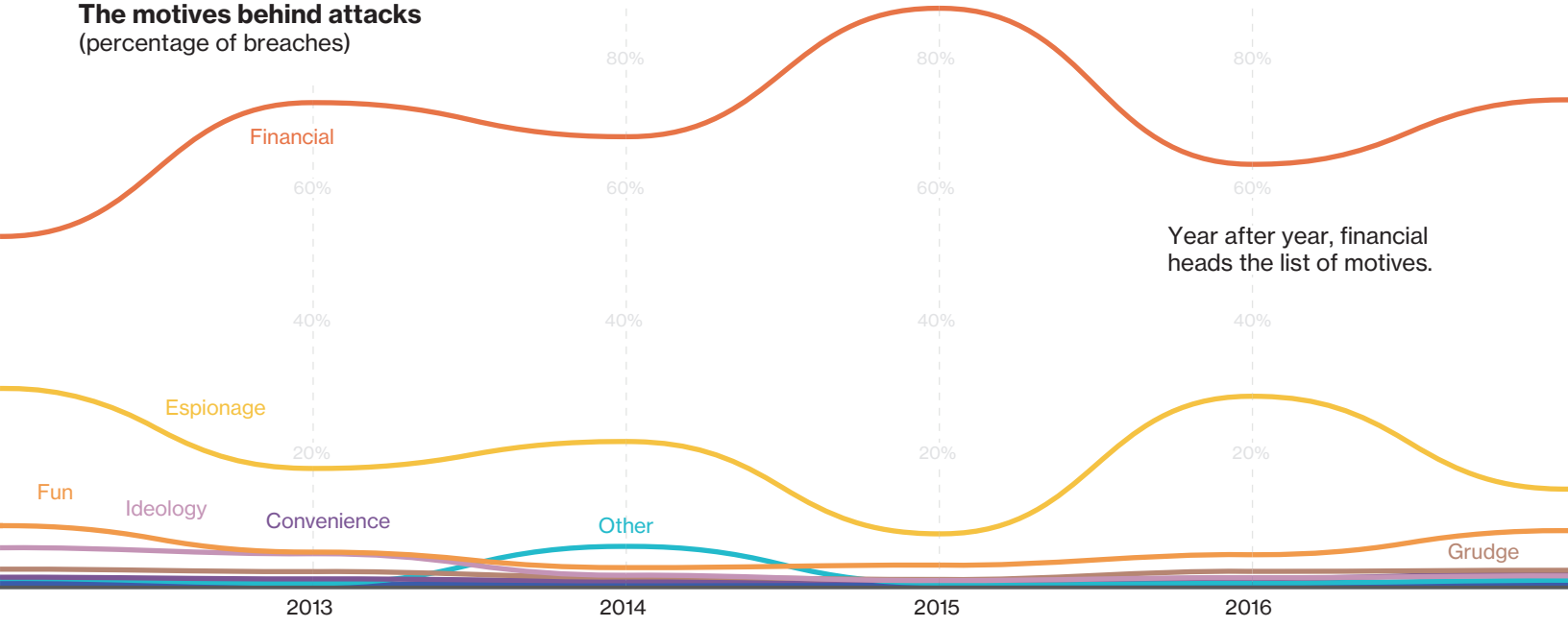
76% of breaches were financially motivated.

So who are you up against?

Almost three-quarters (73%) of cyberattacks were perpetrated by outsiders. Members of organized criminal groups were behind half of all breaches, with nation-state or state-affiliated actors involved in 12%.

Not all the baddies are outsiders though. Over a quarter (28%) of attacks involved insiders. The insider threat can be particularly difficult to guard against – it's hard to spot the signs if someone is using their legitimate access to your data for nefarious purposes.

The motives behind attacks
(percentage of breaches)



verizon

People make mistakes

Malicious employees looking to line their pockets aren't the only insider threat you face. Errors were at the heart of almost one in five (17%) breaches. That included employees failing to shred confidential information, sending an email to the wrong person or misconfiguring web servers. While none of these were deliberately ill-intentioned, they could all still prove costly.

4% of people will click on any given phishing campaign.

This is something we've been saying for the last three years, and sadly it's still true today – people are still falling for phishing campaigns. The good news is that 78% of people don't click on a single phishing campaign all year. But, on average, 4% of the targets in any given phishing campaign will click it. And incredibly, the more phishing emails someone has clicked, the more likely they are to do so again.

You have 16 minutes until the first click on a phishing campaign. The first report from a savvy user will arrive after 28 minutes.

Don't get held to ransom

Cybercriminals don't have to steal data to make money – they can just stop you using it. We first saw ransomware rear its ugly head in the 2013 DBIR. In this year's report, it's the most prevalent variety of malware.

Ransomware is the top variety of malicious software, found in 39% of cases where malware was identified.

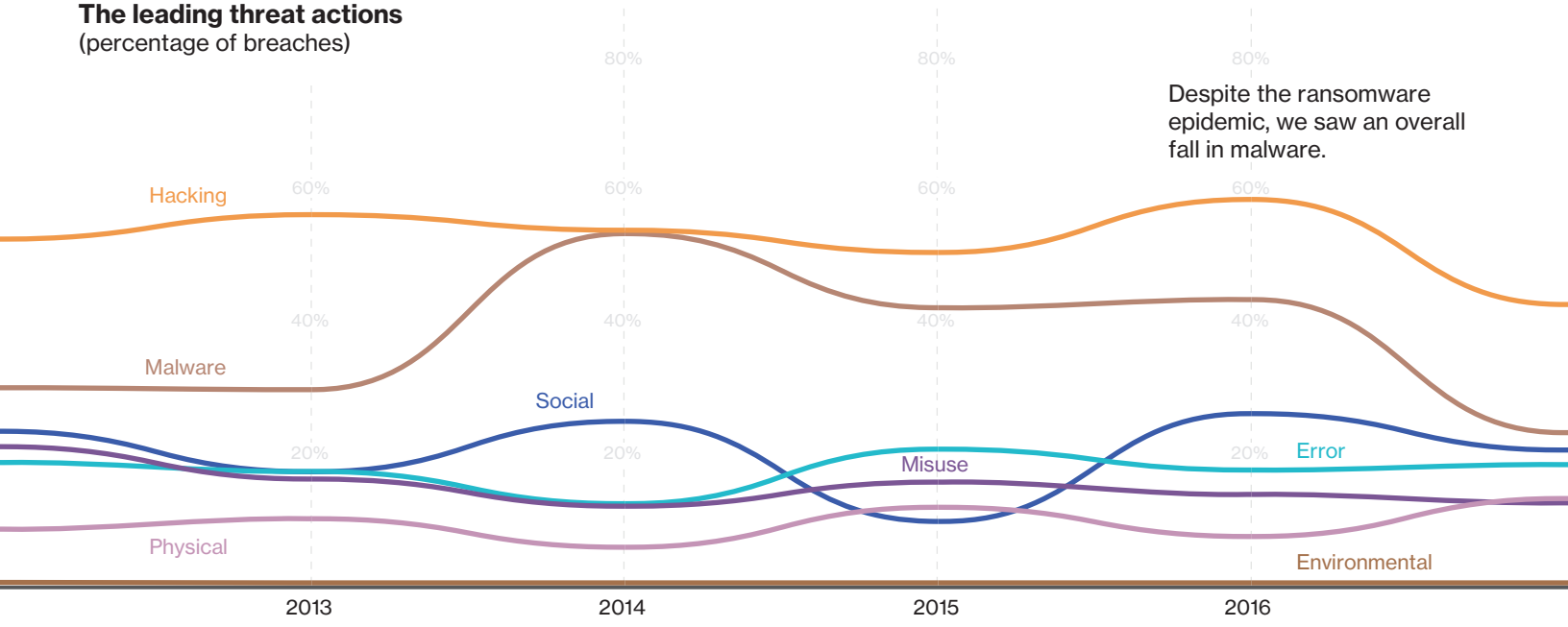
Why has ransomware become so commonplace? Because it's easy to deploy and can be very effective – you don't have to be a master criminal; off-the-shelf toolkits allow any amateur to create and deploy ransomware in a matter of minutes. There's little risk or cost involved and there's no need to monetize stolen data.

Increasingly, cybercriminals aren't looking to just encrypt single user devices. They can do much more damage, and make much more money, if they can encrypt a file server or database. If you aren't backed up, they could take your business offline.

What you can do

Read on to discover the biggest threats to your industry.

The leading threat actions
(percentage of breaches)



verizon

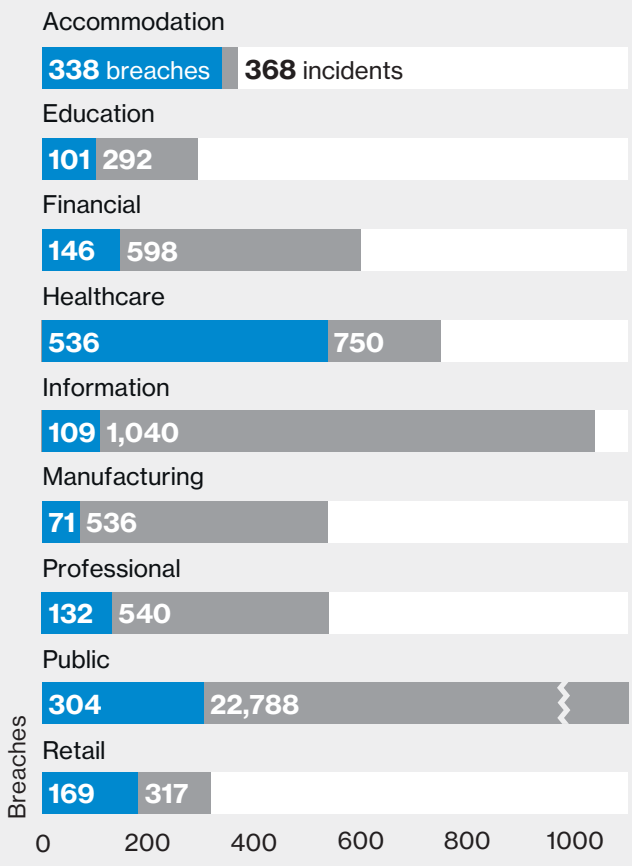
What's the biggest risk to your business?

Each industry faces a different mix of threats. By understanding the biggest threats to your industry, you'll be able to make best use of your security budget and mitigate the risks.

We report on the threats facing nine industries in this year's DBIR – you can see a summary of the findings below. If your sector isn't there, that doesn't mean you're safe; it just means we didn't have a large enough pool of data to enable us to provide valid insights.

The 2018 DBIR provides a lot more detail on the threats facing each industry, as well as guidance on the steps you can take to manage the risks.

Number of incidents and breaches by sector



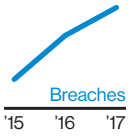
Accommodation

Who	99% external, 1% internal
What	93% payment, 5% personal, 2% credentials
How	93% hacking, 91% malware

It's pretty clear-cut where you need to focus. 90% of all breaches involved POS intrusions. In fact, you're over 100 times more likely than the median industry in our dataset to have a POS controller targeted.

Education

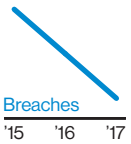
Who	81% external, 19% internal
What	72% personal, 14% secrets, 11% medical
How	46% hacking, 41% social



Social engineering scams are targeting your employees' personal information, which is then used to commit identity fraud. Your highly sensitive research is also at risk – 20% of attacks were motivated by espionage. But sometimes the threats aren't about stealing data for financial gain – 11% of attacks have "fun" as their motive.

Financial

Who	79% external, 19% internal
What	36% personal, 34% payment, 13% bank
How	34% hacking, 34% physical

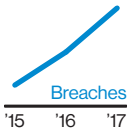


You still need to be alert to payment card skimmers installed on ATMs by organized criminal groups. Now there's ATM jackpotting too, where software or hardware is installed to make the ATM spit out money. There's also still a very real threat that denial of service attacks could disrupt your operations.

verizon

Healthcare

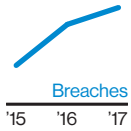
Who	43% external, 56% internal
What	79% medical, 37% personal, 4% payment
How	35% error, 24% misuse



Healthcare is the only industry where the threat from inside is greater than that from outside. Human error is a major contributor to those stats. Employees are also abusing their access to systems or data, although in 13% of cases, it's driven by fun or curiosity – for example, where a celebrity has recently been a patient.

Professional

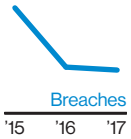
Who	70% external, 31% internal
What	56% personal, 28% credentials, 16% internal
How	50% hacking, 21% social



Attacks are typically financially motivated and often involve phishing or the use of stolen credentials. There's also a danger from your employees making mistakes. While data is typically compromised in hours or less, it can be days before a breach is discovered – typically by a third party.

Information

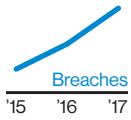
Who	74% external, 23% internal
What	56% personal, 41% credentials, 9% internal
How	57% hacking, 26% error



Web application attacks, most often using stolen credentials, are a major issue. Employee error is also having an impact – typically due to misconfigured databases or publishing errors. But perhaps the biggest threat you face is from denial of service attacks – they account for 56% of the incidents witnessed in 2017.

Public

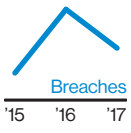
Who	67% external, 34% internal
What	41% personal, 24% secrets, 14% medical
How	52% hacking, 32% social



Cyberespionage remains a major concern – espionage was a motive for 44% of breaches. Attacks usually involve phishing, installations and the use of backdoors or C2 channels. But it's not just state secrets being targeted – the personal data you hold on citizens and employees is also at risk.

Manufacturing

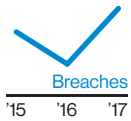
Who	89% external, 13% internal
What	32% personal, 30% secrets, 24% credentials
How	66% hacking, 34% malware



Looking at all-industry data, most cyberattacks are opportunistic. But in manufacturing, 86% are targeted. That target is often the planning, research and development for your new solution. Almost half (47%) of breaches involved the theft of intellectual property to gain competitive advantage.

Retail

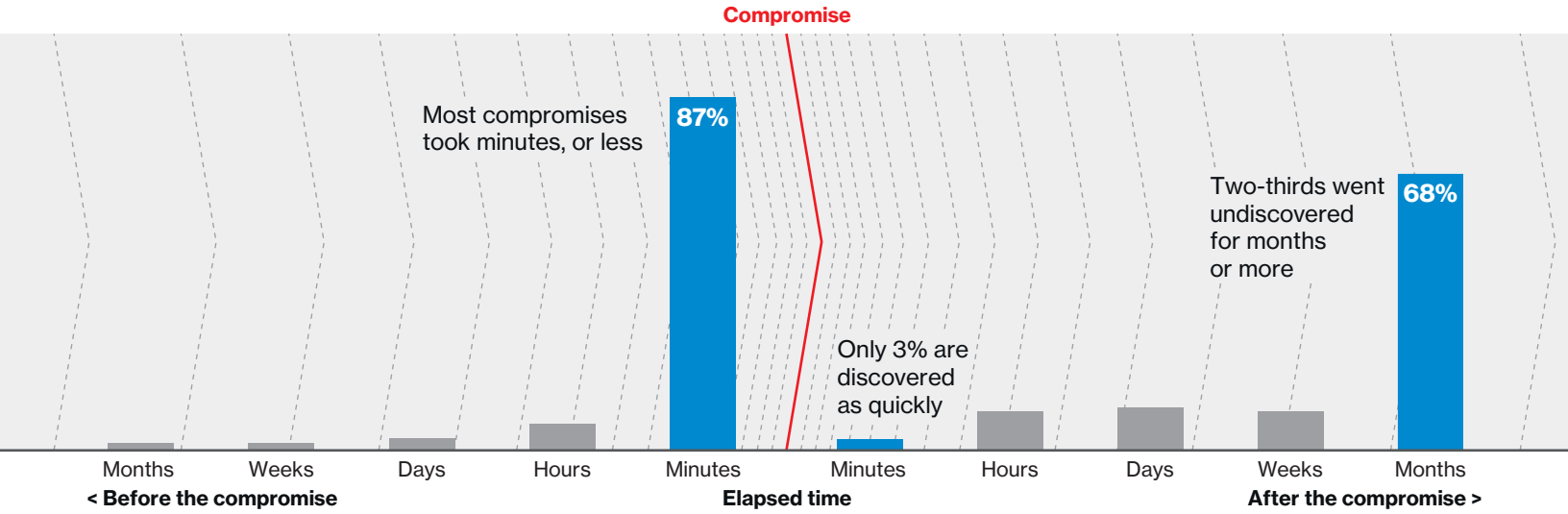
Who	91% external, 10% internal
What	73% payment, 16% personal, 8% credentials
How	46% hacking, 40% physical



In terms of data theft, web application attacks leveraging poor validation of inputs or stolen credentials came top. But it's not just the theft of data you need to worry about. Denial of service attacks can have serious consequences, including preventing transactions being processed and slowing down your website and in-store systems.

verizon

It's time to act.



The time it takes cybercriminals to compromise a system is often just a matter of minutes – or even seconds. They don't need much time to extract valuable data – they usually have much more than they need as it typically takes organizations weeks or months to discover a breach.

68% of breaches took months or longer to discover.

In many cases, it's not even the organization itself that spots the breach – it's often a third party, like law enforcement or a partner. Worst of all, many breaches are spotted by customers. You don't need us to tell you how bad that would be for your brand reputation.

Protecting your good name comes down to two things: defense and response. You should build defenses that are strong enough to send cybercriminals in the direction of an easier target. But no defense is 100% effective. Should an attacker get through, you need to be prepared to respond quickly and effectively.

What you can do

Be vigilant
Don't wait to find out about a breach from law enforcement or a customer. Log files and change management systems can give you early warning of a security compromise.

Make people your first line of defense
Do your employees understand how important cybersecurity is to your brand, and your bottom line? Get them on board, and teach them how to spot the signs of an attack and how to react.

Only keep data on a need-to-know basis
Do you know who can see your sensitive data and systems? Limit access to the people who need it to do their jobs, and have processes in place to revoke it when they change roles.

Patch promptly
Cybercriminals are still successfully exploiting known vulnerabilities. You can guard against many threats simply by keeping your anti-virus software up to date.

Encrypt sensitive data
Do what you may, one day you're likely to be the victim of a breach. But by encrypting your data you can render it useless if it is stolen.

Use two-factor authentication
Phishing campaigns are still hugely effective. And employees make mistakes. Two-factor authentication can limit the damage that can be done if credentials are lost or stolen.

Don't forget physical security
Not all data theft happens online. Surveillance cameras and entry systems for restricted areas, for example, can help avoid criminals tampering with systems or stealing sensitive material.

verizon

Leverage our intelligence.

Attackers are constantly developing new tactics to help them access your systems and data. But what's clear from our research is that too many organizations continue to make their job easy. Some companies are failing to take the most basic of security measures – like keeping anti-virus software up to date or training staff on how to spot the signs of an attack.

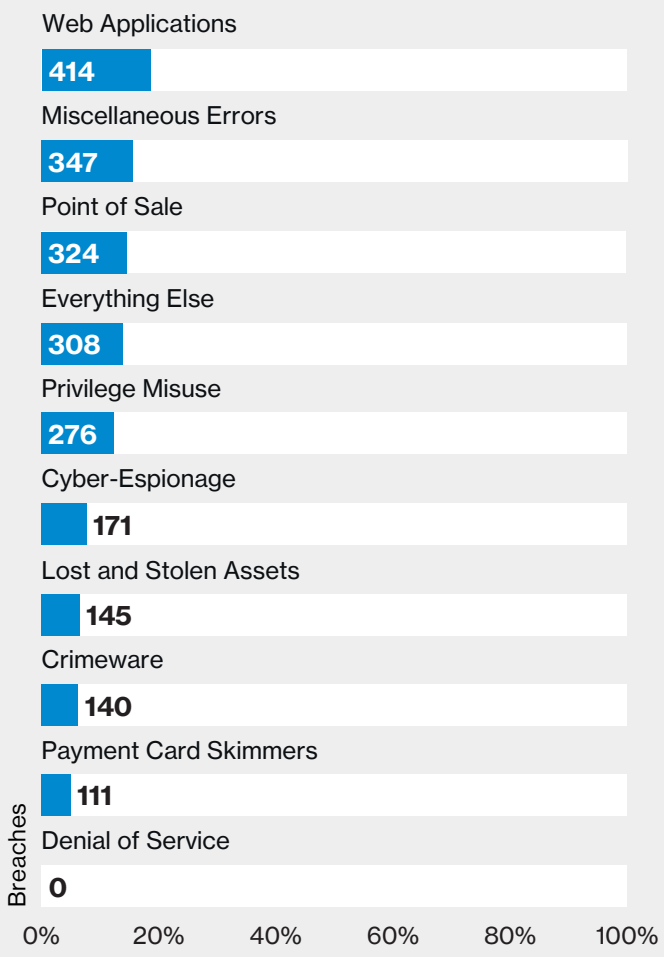
The best way to mitigate the risks is to understand the threats you face. The DBIR can help. Back in 2014, we identified nine incident patterns that cover most of the threats you're likely to face – and these still hold true today.

94% of security incidents and 90% of confirmed data breaches fall into our nine incident classification patterns across all years.

These patterns give you a quick and easy way to assess the biggest risks to your business. That means if you're commissioning a new app or updating systems, you can build more effective security in from the start. And it means that security professionals can prioritize their spend.

For more information on the patterns and how they relate to your industry, take a look at the 2018 DBIR.

Breaches by pattern

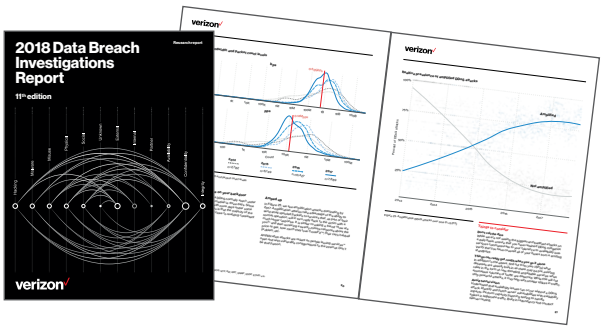


The Verizon Data Breach Investigations Report can help you understand the threats to your organization, and how you can mitigate the risks.

The 2018 report is based on a detailed analysis of over 53,000 security incidents, including 2,216 confirmed data breaches. Now in its 11th year, the DBIR has established itself as one of the security industry's most respected sources of information.

Download the full report:

verizonenterprise.com/DBIR2018



About the cover

The arc diagram on the cover is based on the data in Appendix C: Beaten paths in the main report. It illustrates the actors, actions, and attributes as nodes; and the order of their occurrence in attack paths as edges. We've counted how many times each node occurs in each path and sized them accordingly – the larger the node, the more times it appeared. The edges between nodes are represented as arcs between points. The color of each arc is based on how often an attack proceeds between those two nodes.

verizonenterprise.com