An overview: security depends on you.

Data breaches aren't just a problem for security professionals. The impact is felt across the whole organization — from your legal team embroiled in litigation, to your 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 bad actors 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 data for nefarious purposes.

The motives behind attacks (percentage of breaches)

Year after year, financial heads the list of motives.
Recognize that people make mistakes

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.

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 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.

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.

The leading threat actions (percentage of breaches)

Despite the ransomware epidemic, we saw an overall fall in malware.
It’s time to act.

What you can do

Be vigilant
Don’t wait to find out about a breach from law enforcement. 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.
Cyberespionage remains a large concern for the public sector, with state-affiliated actors accounting for over half of all breaches. Privilege misuse and error by insiders account for a third of breaches.

<table>
<thead>
<tr>
<th>Frequency</th>
<th>22,788 incidents, 304 with confirmed data disclosure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top patterns</td>
<td>Cyber-Espionage, Privilege Misuse, Everything Else, Web Applications, and Miscellaneous Errors represent 92% of breaches</td>
</tr>
<tr>
<td>Threat actors</td>
<td>External (67%), Internal (34%), Partner (2%), Multiple parties (3%) (breaches)</td>
</tr>
<tr>
<td>Actor motives</td>
<td>44% Espionage, 36% Financial, 14% Fun (breaches)</td>
</tr>
<tr>
<td>Data compromised</td>
<td>Personal (41%), Secrets (24%) Medical (14%)</td>
</tr>
</tbody>
</table>

Close enough for government work

A quick look at the number of incidents within this industry could provide many citizens with another point of frustration to take up with the government. But, as in prior years, it is our duty to point out that there is more going on here than meets the eye. In the United States, entities of the federal government are required to report security incidents to the US-CERT. Thanks in large part to these agencies and other contributors we have a degree of visibility into what is going on in the public sector in the US. It is important to keep in mind that many of these incidents are of the general policy violations ilk, or routine malware events in which a system gets infected and is cleaned up by a regular process that does not result in any breach of data. No harm, no foul. In other industry verticals they would not be required to disclose such events, and therefore we do not see them. For the purposes of this report, we will focus on the 304 confirmed data breaches that were reported.
The past several years have provided us with a few constants with regard to attack patterns for this sector. The familiar faces looking back at us this time include Cyber-Espionage, Privilege Misuse and Miscellaneous Errors to name a few. This year we have a rat pack of five patterns that show statistically similar numbers, with a new arrival in the form of the Everything Else pattern.²²

The consistent association of espionage with government targets is not shocking. Governments like to know what their counterparts in other countries are up to, and this year is no different. When the threat actor is known, state-affiliated adversaries tend to figure somewhat prevalently.

Phishing attacks, installations and subsequent uses of backdoors or C2 channels are front and center in espionage related breaches. Malware functionalities that are often used to pop credentials, in the form of keyloggers and password dumpers, are also found in significant numbers.

---

²² Over three-quarters of the breaches within Everything Else featured hacking as an action. Unfortunately, most did not have a particular variety of hacking recorded, nor what asset was affected.
Personnel’s personalities and personal information

Governments have a unique relationship to the people whose data they maintain—there are a number of roles, depending on the area and level of the government. Governments are storing information not only for citizens they serve, but also the citizens under their employ—governments remain the largest employer for most countries. Personal information is in the top group of data varieties lost in Public Administration breaches, along with secrets\(^2\) attributed to espionage.

Not only do governments have to worry about the protection of personal data, but also must address personnel as a likely driver of breaches.

Public Administration trails only Healthcare in the prevalence of insiders as causal actors in data breaches. Malicious or inappropriate behavior is categorized in the Privilege Misuse pattern. Most often the misuse is privilege abuse (78%) which is using existing privileges in a manner that is unauthorized and/or out of policy. Mishandling of data and unapproved workarounds (both 24%) are other ways that insiders will misuse their access to systems and data. Erroneous behavior will fall either into Miscellaneous Errors, where acts such as mis-delivery of data or publishing errors are recorded, or Lost and Stolen Assets if the breach was caused by a misplaced organizational asset.

Finally, with regard to timelines, the small sample of breaches where time to compromise was known were indicative of quick compromises, much like we see for the entire dataset. In contrast, almost half of breaches were discovered months or years after the initial compromise.

<table>
<thead>
<tr>
<th>Breaches</th>
<th>Per cent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal</td>
<td>41%</td>
</tr>
<tr>
<td>Secrets</td>
<td>24%</td>
</tr>
<tr>
<td>Medical</td>
<td>13%</td>
</tr>
<tr>
<td>Credentials</td>
<td>13%</td>
</tr>
<tr>
<td>Internal</td>
<td>13%</td>
</tr>
<tr>
<td>System</td>
<td>9%</td>
</tr>
<tr>
<td>Classified</td>
<td>7%</td>
</tr>
<tr>
<td>Payment</td>
<td>3%</td>
</tr>
<tr>
<td>Bank</td>
<td>1%</td>
</tr>
</tbody>
</table>

Data compromised in Public Sector breaches (n=250)

Things to consider

Everybody wants you

Depending on function, government entities may be targeted by state-affiliated groups, organized crime or employees. Keep in mind the type of data you handle and consider who might benefit from access to it and plan your security accordingly.

 Auditor, audit thyself

Detection and remediation times are poor. Conduct routine monitoring and security audits to help stop the bleeding faster.

It’s a privilege, not a right

Make sure that access privileges are provided on a “need to know” basis and have exit programs in place when employees leave the organization to ensure access to systems is closed upon their exit.

---

23. The VERIS (Vocabulary for Event Recording and Incident Sharing) framework features a data variety of Secrets as well as Classified. It is likely that many of the breaches actually dealt with classified information as opposed to intellectual property.
Leverage our intelligence.

Download and share the complete DBIR.

Attacker styles are constantly developing new tactics to help them access your systems and data. But what's clear from our research is that many organizations continue to make their job easy. Some organizations 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

<table>
<thead>
<tr>
<th>Breach Type</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Applications</td>
<td>414</td>
</tr>
<tr>
<td>Miscellaneous Errors</td>
<td>347</td>
</tr>
<tr>
<td>Point of Sale</td>
<td>324</td>
</tr>
<tr>
<td>Everything Else</td>
<td>308</td>
</tr>
<tr>
<td>Privilege Misuse</td>
<td>276</td>
</tr>
<tr>
<td>Cyber-Espionage</td>
<td>171</td>
</tr>
<tr>
<td>Lost and Stolen Assets</td>
<td>145</td>
</tr>
<tr>
<td>Crimeware</td>
<td>140</td>
</tr>
<tr>
<td>Payment Card Skimmers</td>
<td>111</td>
</tr>
<tr>
<td>Denial of Service</td>
<td>0</td>
</tr>
</tbody>
</table>

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