2016 Data Breach Investigations Report

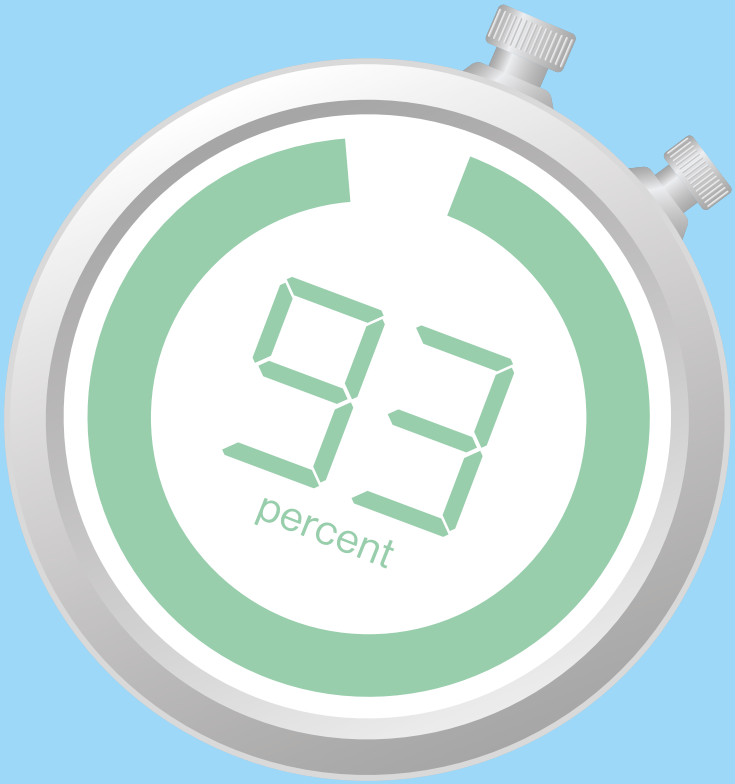
Executive Summary

Cybersecurity isn't just for security experts. The C-level guide to what you need to know.

verizon

Have you already been compromised?

In 93% of cases, it took attackers minutes or less to compromise systems. Organizations, meanwhile, took weeks or more to discover that a breach had even occurred – and it was typically customers or law enforcement that sounded the alarm, not their own security measures.



100,000+ incidents. Analysis of 2,260 breaches. 82 countries. 67 contributing organizations.

The Verizon Data Breach Investigations Report (DBIR) is accepted by security experts as an unparalleled source of insight – and our ninth edition is the most comprehensive yet. But if you're a CIO, CMO or CEO, you need to understand the risks too, and this guide is for you.

Security should be a driving force, not an afterthought.

Data is the power behind innovation. It's accelerating supply chains and redefining customer experiences. But companies and consumers are concerned about security. It's critical that you address risk, both to reassure your customers and to give you the confidence to embrace digital acceleration fully.

Every organization relies on digital in some way – to communicate, to transact, to compete. Today, gaining competitive advantage is about being able to do digital – better. But to do that, you need systems that are reliable and secure. And that means data security is something we all need to care about.

Data breaches are expensive. It's not just restitution and fines; fees for legal and remediation services can be substantial, too. Breaches can also cost you in terms of brand reputation. That's particularly crucial because having the trust of your customers and partners has never been more important.

A breach probably won't put you out of business immediately, but can seriously damage your future.

Say you're a DIY store. Customers may still shop at your outlet – though they will probably be more likely to pay by cash – but will they download your new app or buy your new connected home solution?

Most breaches are about money

Forget that Hollywood movie. Most cyberattacks are indiscriminate and motived by greed – not revenge or public service. Most attackers are out to steal your data because of what it's worth, not who you are. Anything that can be converted to money will do. As the value of payment card information falls – as banks improve fraud detection – attackers may increasingly turn to things like intellectual property and protected health information.

Attackers take the easiest route

It would be a mistake to think the biggest risk you face is from new-to-the-world vulnerabilities. Most attacks exploit known vulnerabilities – where a patch has often been available for months, if not years.

63% of confirmed data breaches involved leveraging weak, default or stolen passwords.

Often the reason why criminals were so quick at breaking in was that they already had the key. Social engineering remains worryingly effective – "click here to reset your banking password". We found that almost a third (30%) of phishing messages were opened – up from 23% in 2014. And 12% of targets went on to open the malicious attachment or click the link – about the same as 2014 (11%).

Make their lives more difficult

There's no such thing as an impenetrable system, but often even a half-decent defense will deter many cybercriminals – they'll move on and look for an easier target. Sadly, many organizations fail to achieve even that modest ambition.

95% of breaches fit into nine patterns.

This year's DBIR again focuses on the nine incident patterns we identified in 2014. Understanding them will help you focus your security efforts on the right areas.

95% of breaches, and 86% of incidents, are covered by just nine patterns.

Spend smarter.

The bad guys keep improving and your infrastructure is evolving faster than ever. How can you keep on top without breaking the bank?

The pressure on organizations to become more digital is growing by the day. There are more devices to protect, more people with access to data and ever more partners to integrate with.

New technologies—like mobile and the Internet of Things (IoT)—threaten to give attackers new opportunities.

We've not seen a significant volume of incidents involving mobile or IoT devices yet. But the threat is certainly real. Proof of concept exploits have been demonstrated and it's only a matter of time before we see a large-scale breach.

Nine patterns describe 80%+

Incidents
Breaches

Switch

And the bad guys are upping their game. They're having to because the market value of some kinds of data, particularly payment card information, is falling. To maintain their income, attackers must steal more data or find new, more lucrative forms of information to sell – like protected health information and intellectual property.

You need to hit them where it hurts – in their wallets. But you haven't got a limitless budget. That means you need to spend smarter. The nine incident classification patterns we first published in 2014 cover the vast majority of both incidents and confirmed breaches, as shown in Figure 1. And when you look at any single industry, the majority of threats fall into just three patterns – see Figure 2. Studying these patterns will help you understand how to best deploy your limited headcount and budget to achieve the best results.

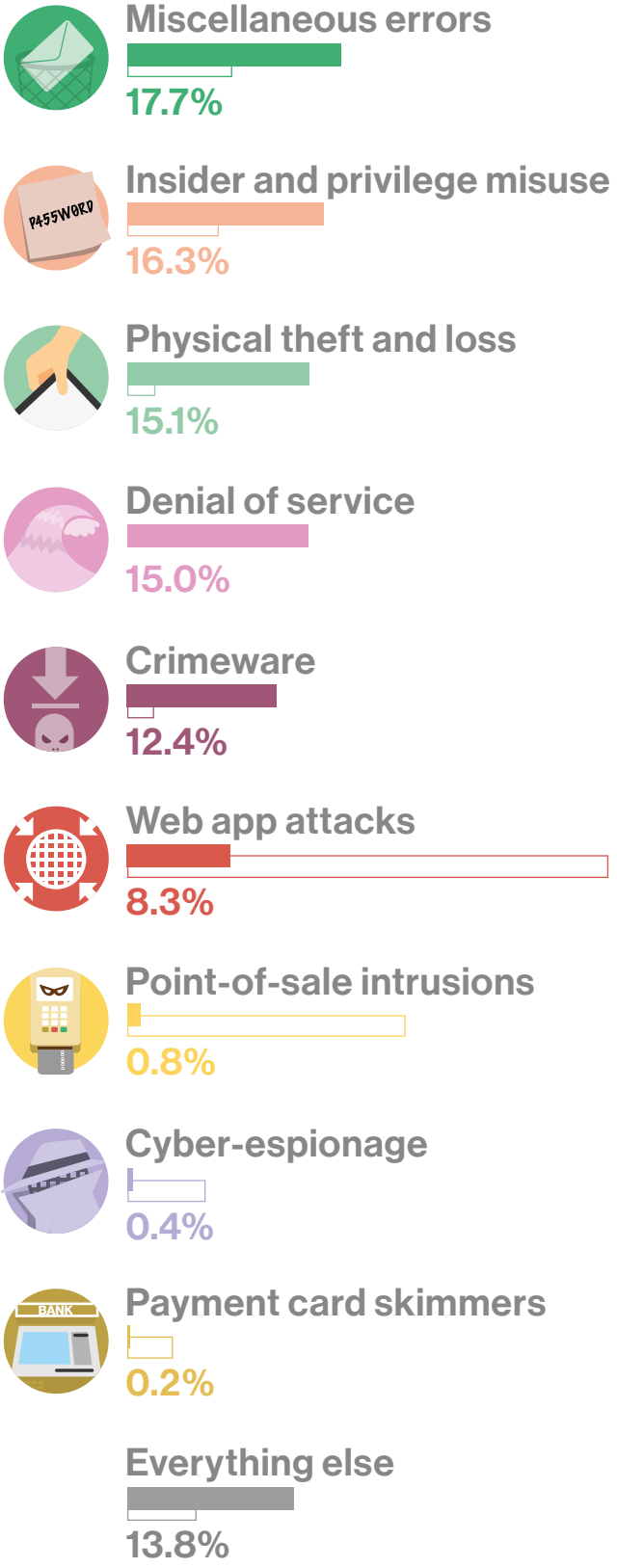


Figure 1: Incidents/breaches by classification patterns, all industries

In most industries, three quarters of incidents and breaches are covered by just three patterns.

Accommodation (3 patterns = 96% of incidents)

Entertainment (3 patterns = 100% of incidents)

Financial services (3 patterns = 88% of incidents)

Healthcare (3 patterns = 73% of incidents)

Manufacturing (3 patterns = 55% of incidents)

Professional services (3 patterns = 94% of incidents)

Public sector (3 patterns = 66% of incidents)

Retail (3 patterns = 90% of incidents)

Transportation (3 patterns = 77% of incidents)

Utilities (3 patterns = 69% of incidents)

Figure 2: Top three incidents/breaches by industry

Miscellaneous errors

Any unintentional action or mistake that compromises security, excluding the loss of assets.

Most affected industries:
Public sector, Healthcare, Information

40% of incidents in this pattern were caused by a shortage of server capacity, where non-malicious spikes in web traffic overwhelm systems and cause key applications to crash. But it's often a simple mistake by one of your employees that triggers an incident.

26% of miscellaneous errors involved sending sensitive information to the wrong person.

What can you do?

- **Learn from your mistakes:** Keep a record of common errors that have occurred in the past. You can use this to improve security awareness training and measure the effectiveness of your controls.
- **Strengthen controls:** Consider using data loss prevention (DLP) software, which can restrict sensitive information being shared outside the company.
- **Implement thorough disposal procedures:** Make sure your assets are wiped of sensitive data before they're sold. Sounds obvious, but we've seen lots of examples where this hasn't happened.

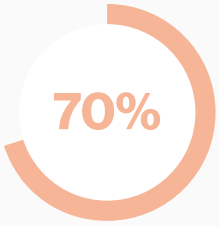
Insider and privilege misuse

This mainly consists of incidents involving misuse by insiders. But outsiders (due to collusion) and partners granted privileged access to systems also show up.

Most affected industries:
Healthcare, Public sector, Administrative

Contrary to what some people think, it's rarely system admins or developers with elevated privileges that fall victim. End users account for a third of insider misuse. Attacks are typically motivated by money: 34% of breaches involving misuse were motivated by financial gain – although a quarter (25%) can be linked with espionage, such as the theft of intellectual property.

70% of breaches involving insider misuse took months or years to discover.



What can you do?

- **Know your data:** You need to know what sensitive data you have, where it is, and who has access to it. Governance should ensure that access is limited to those who really need it and actual access is checked against this list.
- **Monitor user behavior:** Track system usage – particularly access to data that can be used for financial gain – and revoke access immediately when employees leave.
- **Track USB usage:** Don't leave yourself in a position where you only find out that an employee has taken data after they've left.

Physical theft and loss

The loss or theft of laptops, USB drives, printed papers and other information assets.

Most affected industries:
Healthcare, Public sector

It's usually a case of a laptop or mobile being lost by an employee that triggers a security incident. But the biggest threat of a data breach is from lost or stolen documents, which can't be encrypted.

39% of theft is from victims' own work areas, and 34% from employees' personal vehicles.

What can you do?

- **Encrypt your data:** If stolen devices are encrypted it's much harder for attackers to access the data.
- **Train your staff:** Developing security awareness in your organization is critical. Work with HR to include education on physical security of assets as part of the orientation and ongoing training of employees.
- **Reduce use of paper:** Cut down on printing. Establish data classification rules and create a company policy covering the printing and transportation of sensitive data.

Denial of service (DoS)

The use of botnets – a "zombie" army of computers, typically taken over without the owner's permission – to overwhelm an organization with malicious traffic. DoS attacks can bring normal operations to a halt, causing chaos.

Most affected industries:
Entertainment, Professional, Educational

Don't underestimate the impact a DoS attack could have on your organization. They're the fourth most common pattern in our data for all security incidents. And a large-scale attack could take your website or mission-critical systems offline for weeks.

The median traffic of a DoS attack is 1.89 million packets per second—that's like over 113 million people trying to access your server every minute.

What can you do?

- **Segregate key servers:** Separate primary systems to protect them from attack.
- **Choose your providers carefully:** Make sure your cloud service providers have solutions in place to protect the availability of their services and infrastructure.
- **Test your anti-DoS service:** It shouldn't be a case of install and forget. Make sure you have a solid understanding of your service level agreements (SLAs) for DoS mitigation.

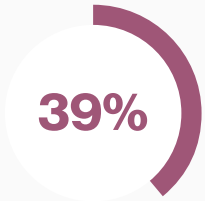
Crimeware

This covers any use of malware that doesn't fit into a more specific pattern. Crimeware often affects consumers.

Most affected industries:
Public sector, Manufacturing, Information

Attacks are typically opportunistic and motivated by financial gain. The malware gets onto your system when someone clicks on a malicious email link or visits an infected website. Ransomware is on the rise. It involves attackers encrypting the contents of a device, rendering it useless. They then demand a ransom to unlock the data.

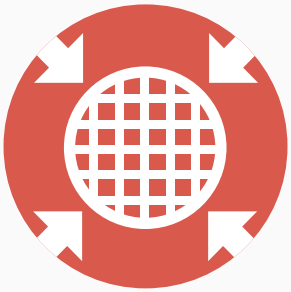
39% of crimeware incidents in 2015 involved ransomware.



What can you do?

- **Patch promptly:** Cybercriminals are successfully exploiting known vulnerabilities; timely patching could block many attacks.
- **Implement configuration change monitoring:** Many attack methods can be easily detected by watching key indicators.
- **Back up your systems regularly:** This will keep your business running should any systems fall foul of ransomware.
- **Capture data on attacks:** Examine the different types of malware you've fallen foul of – and, if possible, the entry point. This gives you intelligence on where to prioritize your efforts.

Web app attacks

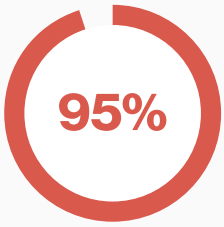


Where a web app – such as a content management system (CMS) or e-commerce platform – was used as the means of entry.

Most affected industries:
Financial services, Retail, Information

Many web app attacks are indiscriminate – the attackers found a weak target with a vulnerability they could compromise; or got a foothold through a phishing campaign. Cybercriminals had a lot of success using CMS plugins to deploy malicious software. Once in, many attacks defaced the target's website. But we saw almost 20,000 incidents where compromised websites were used in distributed denial of service (DDoS) attacks or repurposed as phishing sites.

95% of web app attacks where criminals stole data were financially motivated.



What can you do?

- **Use two-factor authentication:** And lock out accounts after repeated failed attempts. You should also consider using biometrics.
- **Patch promptly:** Establish a robust process for patching CMS platforms, including third-party plugins, and e-commerce systems. See "Effective patching can stop them" on page 10.
- **Monitor all inputs:** Review all your logs to help identify malicious activity.

Point-of-sale (POS) intrusions

When attackers compromise the computers and servers that run POS applications, with the aim of capturing payment data.

Most affected industries:
Accommodation, Retail

In 2015, hotel chains made the headlines for remote payment card breaches. In 2014, it was large retailers. Successful breaches were often via a POS vendor, rather than a result of poorly configured, internet-facing POS devices.

95% of confirmed breaches in hospitality involved POS intrusions.

What can you do?

- **Patch servers promptly:** And only give access to people who absolutely need it.
- **Choose your providers carefully:** Make sure your cloud service providers have solutions in place to protect your systems.
- **Reserve POS systems for POS activities:** Do not allow staff to use them to browse the web, check email, or play games.
- **Use two-factor authentication:** Your POS provider should be using two-factor authentication.

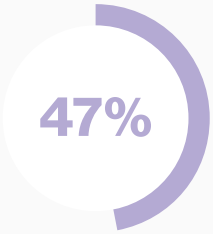
Cyber-espionage

Attacks motivated by espionage carried out by state-affiliated actors, often looking for intellectual property.

Most affected industries:
Manufacturing, Information, Professional

These attacks typically begin with the same tools and techniques used successfully elsewhere, before moving on to more sophisticated methods. That means that basic security measures are surprisingly effective in protecting against cyber-espionage and should not be forgotten in favor of specialized protection.

47% of all confirmed breaches in manufacturing could be classified as cyber-espionage.



What can you do?

- **Patch promptly:** Cybercriminals are successfully exploiting known vulnerabilities; timely patching could block many attacks.
- **Implement configuration change monitoring:** Many attack methods can be easily detected by watching key indicators.
- **Segregate systems:** Make sure a compromised desktop isn't a doorway to more critical systems and data.

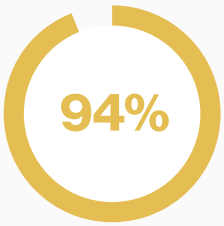
Payment card skimmers

Incidents involving physical installation of a device on an ATM, gas pump or POS terminal that intercepts card data.

Most affected industries:
Financial services, Retail, Accommodation

Most of these attacks happen at ATMs, but gas pumps and other devices show up too. Skimmers can be almost impossible to detect, even for the trained eye.

94% of breaches involving payment card skimmers were at an ATM.



What can you do?

- **Use tamper-resistant terminals:** Some terminals are more susceptible to tampering than others. Pick one that's been designed to deter the criminals.
- **Watch for tampering:** Establish a process for regularly checking the integrity of ATMs and gas pump card readers. Train employees to spot skimmers and make it easy for them to report anything suspicious.
- **Use tamper-evident controls:** This could be as simple as a putting a seal over the door of a gas pump.

The bad guys are quicker

Cybercriminals can break in and steal (exfiltrate) data in a matter of minutes. In 93% of cases where data was stolen, systems were compromised in minutes or less. And exfiltration happened within minutes in 28% of cases. But even where exfiltration took days, the criminals didn't need to worry. In 83% of cases, victims didn't find out they'd been breached for weeks or more.

The longer it takes you to discover a breach, the more time criminals have to find the valuable data they're looking for and disrupt your business. This is why protection isn't enough—you need to have effective detection and remediation systems and processes in place to thwart attacks and reduce the possible damage.

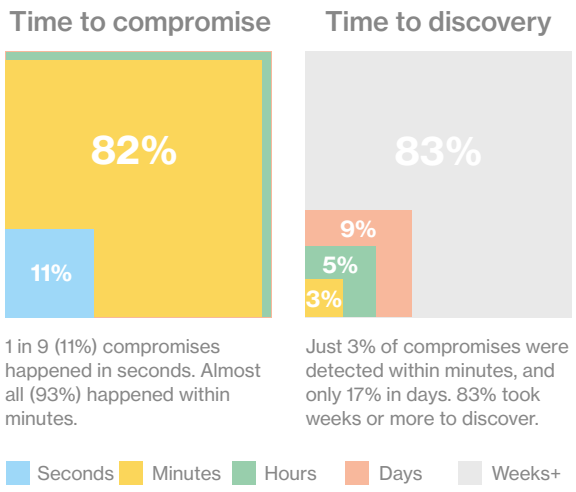


Figure 3: Breach timeline

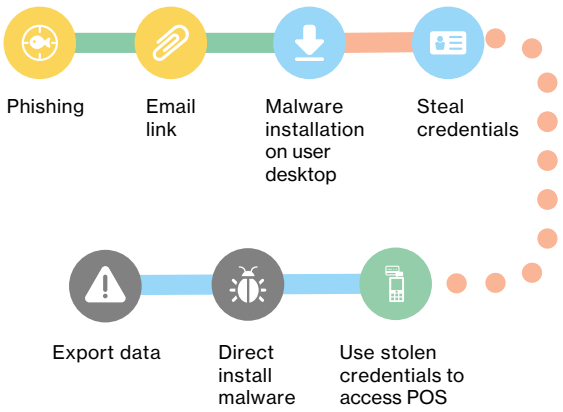


Figure 4: Birth and rebirth of a data breach

How they strike

Understanding the building blocks of an attack can help you construct solid defenses and detect a breach quickly if one does occur.

Even sophisticated attacks share DNA with the simplest. But the individual parts of an attack don't always fit together in the same order. And you don't just face one attack at a time. Attack graphs can help by highlighting your entire attack surface, not just the paths you've seen.

Effective patching can stop them

The top 10 vulnerabilities [Common Vulnerabilities and Exposures, or CVEs] accounted for 85% of successful exploit traffic. The other 15% comprises over 900 CVEs.

Patching promptly is important, but with so many new vulnerabilities being discovered, it's hard to know where to start. This year's DBIR provides valuable information to help you solve that problem.

Data provided by Kenna Security suggests that vulnerabilities in Adobe products were exploited quickest; ones in Mozilla products the slowest—see Figure 5. Studying this information will help you move away from conducting "fire drills" and focus your patching efforts.

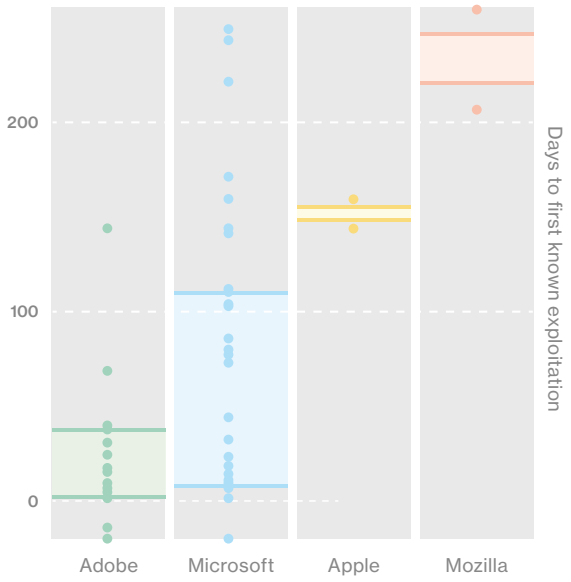


Figure 5: Days to first known exploitation

Use intelligence, the crooks do!

The cybercriminals aren't content with the status quo. As the value of some forms of data falls, they are casting their nets wider and improving their tactics.

No system is 100% secure, but too many organizations are making it easy for them. They are leaving well-known vulnerabilities open and letting employees use easy-to-guess passwords – and often even the defaults that devices come with.

This means a lot of the breaches we've seen were avoidable, if organizations had put in place some basic security measures. Our seven tips to the right cover the simple mistakes that we see time and time again.

But your IT team should have a thorough understanding of the threats your organization faces. Cybercriminals are using all the information they can get hold of to up their game. So should you. The 2016 Data Breach Investigations Report is a must-read for any organization that is serious about cybersecurity.

Quick takeaways

- **Be vigilant:** Log files and change management systems can give you early warning of a breach.
- **Make people your first line of defense:** Train staff to spot the warning signs.
- **Only keep data on a "need to know" basis:** Only staff that need access to systems to do their jobs should have it.
- **Patch promptly:** This could guard against many attacks.
- **Encrypt sensitive data:** Make your data next to useless if it is stolen.
- **Use two-factor authentication:** This can limit the damage that can be done with lost or stolen credentials.
- **Don't forget physical security:** Not all data theft happens online.

Get the 2016 Data Breach Investigations Report

The DBIR is our foremost annual publication on security, and one of the industry's most respected sources of information. As well as the full report and this summary, we also publish a number of other resources to help you understand the threats and improve your defenses. Take a look.

Get our full 2016 DBIR and other helpful resources. Read more ›

Are you doing cybersecurity wrong? View our SlideShare. SlideShare ›

VerizonEnterprise.com

© 2016 Verizon. All Rights Reserved. The Verizon name and logo and all other names, logos, and slogans identifying Verizon's products and services are trademarks and service marks or registered trademarks and service marks of Verizon Trademark Services LLC or its affiliates in the United States and/or other countries. All other trademarks and service marks are the property of their respective owners. WP16705 04/16