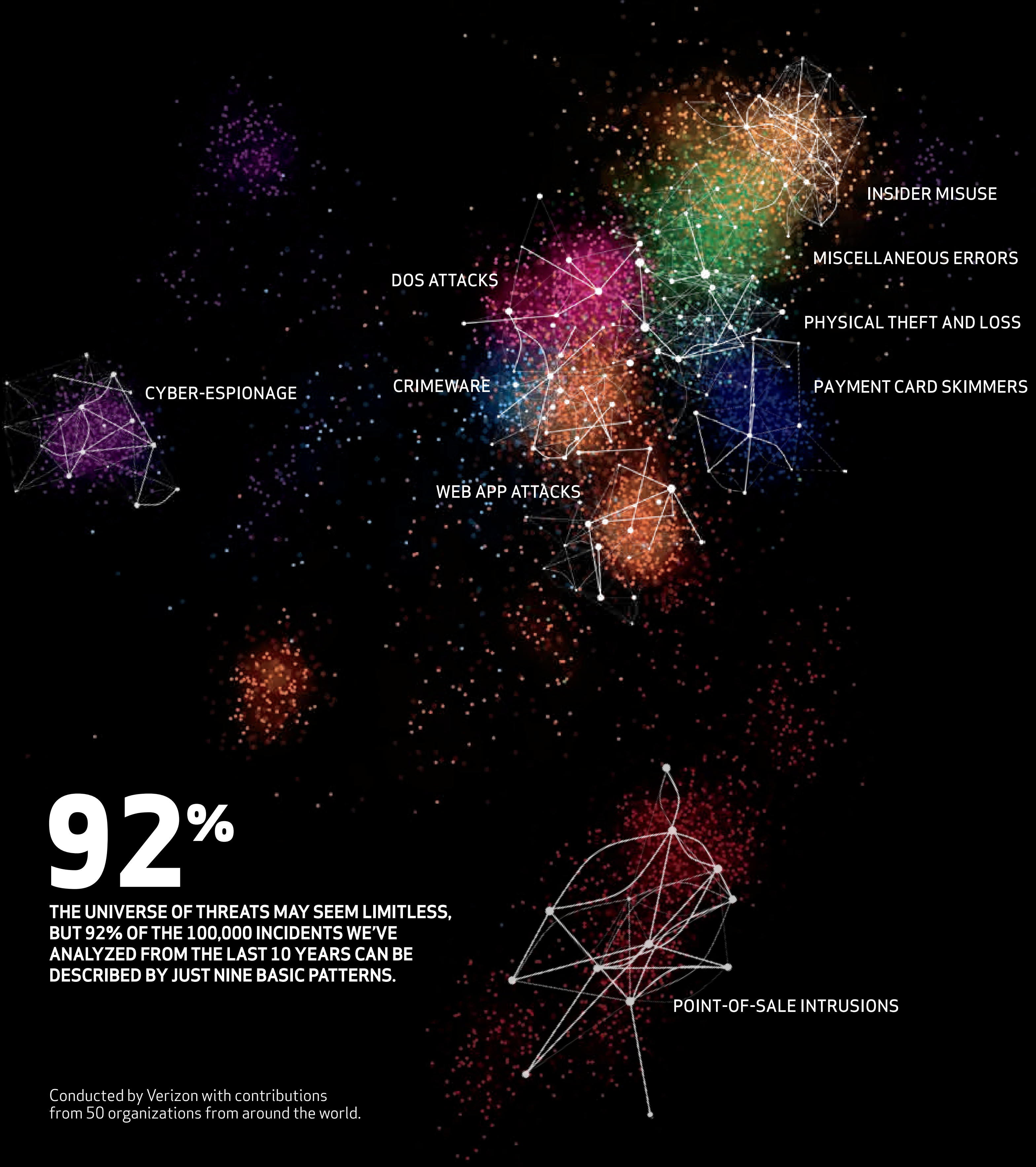
2014 DATA BREACH INVESTIGATIONS REPORT



92%

THE UNIVERSE OF THREATS MAY SEEM LIMITLESS, BUT 92% OF THE 100,000 INCIDENTS WE'VE ANALYZED FROM THE LAST 10 YEARS CAN BE DESCRIBED BY JUST NINE BASIC PATTERNS.

Conducted by Verizon with contributions
from 50 organizations from around the world.

2014 Data Breach Investigations Report

EXECUTIVE SUMMARY

Data security should matter to you, no matter what your role in your organization. Why? Because when you suffer a breach of any kind — whether it's an attacker skimming customer credit card details, or an employee accidentally leaving a USB key full of blueprints in a taxi — the impact is company-wide.

50
ORGANIZATIONS FROM AROUND THE WORLD CONTRIBUTED DATA.

63,000+
SECURITY INCIDENTS WERE ANALYZED.

1,367
CONFIRMED DATA BREACHES WERE STUDIED.

When word of a data breach gets out — as it often does — you may face fines and legal action. Just as importantly, your customers and partners may lose faith in your ability to protect their interests, which can directly impact your reputation and your bottom line. And then there's the further expense of finding out what went wrong, and patching any holes in your defenses.

The costs of a data breach can be enormous. And it's not just the remediation costs and potential fines; the damage to your reputation and loss of customer confidence could impact your success for years. Many companies never recover from a major data breach.

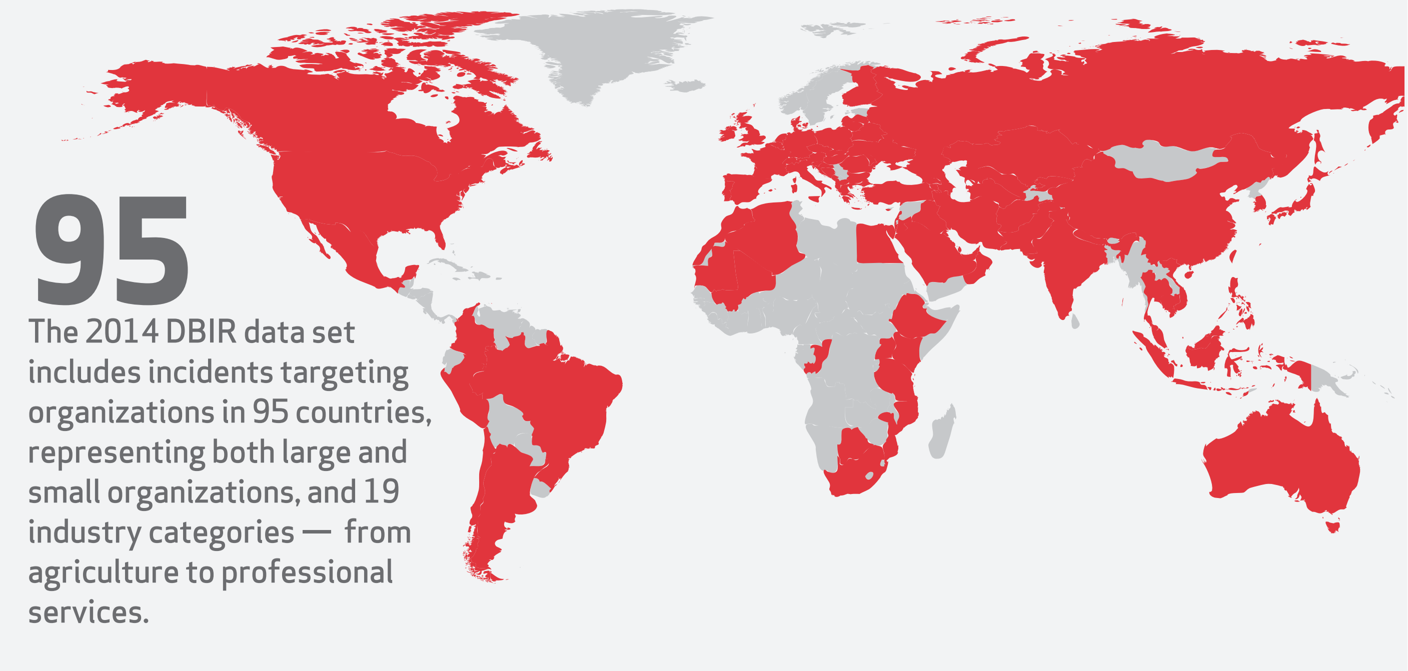
WHO CAN YOU TRUST?

The range of threats to your data and systems can be forbidding. And trusting gut feel — or even historical best practice — can be unreliable.

Media coverage has created a distorted picture of data breaches. The reality is that it's not just retailers that are affected; our data shows that attacks on point-of-sale (POS) systems have actually been trending downwards over the last few years. Conversely, espionage attacks continue to grow — affecting all kinds of companies, not just government agencies and military contractors.

It's clear: when it comes to security, you can't rely on instinct. The threat landscape is constantly changing, and keeping up-to-date is a constant challenge.

In order to build the right defenses and effectively protect your business, you need to know more about the threats you face. The Verizon DBIR has, for years, been the best source of insight about the threat landscape. This year's report covers over 63,000 security incidents from 95 countries, including 1,367 confirmed data breaches. This includes denial of service (DoS) attacks for the first time — these rarely involve the loss of data, but are still a significant threat to your business.



95
The 2014 DBIR data set includes incidents targeting organizations in 95 countries, representing both large and small organizations, and 19 industry categories — from agriculture to professional services.

A NEW APPROACH

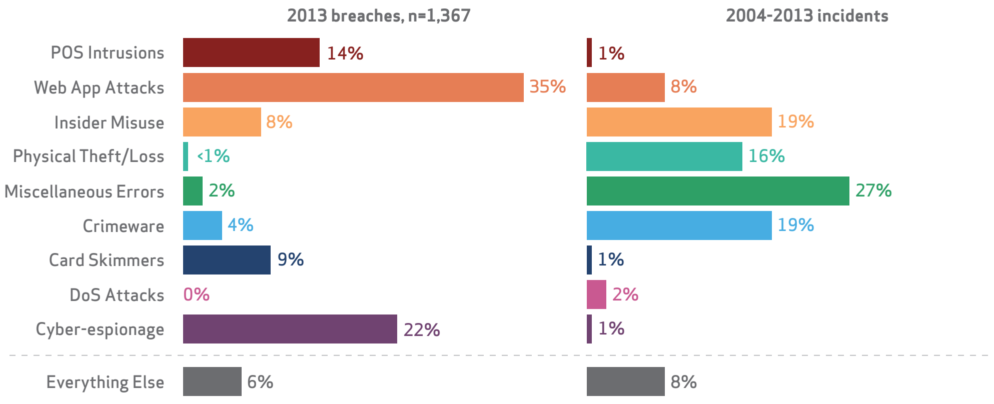
The variety and volume of threats is growing. And securing your business has never been more important. That's why we've made this year's DBIR the most informative and actionable yet.

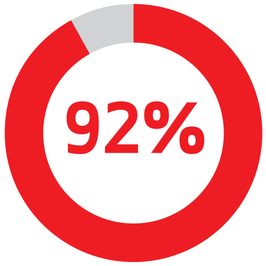
Using more than ten years of breach and incident data, we can build a clear picture of the elements involved in the average breach.

THE VICTIM	It could be you. All sizes of business and all industries are at risk of some kind of security event. Even if you think your organization is at low risk of external attacks, there remains the possibility of insider misuse and errors that harm systems and expose data.
THE CULPRIT	Most attacks are perpetrated by external actors, as opposed to employees and partners. Financially motivated criminal gangs are still the dominant type of perpetrator in external attacks — although espionage appears increasingly often in our data set. Despite all the emphasis on "hacktivism" in the press, ideology-driven attacks remain a very small percentage of the total.
THE TARGET	Attackers are mainly going for payment and bank data, which they can quickly convert into cash. User credentials are also a popular target, but mainly as a gateway to other kinds of data or other systems. Reflecting the rise in espionage attacks is a growth in theft of secrets and internal data.
THE ATTACK	Hacking and malware are the most popular attack methods. Servers and user devices (such as PCs) are the main targets. Physical tampering attacks are becoming less common, but social attacks have grown in recent years.
THE CHASE	Attackers have got faster at breaching systems. Defenders are getting faster too — but they're falling further behind. Many successful breaches are detected by third parties, such as law enforcement agencies, specialist fraud detection organizations, or even customers.

When you're focusing on attempted breaches by outside attackers, it's easy to forget about the other kinds of risks to your data. But data leakage via process error or device loss is a constant problem. And attackers are also increasingly using denial of service attacks — which, while they don't steal any data, can be just as damaging to your business operations.

But you need more than a general picture. So, the biggest change we made this year is to use statistical methods to identify 'clusters' of similar incidents and breaches. We were sure that there were patterns in the incident data: certain groups of attack methods, targets and perpetrators that appeared time and again. From the complexity and diversity of the threat landscape, we've identified nine patterns that cover 92% of the security incidents that we've analyzed over the last ten years, and 94% of the breaches that we looked at last year. We call these incident classification patterns.





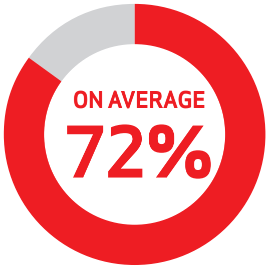
OF THE INCIDENTS WE'VE SEEN OVER THE LAST 10 YEARS — AND 94% OF THE BREACHES IN 2013 — CAN BE DESCRIBED BY JUST NINE PATTERNS.

THE INDUSTRY VIEW

Our nine patterns classify almost all of the attacks that your industry is likely to face. This will help you to make sense of the threats, and prioritize your security efforts.

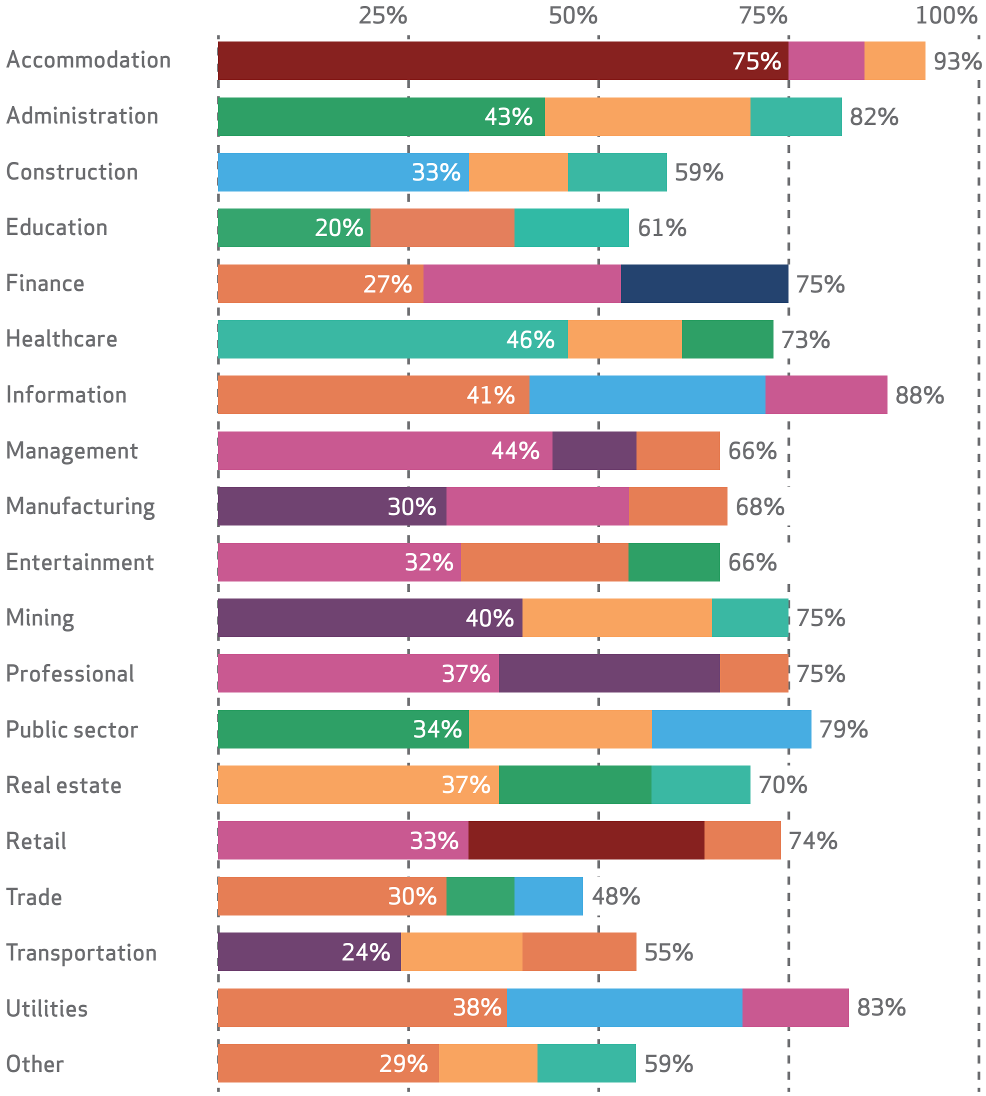
By identifying the nine incident classification patterns, we've made it easier to understand the threat landscape, enabling you to focus your strategy, and prioritize your security investments more effectively.

The chart below shows how frequently these patterns appeared in different industry sectors. Not only do nine patterns cover 92% of over 100,000 incidents, but on average just three of those patterns cover 72% of the incidents in any industry.



OF THE INCIDENTS IN AN INDUSTRY CAN BE DESCRIBED BY JUST THREE OF THE NINE PATTERNS.

TOP 3 PATTERNS COVER AVERAGE OF 72% OF INCIDENTS



In most industries, more than 50% of incidents are covered by just three of the nine patterns.

THE NINE PATTERNS

The following pages summarize the nine patterns — and our advice for how you can respond to them.

MISCELLANEOUS ERRORS

What is it?

Simply, any mistake that compromises security: which may mean posting private data to a public site accidentally, sending information to the wrong recipients, or failing to dispose of documents or assets securely.

Is my industry a target?

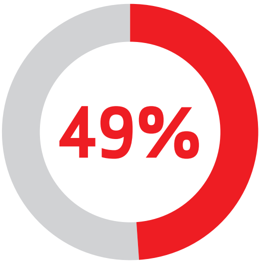
People make mistakes, no matter what industry they work in. But industries that deal in the communication of information — such as public sector, administration, education and healthcare — suffer most.

What can we do?

Implement DLP. Consider implementing data loss prevention software to block sensitive information being sent — perhaps in error — by email.

Strengthen controls on publishing. Decrease the frequency of publishing errors by tightening up controls around posting documents to websites. Regularly scan the web for private data.

Teach staff about asset disposal. They must understand that documents and computers can't just be put in the bin.



OF MISCELLANEOUS ERRORS INVOLVED PRINTED DOCUMENTS.

CRIMEWARE

What is it?

Crimeware is a broad category, covering any use of malware (often web-based) to compromise systems such as servers and desktops. This pattern includes phishing.

Is my industry a target?

We found public sector, information, utilities and manufacturing were most at risk.

What can we do?

Patch anti-virus and browsers. This could block many attacks.

Disable Java in the browser. Given the history of vulnerabilities, avoid using Java browser plugins whenever possible.

Use two-factor authentication. It won't prevent the theft of credentials, but it will limit what damage can be done.

Implement configuration change monitoring. Many methods can be easily detected by watching key indicators.

THE MAJORITY OF CRIMEWARE INCIDENTS START VIA WEB ACTIVITY, NOT LINKS OR ATTACHMENTS IN EMAIL.

INSIDER AND PRIVILEGE MISUSE

What is it?

This is mainly by insiders misuse, but outsiders (due to collusion) and partners (because they are granted privileges) show up as well. Potential culprits come from every level of the business, from the frontline to the boardroom.

Is my industry a target?

A wide range of industries were represented: real estate, public sector, mining, administrative, and others. Wherever a business trusts people, you'll find this risk.

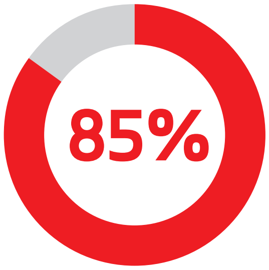
What can we do?

Know your data. The first step in protecting your data is in knowing where it is, and who has access to it.

Review user accounts. Having identified who has access to sensitive data, implement a process for revoking access when employees leave or change role.

Watch the exits. Set up controls to watch for data transfer out of the organization.

Publish anonymized results of audits. Seeing that policies are being enforced and policed can be a powerful deterrent.



OF INSIDER AND PRIVILEGE MISUSE ATTACKS USED THE CORPORATE LAN.

PHYSICAL THEFT AND LOSS

What is it?

The loss or theft of laptops, USB drives, printed papers and other information assets, mostly from offices, but also from vehicles and homes.

Is my industry a target?

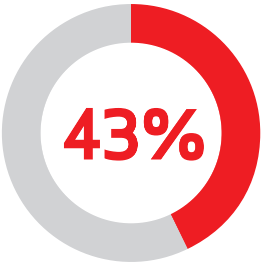
Accidents happen anywhere — but 45% of all incidents in the healthcare sector fit this profile. Public sector was also saw a lot of incidents fitting this pattern.

What can we do?

Encrypt devices. While encryption won't affect the chances of an asset going missing, it will protect the data it stores.

Back it up. Regular backups can prevent the loss of valuable data, reduce downtime, and help with forensics should you be breached.

Lock it down. Secure IT equipment to immovable fixtures, and store sensitive assets — including paper documents — in a separate, secure area.



OF THEFT/LOSS HAPPENED AT WORK.

WEB APP ATTACKS

What is it?

When attackers use stolen credentials or exploit vulnerabilities in web applications — such as content management systems (CMS) or e-commerce platforms.

Is my industry a target?

Most sectors now have many of their applications web-facing, but top targets included information, utility, manufacturing and retail companies.

What can we do?

Use two-factor authentication. Look at soft tokens and biometrics.

Consider switching to a static CMS. These don't need to execute code for every request, reducing the opportunity for exploits.

Enforce lockout policies. Locking accounts after repeated failed login attempts will help to thwart brute-force attacks.

Monitor outbound connections. Unless your server has a good reason to send millions of packets to a foreign government's systems, lock down its ability to do so.

WEB APP ATTACKS OFTEN TARGET CMS LIKE WORDPRESS AND DRUPAL.

DENIAL OF SERVICE ATTACKS

What is it?

These are attacks, not attempted breaches. Attackers use "botnets" of PCs and powerful servers to overwhelm an organization's systems and applications with malicious traffic, causing normal business operations to grind to a halt.

Is my industry a target?

Attacks are often on mission-critical transactional systems in finance, retail and similar sectors.

What can we do?

Ensure that servers are patched promptly. And only give access to people that need it.

Segregate key servers. Buy a small backup circuit and announce IP space. That way if it's attacked, primary systems won't be affected.

Test your anti-DoS service. This isn't an install-and-forget type of service.

Have a plan. Key operations teams need to know how to react if there is an attack. And know what you'll do if your anti-DoS service doesn't work.

+115%

MORE POWERFUL BOTNETS AND REFLECTION ATTACKS HAVE HELPED DRIVE THE SCALE OF DDOS ATTACKS UP 115% SINCE 2011.

CYBER-ESPIONAGE

What is it?

When state-affiliated actors breach an organization, often via targeted phishing attacks, and after intellectual property.

Is my industry a target?

Espionage is not just a problem for government and military organizations. Professional services, transportation, manufacturing, mining and public sector are all popular targets.

What can we do?

Patch promptly. Exploiting software vulnerabilities is a common first step.

Use anti-virus, and keep it up to date. It won't protect you from zero-day attacks, but many still fall prey to well-known dangers.

Train users. Give them the knowledge they need to recognize and report danger signs.

Keep good logs. Log system, network, and application activity. This is a good foundation for incident response, and will support many proactive countermeasures.

3X

THIS YEAR'S DATA SET SHOWS A THREEFOLD INCREASE IN ESPIONAGE ATTACKS YEAR ON YEAR.

POINT-OF-SALE INTRUSIONS

What is it?

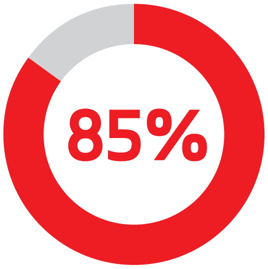
When attackers compromise the computers and servers that run POS applications, with the intention of capturing payment data.

Is my industry a target?

Hospitality and retail companies are the top targets — hardly surprising as that's where most POS devices are. But other sectors, such as healthcare, also process payments and so are also at risk.

What can we do?

Restrict remote access. Limit remote access into POS systems by third-party companies.
Enforce strong password policies. Our PCI Compliance Report found that over 25% of companies still use factory defaults.
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. Stronger passwords would reduce the problem, but two-factor would be better.



OF POS INTRUSIONS TOOK WEEKS TO BE DISCOVERED.

PAYMENT CARD SKIMMERS

What is it?

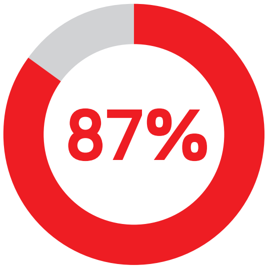
The physical installation of a "skimmer" on an ATM, forecourt gas pump or POS terminal, to read your card data as you pay.

Is my industry a target?

Banks, retailers and hospitality companies are the primary targets.

What can we do?

Use tamper-resistant terminals. Some terminals are more susceptible to skimming than others.
Watch for tampering. Train employees to spot skimmers and recognize suspicious behavior.
Use tamper-evident controls. This may be as simple as a seal over the door of a gas pump, or something more sophisticated like automated video monitoring to detect anomalies.



OF SKIMMING ATTACKS WERE ON ATMS.

SUMMARY

The DBIR is packed with more detailed information and recommendations. But seven common themes are clear:

- **Be vigilant.** Organizations often only find out about security breaches when they get a call from the police or a customer. Log files and change management systems can give you early warning.
- **Make your people your first line of defense.** Teach staff about the importance of security, how to spot the signs of an attack, and what to do when they see something suspicious.
- **Keep data on a 'need to know basis'.** Limit access to the systems staff need to do their jobs. And make sure that you have processes in place to revoke access when people change role or leave.
- **Patch promptly**. Attackers often gain access using the simplest attack methods, ones that you could guard against simply with a well-configured IT environment and up-to-date anti-virus.
- **Encrypt sensitive data.** Then if data is lost or stolen, it's much harder for a criminal to use.
- **Use two-factor authentication.** This won't reduce the risk of passwords being stolen, but it can limit the damage that can be done with lost or stolen credentials.
- **Don't forget physical security.** Not all data thefts happen online. Criminals will tamper with computers or payment terminals or steal boxes of printouts.

Want to know more?

This executive summary gives just a taste of the information in the full Verizon 2014 Data Breach Investigations Report. The analysis that it provides can help you to understand the threats to your industry, and improve your defenses against them.

2014 DATA BREACH INVESTIGATIONS REPORT
92%
2014 | Data Breach Investigations Report

Download the full report and other resources from:
verizonenterprise.com/dbir/2014

ABOUT VERIZON

We design, build, and operate the networks, information systems, and mobile technologies that help businesses and governments around the globe expand reach, increase productivity, improve agility, and maintain longevity.

Our solutions across Security, Connected Machines, Dynamic Cloud, Intelligent Networking and Mobile Workforce are designed to help enterprises pursue new possibilities and create entirely new revenue streams — more efficiently and securely than ever.

We believe that businesses and individuals empowered by technology can change the world. We create solutions with that belief in mind; we perpetually challenge ourselves to enable, advance, and pave the way for new possibilities across a variety of industries.

verizonenterprise.com