2017 Data Breach Investigations Report

Executive Summary

verizon

Snapshot

For the tenth time, the Verizon Data Breach Investigations Report (DBIR) delves into the murky world of cybersecurity. It brings together the collective experience of 65 organizations to give you the full picture on cybercrime.

Who's behind the breaches?

75% perpetrated by outsiders.

25% involved internal actors.

18% conducted by state-affiliated actors.

3% featured multiple parties.

2% involved partners.

51% involved organized criminal groups.

What tactics do they use?

62% of breaches featured hacking.

51% over half of breaches included malware.

81% of hacking-related breaches leveraged either stolen and/or weak passwords.

43% were social attacks.

14% Errors were causal events in 14% of breaches. The same proportion involved privilege misuse.

8% Physical actions were present in 8% of breaches.

Who are the victims?

24% of breaches affected financial organizations.

15% of breaches involved healthcare organizations.

12% Public sector entities were the third most prevalent breach victim at 12%.

15% Retail and Accommodation combined to account for 15% of breaches.

What else is common?

66% of malware was installed via malicious email attachments.

73% of breaches were financially motivated.

21% of breaches were related to espionage.

27% of breaches were discovered by third parties.

Are you Gambling with your Future?

If you haven't suffered a data breach you've either been incredibly well prepared, or very, very lucky. Are you incredibly well prepared?

No one thinks it's going to be them. Until it is.

Hollywood has a lot to answer for. According to the movies, cybercriminals operate out of badly lit disused warehouses, target carefully selected conglomerates and use things like "worms" and "keys" to gain access. This caricature has lulled many into a false sense of security, believing that data breaches are something that happen to someone else.

The reality is that cybercriminals rarely fit that profile. They're opportunistic; using scattergun techniques like phishing to trawl for weak points that they can use as a foothold to launch their attack. And their intent is rarely world domination, it's normally just money.

Whether it's design plans, medical records or good, old-fashioned payment card details – someone, somewhere will see it as their meal ticket. Most cybercriminals are not fussy about who they steal from.

Organizations think they've got the basics covered.

People are still falling for phishing – yes still. This year's DBIR found that around 1 in 14 users were tricked into following a link or opening an attachment – and a quarter of those went on to be duped more than once. Where phishing successfully opened the door, malware was then typically put to work to capture and export data – or take control of systems.

People are also still failing to set strong passwords.

80% of hacking-related breaches leveraged either stolen passwords and/or weak or guessable passwords.

See pages 6-7 to learn about the nine attack patterns that covered 88% of breaches we investigated in our 2017 report.

People rely on how they've always done things.

Many organizations are still relying on defenses that are out of date. It's tempting, especially if you didn't suffer a major incident, to keep the same defenses from year to year. But are those defenses aligned with the threats that organizations like yours really face?

See pages 4-5 to learn about the threats that we've found are most prevalent in your industry.

61%

of the data breach victims in this year's report are businesses with under 1,000 employees.

95%

of phishing attacks that led to a breach were followed by some sort of software installation.

Build your Defenses Wisely

While attackers are using new tactics and tricks, their overall strategies remain relatively unchanged. Understanding them is critical to knowing how to defend your organization from cyberattacks.

88%

of breaches fall into the nine patterns we first identified back in 2014.

Understanding these attack patterns helps struggling security professionals gain insight on where and how to invest their limited resources. For everyone else, the patterns provide a quick and easy way to assess where the most likely danger will arise. So, if you're commissioning a new app or creating a new process, you can build security in from the start.

Take a look at the 2017 Data Breach Digest to see how these attack patterns play out in real life. Each of the DBD's 16 scenarios maps to one of these attack patterns.

Cyber-Espionage

Attacks linked to state-affiliated actors, and/or with the motive of espionage.

Welcome to the long game

A malicious email is the cyber spy's favored way in. But this is no smash and grab. The initial email is typically followed by tactics aimed at blending in, giving the attacker time to collect the data that they need.

What you can do

Throw your weight behind security awareness training and encourage your teams to report phishy emails. Make it difficult for the adversary to pivot from a compromised desktop to other devices on your network.

Denial of Service

Any attack intended to compromise the availability of networks and systems.

Being hit where it hurts

DDoS attacks are nearly always (98%) targeted at large organizations. And while some unlucky souls face a constant barrage all year round, most attacks are over within a couple of days.

What you can do

Check that you have DDoS mitigation services in place to thwart any attacks, that they're regularly tested, and that they actually work.

Crimeware

All instances involving malware that did not fit into a more specific pattern.

Ransomware is big business

In the 2014 DBIR, ransomware was the 22nd most common form of malware. This year it's number five, and the most common in the Crimeware pattern. For the attacker, holding files for ransom is fast, low risk and easily monetizable – especially with Bitcoin to collect anonymous payment.

What you can do

Watch out for macro-enabled MS Office documents and stress the importance of software updates to anyone who'll listen.

Insider and Privilege Misuse

Any unapproved or malicious use of organizational resources.

The enemy within

In 60% of cases, insiders abscond with data in the hope of converting it to cash in the future. But sometimes it's a case of unsanctioned snooping (17%), or taking data to a new employer or to start a rival company (15%).

What you can do

Implement limiting, logging and monitoring of use, and watch out for large data transfers and use of USB devices.

Miscellaneous Errors

Unintentional actions that directly compromised the security of company data.

Mistakes were made

They can appear innocuous, but data lost through errors can be harmful too. Especially if – as in 76% of cases – it's the customer who makes you aware of your slip-up.

What you can do

Have, and enforce, a formal procedure for disposing of anything that might contain sensitive data. And establish a four-eyes policy for publishing information.

Physical Theft and Loss

Any incident where physical assets went missing – deliberately or accidentally.

People lose things

Measures such as encryption can stop theft and loss incidents from becoming breaches. But encryption can't always help – the majority of confirmed breaches involved the loss of hardcopy documents.

What you can do

Encrypt wherever possible and establish a corporate culture that frowns upon printing out sensitive data.

Payment Card Skimmers

All incidents where a skimming device was placed on a payment card reader.

Hit the gas

While ATMs continue to be the main target for skimming, the number of gas pump terminals used to harvest payment card information more than tripled compared to last year's DBIR. Skimming attacks are almost always discovered by third parties.

What you can do

Train employees to spot signs of tampering, monitor payment terminals with video surveillance and make sure the tapes are reviewed regularly.

Web Application Attacks

Any incident in which a web application was used as the means of attack.

Don't become a stepping stone

Not all websites hold payment card data, but they still often request users to sign up: submitting their names, addresses and more. Security is often weaker than online retail sites, so attackers use them as an easy way to grab personal data and credentials to use elsewhere.

What you can do

Encourage customers to vary their passwords and use two-factor authentication. Limit the amount of sensitive information stored in web-facing applications.

Point of Sale Intrusions

Remote attacks against POS terminals and controllers.

Fruitful POS

Point of sale (POS) environments continue to provide rich pickings for the bad guys, with nearly 98% of all recorded POS attacks resulting in a confirmed data breach. The focus of attacks has shifted from hotel chains to restaurants and small businesses.

What you can do

Request a review of third-party POS vendors and their security practices – with an emphasis on remote access.

Everything Else

Any incident that did not classify as one of the nine patterns.

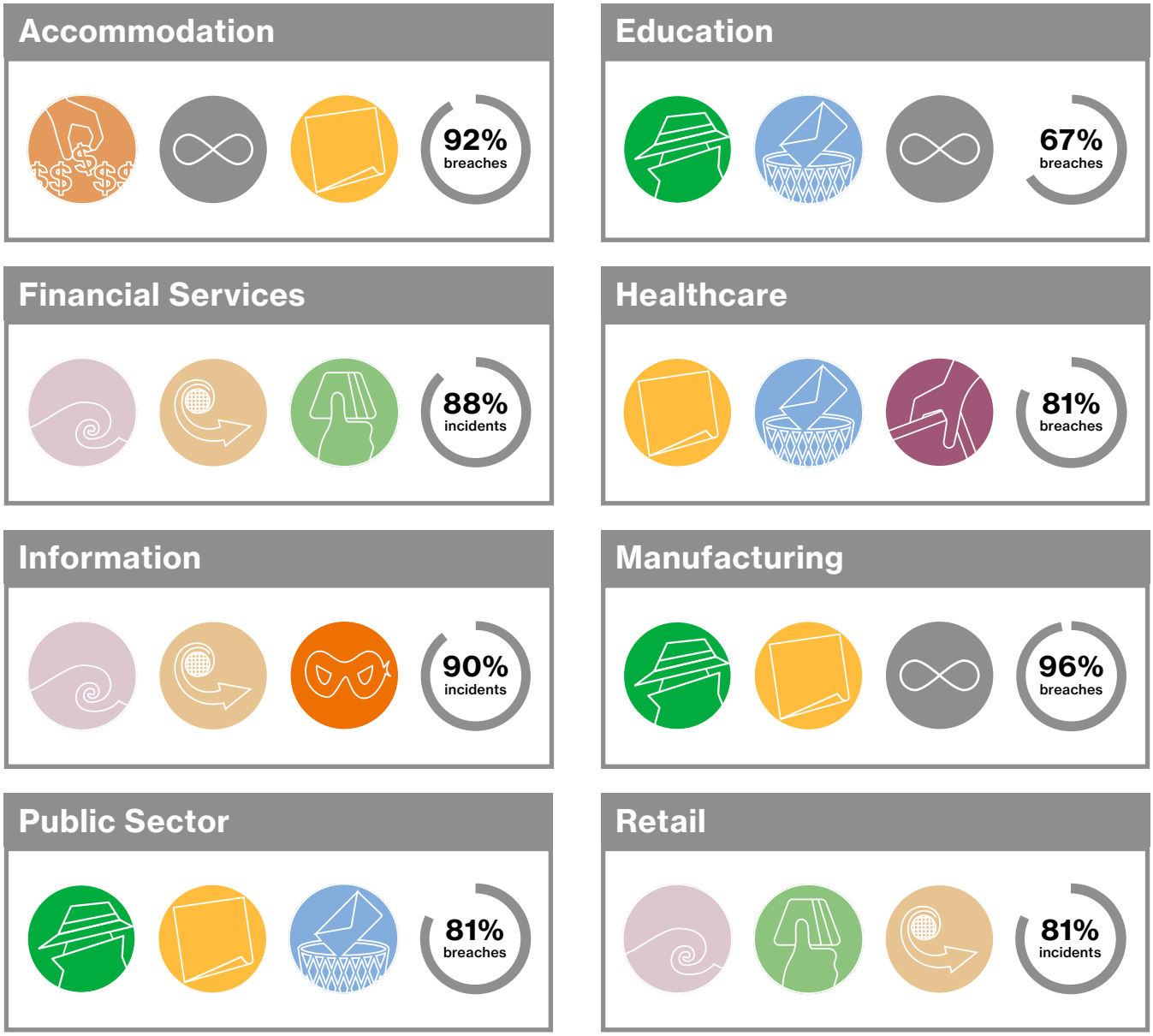
Beware of imposters

This may be a catch-all category, but that doesn't mean there aren't interesting and important trends. A key emerging tactic is email compromises: where "the CEO" orders wire transfers with an urgent and believable back story.

What you can do

Hammer home to your teams – particularly in finance – that no one will request a payment via unauthorized processes. Also ask IT to mark external emails with an unmistakable stamp.

Know the Threats you Face



Align your defenses

If you were off on an Arctic expedition you'd probably leave the shorts at home and double-up on the thermal underwear. The same applies when assessing where to spend your precious budget. The scorecards above help you understand the tactics that have been used against others in your industry. When you know where the greatest threats lie, you can align your defenses with the threats.

You don't have to be big or famous

The insider threat is nothing new in healthcare. But it's not just about taking a sneak peek through health records to reveal the name or sex of a celebrity's newborn before it appears in the press. It's often about identity theft and cloning the identities of everyday people.

Similarly, it's not just household brands that find themselves on the cyber spies' hit list. Start-ups are targeted for their breakthrough technology. More established companies fall victim for their sales lists. And others are identified as a soft target useful as a stepping stone to their partners' systems.

Use Intelligence, the Crooks do!

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.

Social engineering is a common means for cybercriminals to establish a foothold. And employees are making this easy by using easy-to-guess passwords. Users, and even IT departments, are even often guilty of not changing the default passwords that devices come with, and can easily be looked up online.

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 below 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 2017 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.

Want to Learn More?

2017 DBIR

Get the 2017 Data Breach Investigations Report (DBIR). It's our foremost publication on security, and one of the industry's most respected sources of information.

Read now >

2017 DBD

Read the Data Breach Digest for the story of Verizon's most intriguing cybercrime investigations. Learn about the attacker's tactics, the victim's mistakes and the scramble to limit the damage.

Read now >

VerizonEnterprise.com