


2017 Data Breach Investigations Report

Executive Summary



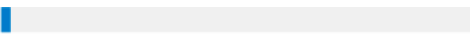
Who's behind the breaches?

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.




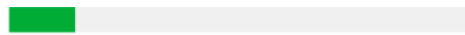
What tactics do they use?

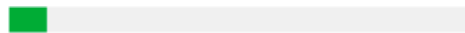
62%  of breaches featured hacking.

51%  over half of breaches included malware.

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

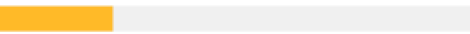
43%  were social attacks.

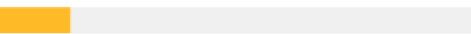
14%  Errors were causal events in 14% of breaches. The same proportion involved privilege misuse.

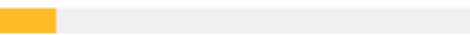
8%  Physical actions were present in 8% of breaches.

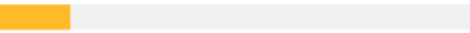


Who are the victims?

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?

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.

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% 

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.

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.

People are also still failing to set strong passwords.

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

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 –

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.