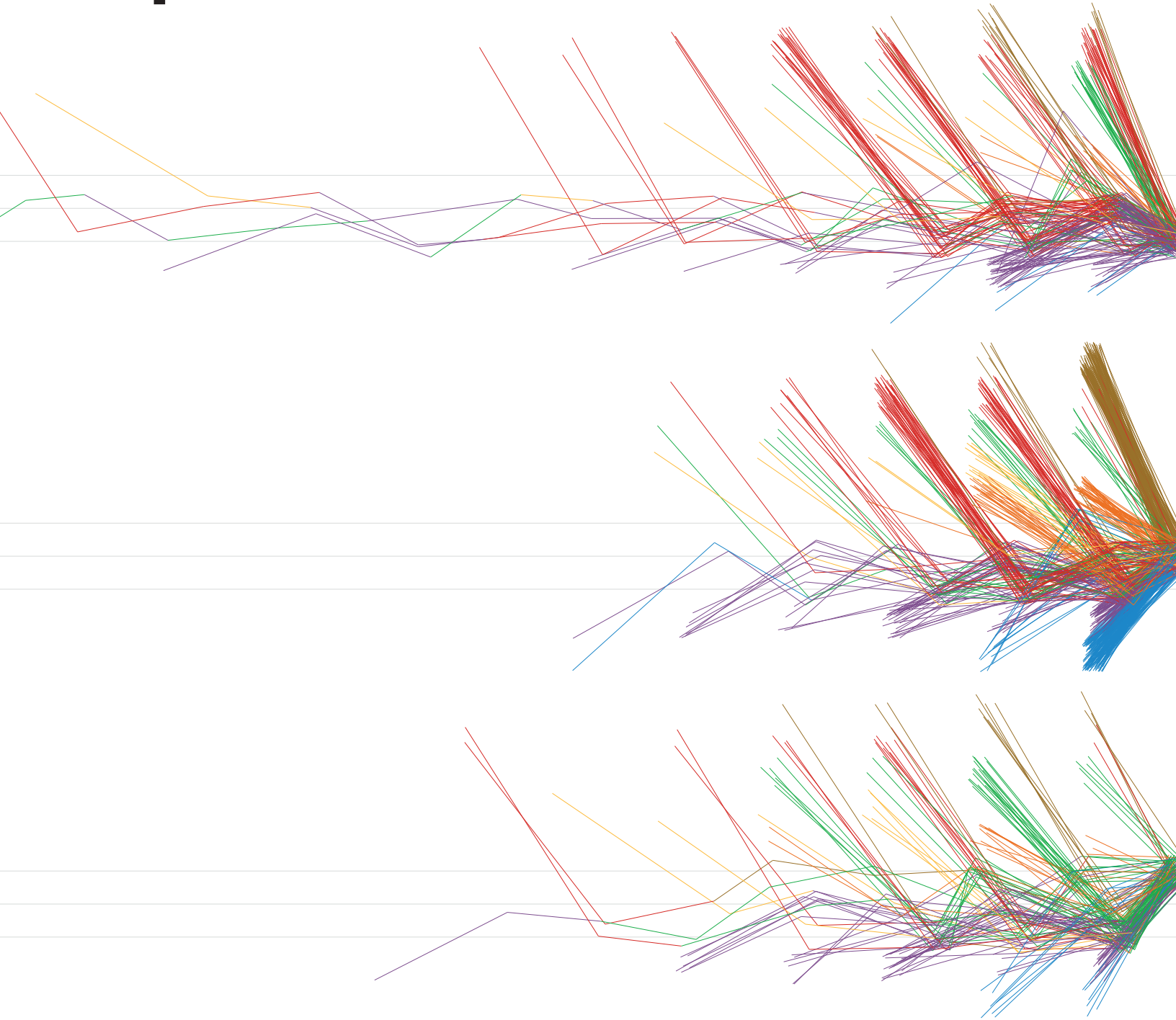


2019 Data Breach Investigations Report

Executive Summary



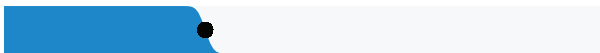
The Verizon Data Breach Investigations Report (DBIR) provides you with crucial perspectives on threats that organizations like yours face. The 12th DBIR is built on real-world data from 41,686 security incidents and 2,013 data breaches provided by 73 data sources, both public and private entities, spanning 86 countries worldwide.

Who is behind the attacks?

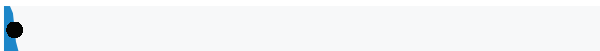
69% perpetrated by outsiders



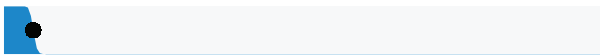
34% involved Internal actors



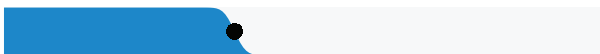
2% involved Partners



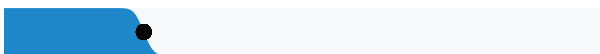
5% featured Multiple parties



Organized criminal groups were behind 39% of breaches



Actors identified as nation-state or state-affiliated were involved in 23% of breaches



0% 20% 40% 60% 80% 100%

Breaches

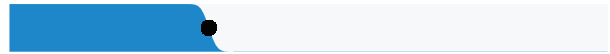
Figure 1.

What actions are being used?

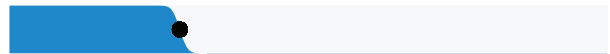
52% of breaches featured Hacking



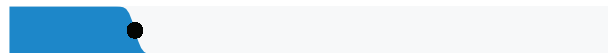
33% included Social attacks



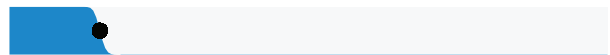
28% involved Malware



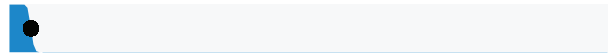
Errors were causal events in 21% of breaches



15% were Misuse by authorized users



Physical actions were present in 4% of breaches



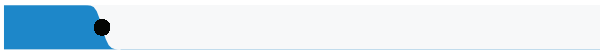
0% 20% 40% 60% 80% 100%

Breaches

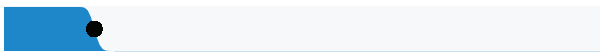
Figure 3.

Who are the breach victims?

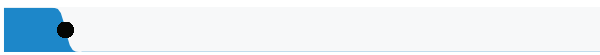
16% were breaches of Public sector entities



15% were breaches involving Healthcare organizations



10% were breaches of the Financial industry



43% of breaches involved small business victims



0% 20% 40% 60% 80% 100%

Breaches

Figure 2.

Data breaches continue to make headlines around the world. Seemingly, no matter what defensive measures security professionals put in place, attackers are able to circumvent them. No organization is too large or too small to fall victim to a data breach. No industry vertical is immune to attack. Regardless of the type or amount of your organization's data, there is someone out there who is trying to steal it. Having a sound understanding of the threats you and your peer organizations face, how they have evolved over time, and which tactics are most likely to be utilized can prepare you to manage these risks more effectively and efficiently.

Key Takeaways

Take me to your leader

C-level executives were twelve times more likely to be the target of social incidents and nine times more likely to be the target of social breaches than in years past. To further underline the growth of financial social engineering attacks, both security incidents and data breaches that compromised executives rose from single digits to dozens in this report.

Get out of my cloud

As companies continue to transition to more cost-efficient cloud-based solutions, their email and other valuable data migrate along with them. Criminals simply shift their focus and adapt their tactics to locate and steal the data they find to be of most value. Consequently, there's been a corresponding increase in hacking cloud-based email servers via the use of stolen credentials. This is not an indication that cloud-based services are less secure, however. It is simply that phishing attacks, credential theft and configuration errors are a natural by-product of the process.

What a tangled web we weave

Payment card web application compromises are well on their way to exceeding physical terminal compromises in payment card-related breaches. Data from one of our contributors, the National Cyber-Forensics and Training Alliance (NCFTA), substantiates this shift appears to have already occurred, and our larger data set is also trending that way.

Still held for ransom

Ransomware attacks are still going strong, and account for nearly 24 percent of incidents where malware was used. Ransomware has become so commonplace that it is less frequently mentioned in the specialized media unless there is a high-profile target in the mix. However, it is still a serious threat to all industries. Meanwhile, some other threats that are frequently hyped, such as cryptomining (2% of malware), occur very infrequently in our data set.

Chip and Pin for the win?

The number of physical terminal compromises in payment card-related breaches is decreasing when compared to web application compromises. This may be partly due to the implementation of chip and pin payment technology starting to show progress.

HR strikes back

Interestingly, attacks on Human Resource personnel have decreased from last year. Our data set showed 6x fewer Human Resource personnel being impacted this year compared to last. This correlates with W-2 tax form scams almost disappearing entirely from the DBIR data set.

I click, therefore I am

Click-through rates on phishing simulations for data partners fell from 24% to 3% during the past seven years. But 18% of people who clicked on test phishing links did so on mobile devices. Research shows mobile users are more susceptible to phishing, probably because of their user interfaces and other factors. This is also the case for email-based spear phishing and social media attacks.

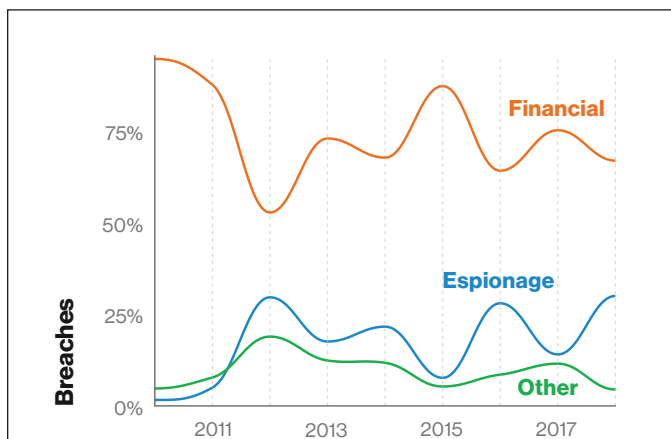


Figure 7. Threat actor motives in breaches over time

Where a motive is known or applicable, financial gain is the most common driver of data breaches, representing 71% of cases. Espionage is the motive in 25% of breaches.

Which threats does your industry face?

Every type of organization is at risk. But certain industries are more prone than others to specific kinds of attack. This is due to a multitude of factors, such as their business model, the type of data transmitted and retained, customer base, and even the various technologies needed to secure their environment. Knowing where an attack is most likely to occur offers the defender the opportunity to optimize their resources and helps to drive budget

allocation. Many DBIR readers go directly to their industry to understand the threats they and their peers face. But you can gain valuable perspective from the experiences of other sectors, as well.

Our 2019 DBIR features a deep dive into industries, and covers the specific threats, motivations and bad actors they face.

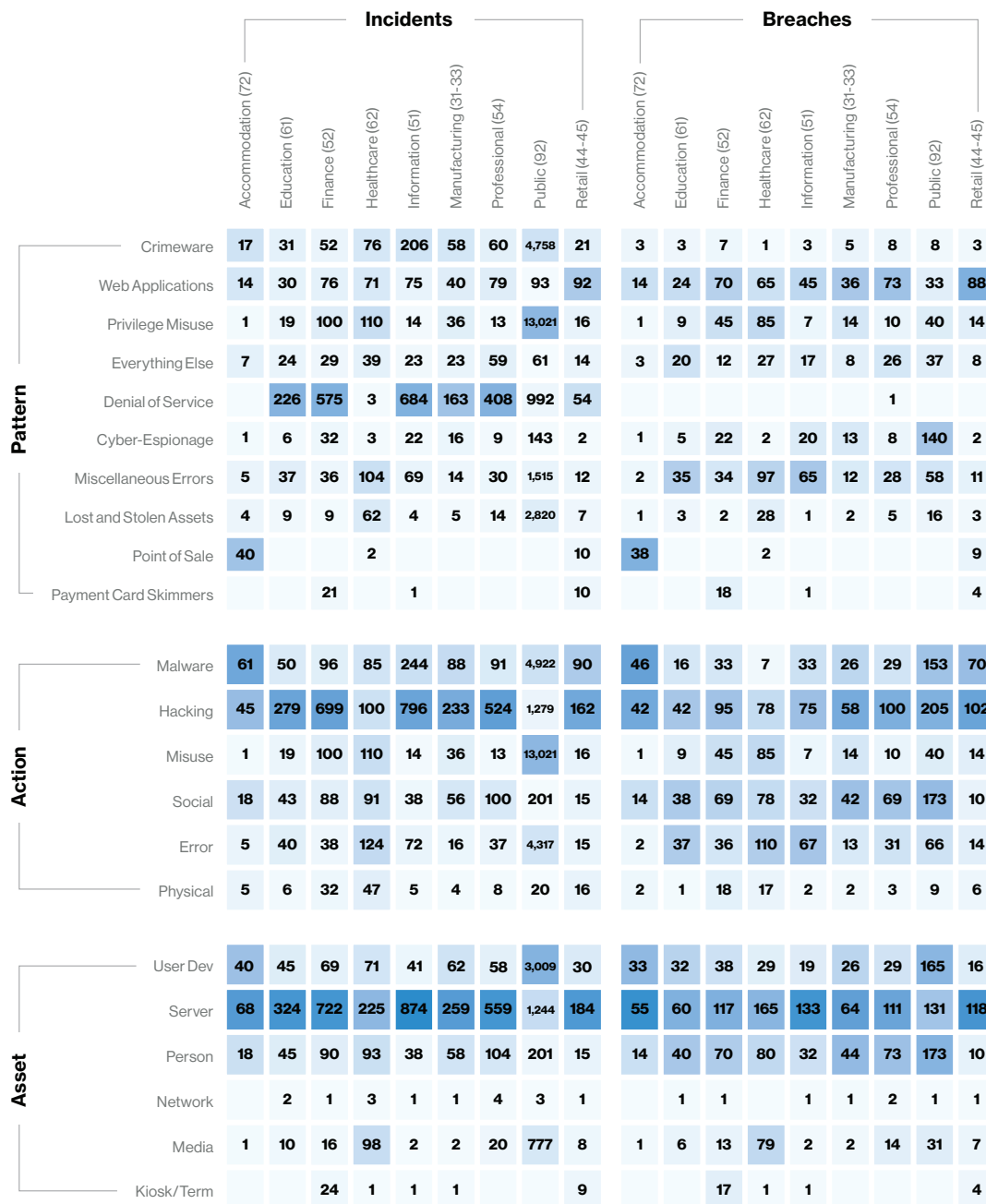
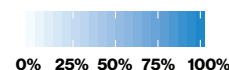


Figure 39. Industry Comparison
(left: all security incidents, right: only breaches)



Accommodation & Food Services

The breach totals in our data set have decreased from last year, primarily due to a lack of POS vendor incidents that have led to numerous organizations being compromised with stolen partner credentials.

Frequency	87 incidents, 61 with confirmed data disclosure
Top 3 patterns	Point of Sale intrusions, Web applications and Crimeware patterns represent 93% of all data breaches within Accommodation
Threat actors	External (95%), Internal (5%) (breaches)
Actor motives	Financial (100%) (breaches)
Data compromised	Payment (77%), Credentials (25%), Internal (19%) (breaches)

Educational Services

Education continues to be plagued by errors, social engineering and inadequately secured email credentials. With regard to incidents, DoS attacks account for over half of all incidents in Education.

Frequency	382 incidents, 99 with confirmed data disclosure
Top 3 patterns	Miscellaneous Errors, Web Application Attacks, and Everything Else represent 80% of breaches
Threat actors	External (57%), Internal (45%), Multiple parties (2%) (breaches)
Actor motives	Financial (80%), Espionage (11%), Fun (4%), Grudge (2%), Ideology (2%) (breaches)
Data compromised	Personal (55%), Credentials (53%), and Internal (35%) (breaches)

Financial and Insurance

Denial of Service and use of stolen credentials on banking applications remain common. Compromised email accounts become evident once those attacked are filtered. ATM Skimming continues to decline.

Frequency	927 incidents, 207 with confirmed data disclosure
Top 3 patterns	Web Applications, Privilege Misuse, and Miscellaneous Errors represent 72% of breaches
Threat actors	External (72%), Internal (36%), Multiple parties (10%), Partner (2%) (breaches)
Actor motives	Financial (88%), Espionage (10%) (breaches)
Data compromised	Personal (43%), Credentials (38%), Internal (38%) (breaches)

Healthcare

Healthcare stands out due to the majority of breaches being associated with internal actors. Denial of Service attacks are infrequent, but availability issues arise in the form of ransomware.

Frequency	466 incidents, 304 with confirmed data disclosure
Top 3 patterns	Miscellaneous Errors, Privilege Misuse and Web Applications represent 81% of incidents within Healthcare
Threat actors	Internal (59%), External (42%), Partner (4%), and Multiple parties (3%) (breaches)
Actor motives	Financial (83%), Fun (6%), Convenience (3%), Grudge (3%), and Espionage (2%) (breaches)
Data compromised	Medical (72%), Personal (34%), Credentials (25%) (breaches)

Information

Web applications are targeted with availability attacks as well as leveraged for access to cloud-based organizational email accounts.

Frequency	1,094 Incidents, 155 with confirmed data disclosure
Top 3 patterns	Miscellaneous Errors, Web Applications, and Cyber-Espionage represent 83% of breaches within Information
Threat actors	External (56%), Internal (44%), Partner (2%) (breaches)
Actor motives	Financial (67%), Espionage (29%) (breaches)
Data compromised	Personal (47%), Credentials (34%), Secrets (22%) (breaches)

Manufacturing

Manufacturing has been experiencing an increase in financially motivated breaches in the past couple of years, but espionage is still a strong motivator. Most breaches involve phishing and the use of stolen credentials.

Frequency	352 incidents, 87 with confirmed data disclosure
Top 3 patterns	Web Applications, Privilege Misuse, and Cyber-Espionage represent 71% of breaches
Threat actors	External (75%), Internal (30%), Multiple parties (6%), Partner (1%) (breaches)
Actor motives	Financial (68%), Espionage (27%), Grudge (3%), Fun (2%) (breaches)
Data compromised	Credentials (49%), Internal (41%), Secrets (36%)(breaches)

Professional, Technical & Scientific Services

Phishing and credential theft associated with cloud-based mail accounts have risen as the prominent attack types.

Frequency	670 incidents, 157 with confirmed data disclosure
Top 3 patterns	Web Applications, Everything Else, and Miscellaneous Errors represent 81% of breaches within Professional Services
Threat actors	External (77%), Internal (21%), Partner (5%), Multiple parties (3%) (breaches)
Actor motives	Financial (88%), Espionage (14%), Convenience (2%) (breaches)
Data compromised	Credentials (50%), Internal (50%), Personal (46%) (breaches)

Public Administration

Cyber-Espionage is rampant in the Public sector, with State-affiliated actors accounting for 79 percent of all breaches involving external actors. Privilege Misuse and Error by insiders account for 30 percent of breaches.

Frequency	23,399 incidents, 330 with confirmed data disclosure
Top 3 patterns	Cyber-Espionage, Miscellaneous Errors and Privilege Misuse represent 72% of breaches
Threat actors	External (75%), Internal (30%), Partner (1%), Multiple parties (6%) (breaches)
Actor motives	Espionage (66%), Financial (29%), Other (2%) (breaches)
Data compromised	Internal (68%), Personal (22%), Credentials (12%) (breaches)

Retail

Card present breaches involving POS compromises or gas-pump skimmers continue to decline. Attacks against e-commerce payment applications are satisfying the financial motives of the threat actors targeting this industry.

Frequency	234 incidents, 139 with confirmed data disclosure
Top 3 patterns	Web Applications, Privilege Misuse, and Miscellaneous Errors represent 81% of breaches
Threat actors	External (81%), Internal (19%) (breaches)
Actor motives	Financial (97%), Fun (2%), Espionage (2%) (breaches)
Data compromised	Payment (64%), Credentials (20%), Personal (16%) (breaches)

Use actionable intelligence to strengthen your security

As security threats and attackers constantly evolve, Information Security professionals may feel attackers are outpacing efforts to stop them. But security professionals and business leaders have powerful tools of their own to deploy against bad actors.

The most important defense is knowledge. By gaining perspective, insight and understanding of the threats they face, organizations can take crucial steps to mitigate them. The DBIR can play an important role in providing up-to-date knowledge. Since 2014, we've specified nine incident patterns that comprise the majority of incidents and breaches. Being aware of these can help you configure your security methods and use your budget to address likely threats.

98% of security incidents and 88% of data breaches continue to occur within one of nine patterns.

The stakes are high, with organizations' data, customer base, proprietary business information and trade secrets vulnerable to attacks. Data breaches continue to threaten organizational reputations and finances. But security professionals have the power to meet these challenges.

Get all the details, including industry-specific attack patterns, in the 2019 DBIR.

Sizing the losses

The FBI Internet Crime Complaint Center (IC3) contributed to the DBIR this year with impact data from business email compromise (BEC) and computer data breach (CDB) reports. Median direct losses to threat actors are about \$8,000 for BECs and \$25,000 for CDBs.

They work hard for the money

Additionally, when the IC3 Recovery Asset Team acts upon BECs and works with the destination bank, half of all US-based business email compromise victims had 99% of the money recovered or frozen; and only 9% had nothing recovered.

Some best practices to prevent breaches

Keep it clean.

Many breaches are a result of poor security hygiene and a lack of attention to detail. Clean up human error where possible, then establish an asset and security baseline around internet-facing assets like web servers and cloud services.

Maintain integrity.

Web application compromises now include code that can capture data entered into web forms. Consider adding file integrity monitoring on payment sites, in addition to patching operating systems and coding payment applications.

Redouble your efforts.

2FA everything. Use strong authentication on customer-facing applications, any remote access and cloud-based email. There are examples of 2FA vulnerabilities, but they don't excuse lack of implementation.

Be wary of inside jobs.

Track insider behavior by monitoring and logging access to sensitive data. Make it clear to staff just how good you are at recognizing fraudulent transactions.

Scrub packets.

Distributed denial of service (DDoS) protection is an essential control for many industries. Guard against nonmalicious interruptions with continuous monitoring and capacity planning for traffic spikes.

Stay socially aware.

Social attacks are effective ways to capture credentials. Monitor email for links and executables. Give your teams ways to report potential phishing or pretexting.

The 2019 Verizon Data Breach Investigations Report offers security professionals and business leaders worldwide a comprehensive look at the threat landscape – how threats are changing, and the newest best practices to mitigate those risks. The 2019 report is based on a detailed analysis of 41,686 security incidents, including 2,013 confirmed data breaches. Now in its 12th year, the DBIR is recognized as one of the security industry's most respected sources of insight and data.

Download the full report:

verizonenterprise.com/DBIR2019

2019 Data Breach Investigations Report Executive Summary

