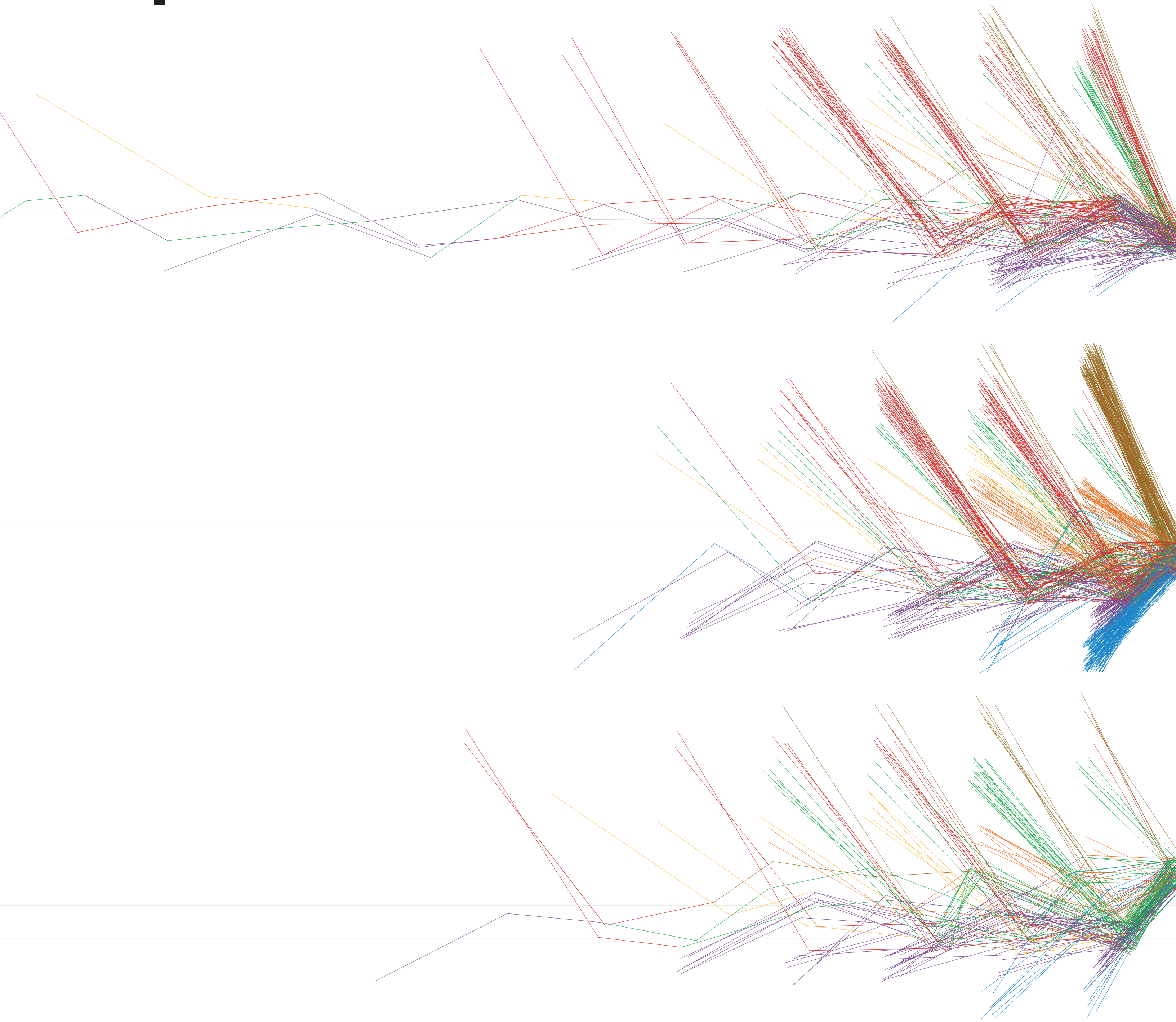
Executive Summary

2019 Data Breach Investigations Report



verizon
business ready

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?

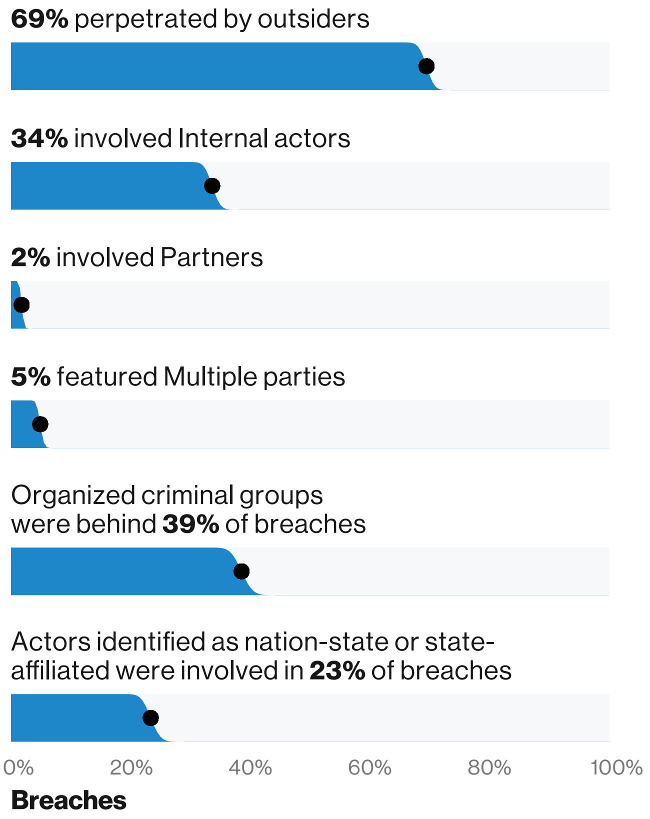


Figure 1.

Who are the breach victims?

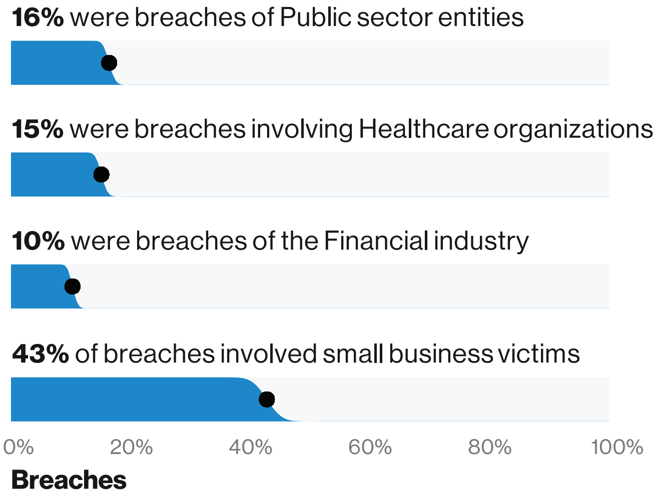


Figure 2.

What actions are being used?

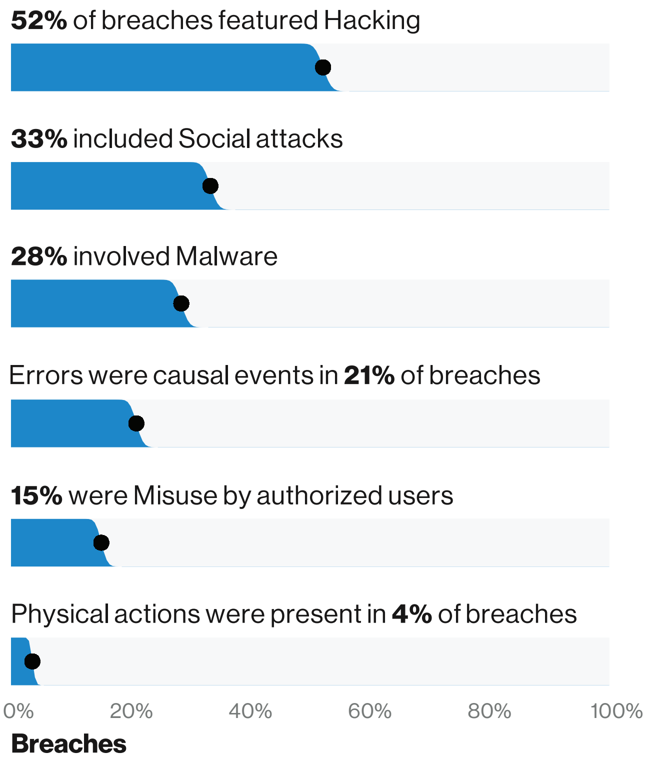


Figure 3.

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.

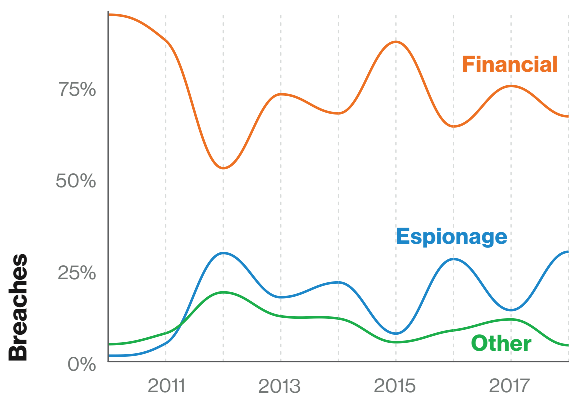


Figure 7. Threat actor motives in breaches over time

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.

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.

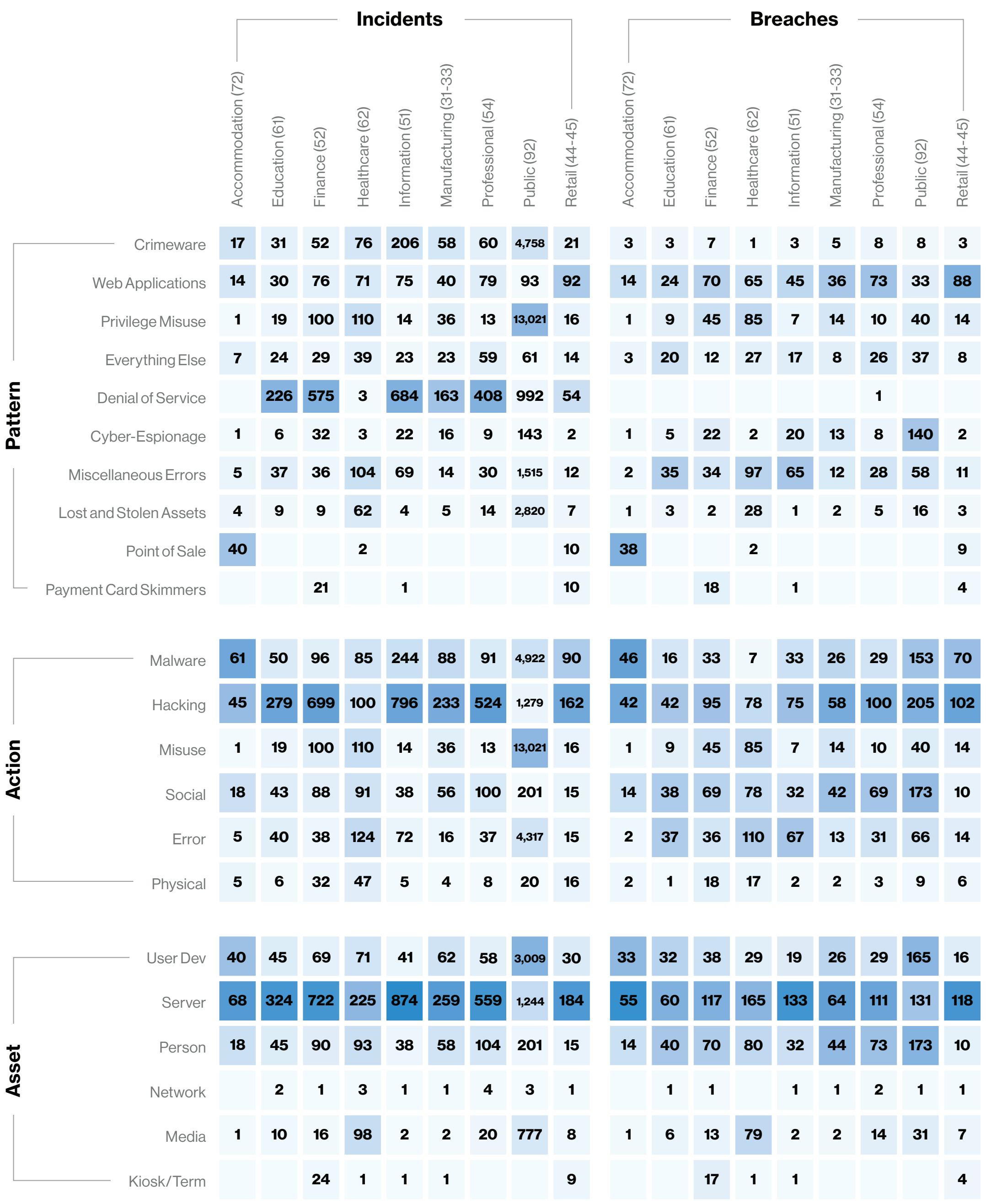
Chip and Pin for the win?
The number of physical terminal compromises in payment card-related breaches is decreasing when compared to web application compromises. This may be partly due to the implementation of chip and pin payment technology starting to show progress.

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.

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.



		Incidents									Breaches								
		Accommodation (72)	Education (61)	Finance (52)	Healthcare (62)	Information (51)	Manufacturing (31-33)	Professional (54)	Public (92)	Retail (44-45)	Accommodation (72)	Education (61)	Finance (52)	Healthcare (62)	Information (51)	Manufacturing (31-33)	Professional (54)	Public (92)	Retail (44-45)
Pattern	Crimeware	17	31	52	76	206	58	60	4,758	21	3	3	7	1	3	5	8	8	3
	Web Applications	14	30	76	71	75	40	79	93	92	14	24	70	65	45	36	73	33	88
	Privilege Misuse	1	19	100	110	14	36	13	13,021	16	1	9	45	85	7	14	10	40	14
	Everything Else	7	24	29	39	23	23	59	61	14	3	20	12	27	17	8	26	37	8
	Denial of Service		226	575	3	684	163	408	992	54							1		
	Cyber-Espionage	1	6	32	3	22	16	9	143	2	1	5	22	2	20	13	8	140	2
	Miscellaneous Errors	5	37	36	104	69	14	30	1,515	12	2	35	34	97	65	12	28	58	11
	Lost and Stolen Assets	4	9	9	62	4	5	14	2,820	7	1	3	2	28	1	2	5	16	3
	Point of Sale	40			2					10	38			2					9
	Payment Card Skimmers			21		1				10			18		1				4
Action	Malware	61	50	96	85	244	88	91	4,922	90	46	16	33	7	33	26	29	153	70
	Hacking	45	279	699	100	796	233	524	1,279	162	42	42	95	78	75	58	100	205	102
	Misuse	1	19	100	110	14	36	13	13,021	16	1	9	45	85	7	14	10	40	14
	Social	18	43	88	91	38	56	100	201	15	14	38	69	78	32	42	69	173	10
	Error	5	40	38	124	72	16	37	4,317	15	2	37	36	110	67	13	31	66	14
	Physical	5	6	32	47	5	4	8	20	16	2	1	18	17	2	2	3	9	6
Asset	User Dev	40	45	69	71	41	62	58	3,009	30	33	32	38	29	19	26	29	165	16
	Server	68	324	722	225	874	259	559	1,244	184	55	60	117	165	133	64	111	131	118
	Person	18	45	90	93	38	58	104	201	15	14	40	70	80	32	44	73	173	10
	Network		2	1	3	1	1	4	3	1		1	1		1	1	2	1	1
	Media	1	10	16	98	2	2	20	777	8	1	6	13	79	2	2	14	31	7
	Kiosk/Term			24	1	1	1			9			17	1	1				4

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 $25,000 for BECs and $8,000 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:
enterprise.verizon.com/DBIR2019/

2019 Data Breach Investigations Report Executive Summary