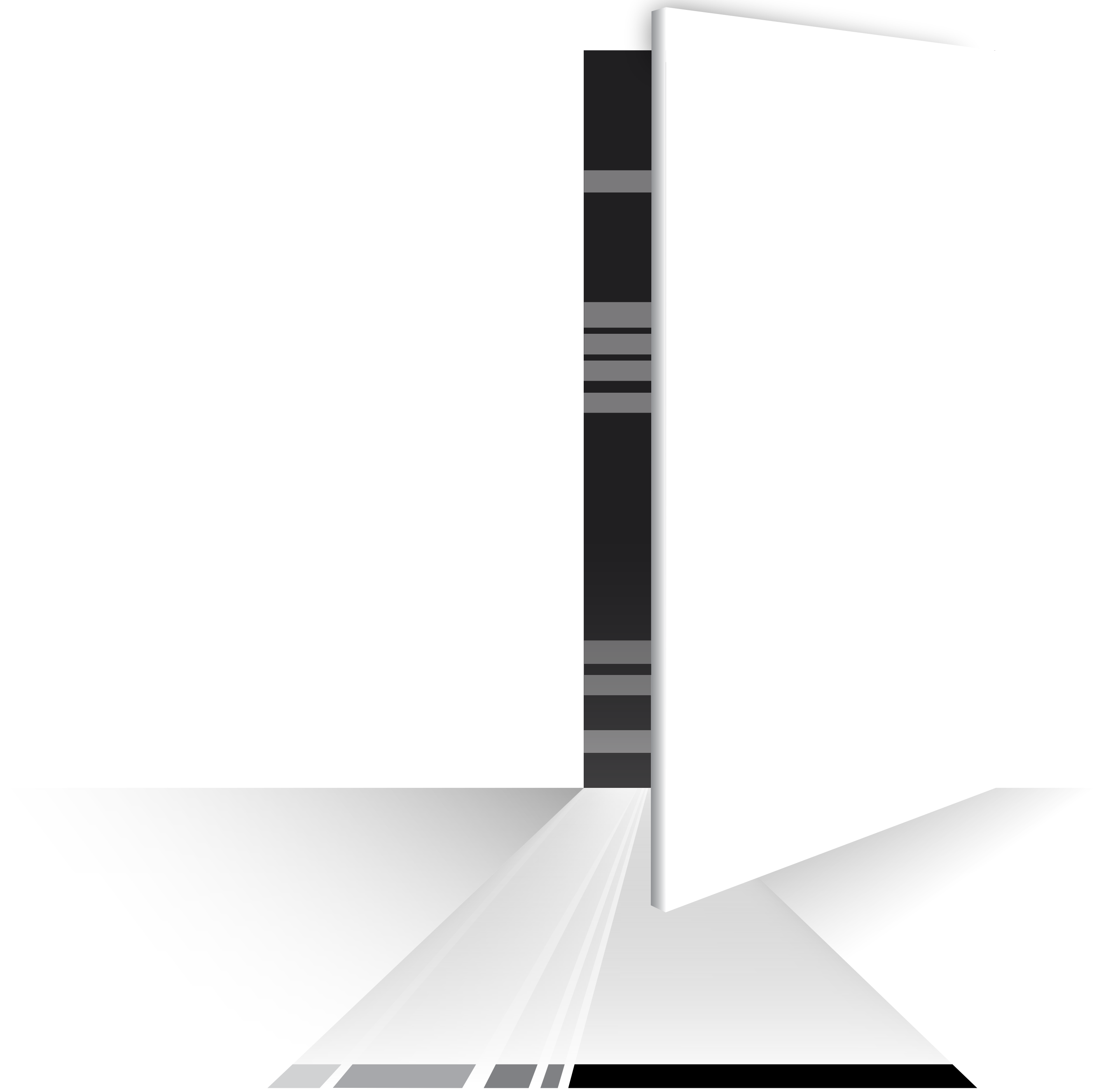
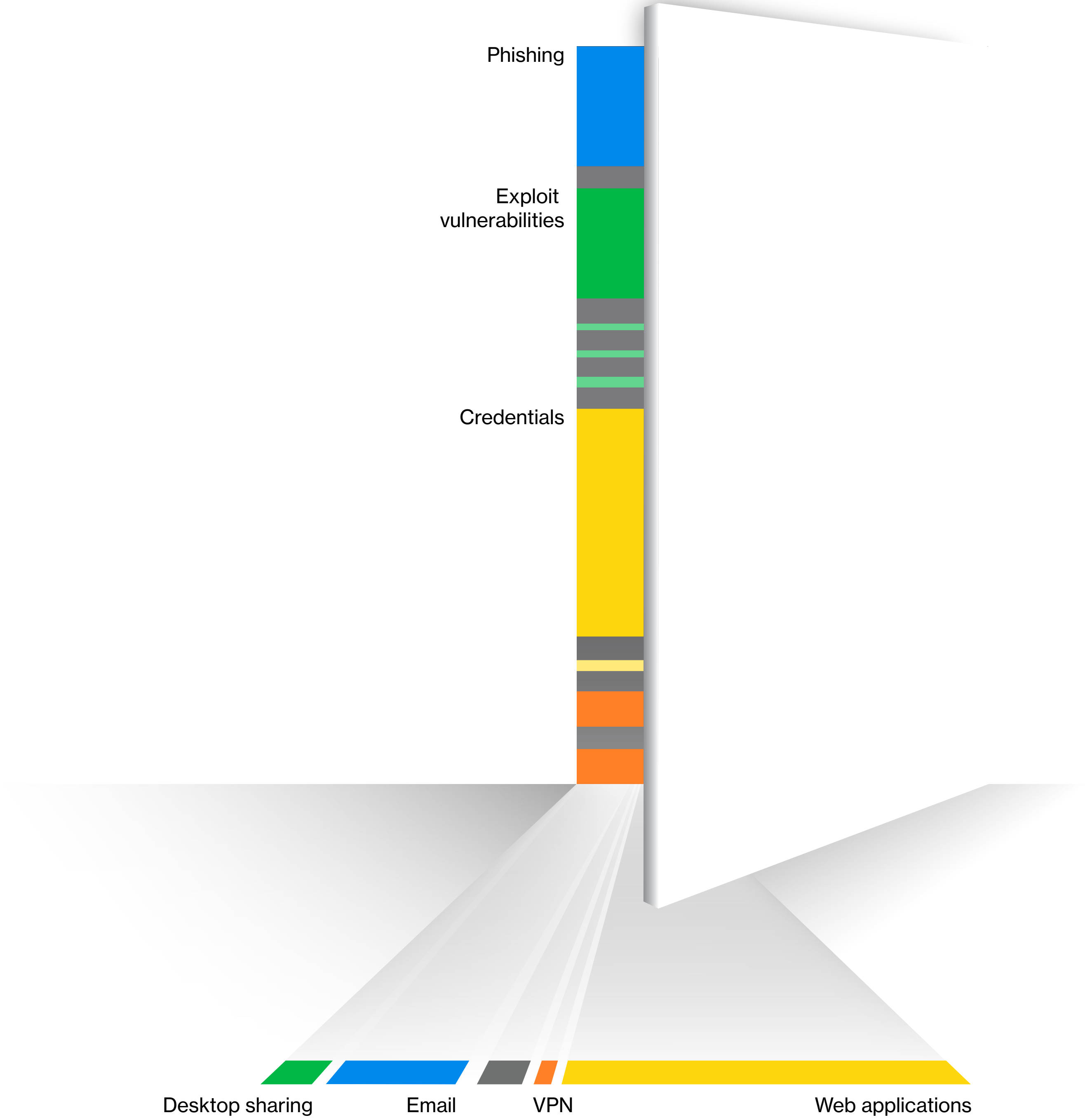
2024 Data Breach Investigations Report

Executive Summary



verizon business


Phishing
Exploit vulnerabilities
Credentials
Desktop sharing
Email
VPN
Web applications

About the cover

This year, the report is delving deeper into the pathway to breaches in an effort to identify the most likely Action and vector groupings that lead to breaches given the current threat landscape. The cracked doorway on the cover is meant to represent the various ways attackers can make their way inside. The opening in the door shows the pattern of our combined "ways-in" percentages (see Figure 7 of the full report for a more straightforward representation), and it lets out a band of light displaying a pattern of the Action vector quantities. The inner cover highlights and labels the quantities in a less abstract way. Hope you enjoy our art house phase.

Table of contents

Welcome

Greetings! Welcome to Verizon's 2024 Data Breach Investigations Report (DBIR).

This year marks the 17th edition of this publication, and we are thrilled to welcome back our old friends and say hello to new readers. As always, the aim of the DBIR is to shine a light on the various Actor types, the tactics they utilize and the targets they choose. Thanks to our talented, generous and civic-minded contributors from around the world who continue to stick with us and share their data and insight, and deep appreciation for our very own Verizon Threat Research Advisory Center (VTRAC) team (rock stars that they are). These two groups enable us to examine and analyze relevant trends in cybercrime that play out on a global stage across organizations of all sizes and types.

From year to year, we see both new and innovative attacks as well as variations on tried-and-true attacks that still remain successful. From the exploitation of well-known and far-reaching zero-day vulnerabilities, such as the one that affected MOVEit, to the much more mundane but still incredibly effective Ransomware, Use of stolen credentials and Denial of Service (DoS) attacks, criminals continue to do their utmost to prove the old adage “crime does not pay” wrong.

The shifting landscape of cyber threats can be confusing and overwhelming, and the past year has been a particularly busy one for cybercrime. We analyzed a record high 30,458 real-world security incidents, of which 10,626 were confirmed data breaches, with victims spanning 94 countries. The following pages provide a few of the more relevant points from the report itself. We hope that you find them useful and informative.

Please continue reading for report highlights, including the latest breach findings for industries and regions. Please feel free to pass this summary to colleagues and download the full report for a more in-depth view of the threats you might face today.

Report highlights/ summary of findings

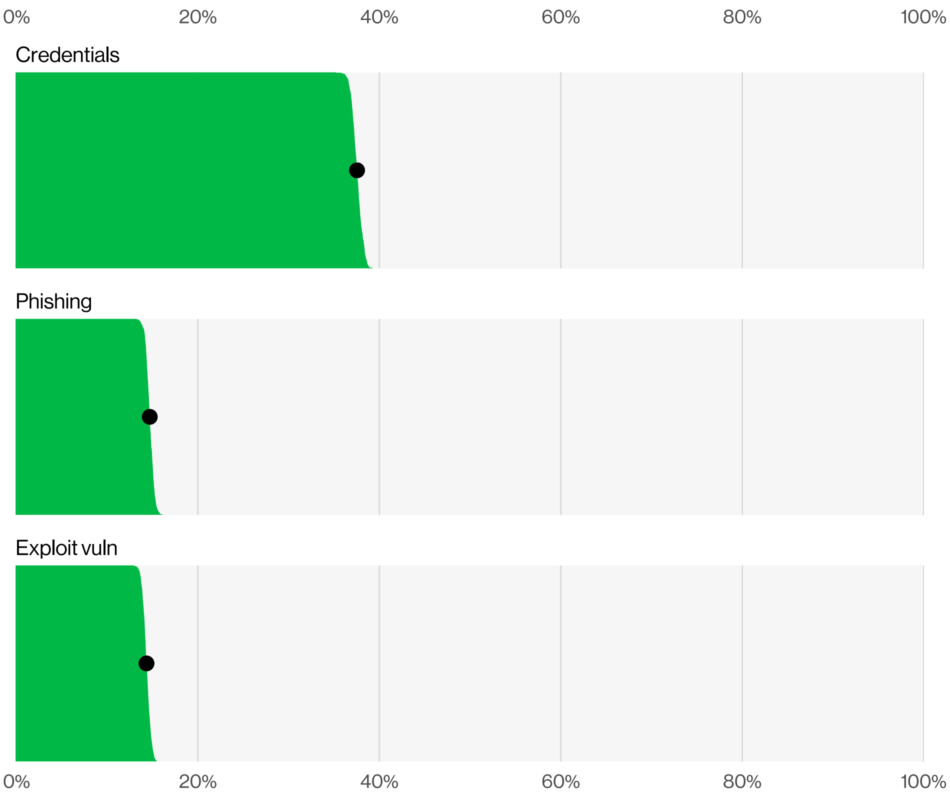


Figure 1. Select ways-in enumerations in non-Error, non-Misuse breaches (n=6,963)

Our ways-in analysis witnessed a substantial growth of attacks involving the exploitation of vulnerabilities as the critical path to initiate a breach when compared to previous years—almost tripling (180% increase) from last year. This was largely due to the effect of MOVEit and similar zero-day vulnerabilities, primarily leveraged by ransomware and other extortion-related threat actors using Web applications as their initial entry points.

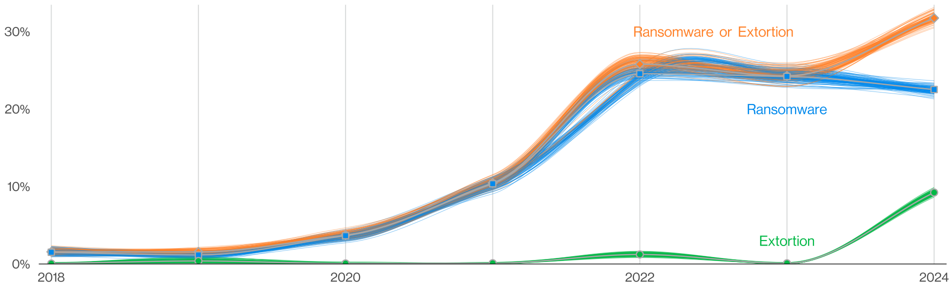


Figure 2. Ransomware and Extortion breaches over time

Roughly one-third of all breaches involved Ransomware or some other Extortion technique. Pure Extortion attacks have risen over the past year and are now a component of 9% of all breaches. Ransomware actors have moved toward these newer techniques, resulting in a bit of a decline in Ransomware to 23%. However, when combined, they represent a strong growth to 32% of breaches. Additionally, Ransomware was a top threat across 92% of industries.

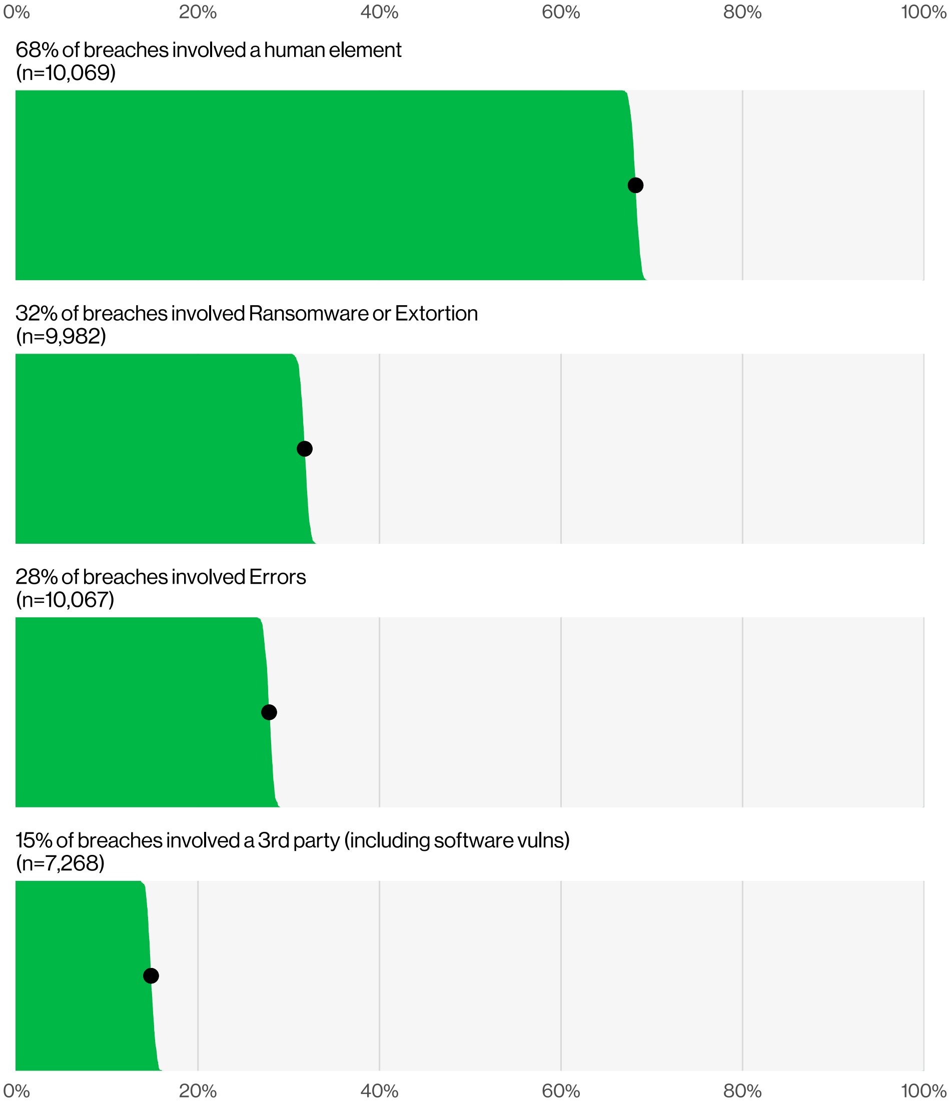


Figure 3. Select key enumerations in breaches

We have revised our calculation of the human element in breaches to exclude malicious Privilege Misuse to provide a clearer metric of what security awareness can impact. For this year's dataset, the human element was a component of 68% of breaches, roughly the same as the previous period described in the 2023 DBIR.

In this issue, we are introducing an expanded concept of a breach involving a third party to include partner infrastructure being affected and direct or indirect software supply chain issues—including when an organization is affected by vulnerabilities in third-party software. In short, these are the breaches an organization could potentially mitigate or prevent by trying to select vendors with better security track records. We see this figure at 15% this year, a 68% increase from the previous year, mostly fueled by the use of zero-day exploits for Ransomware and Extortion attacks.

Our dataset saw a growth of breaches involving Errors, now at 28%, as we broadened our contributor base to include several new mandatory breach notification entities. This validates our suspicion that errors are more prevalent than media or traditional incident response–driven bias would have us believe.

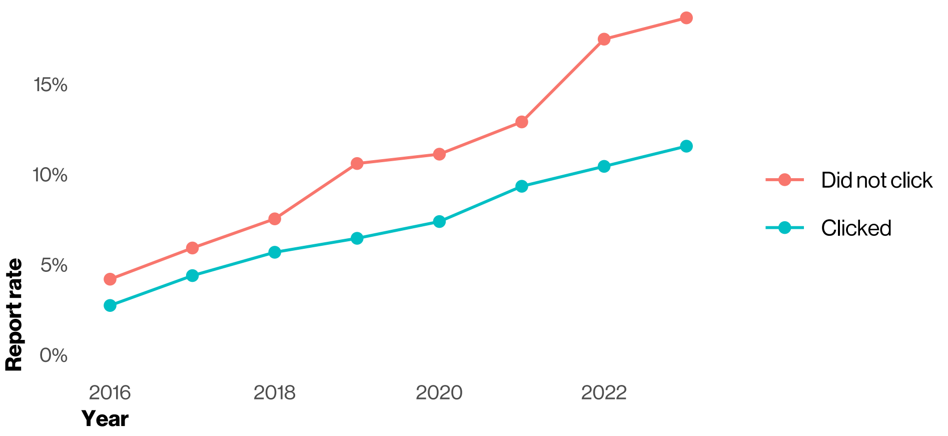


Figure 4. Phishing email report rate by click status

The overall reporting rate of Phishing has been growing over the past few years. In security awareness exercise data contributed by our partners during 2023, 20% of users reported phishing in simulation engagements, and 11% of the users who clicked the email also reported. This is welcome news because the median time to click on a malicious link after the email is opened is 21 seconds and then only another 28 seconds for the person caught in the phishing scheme to enter their data. This leads to an alarming finding: The median time for users to fall for phishing emails is less than 60 seconds.

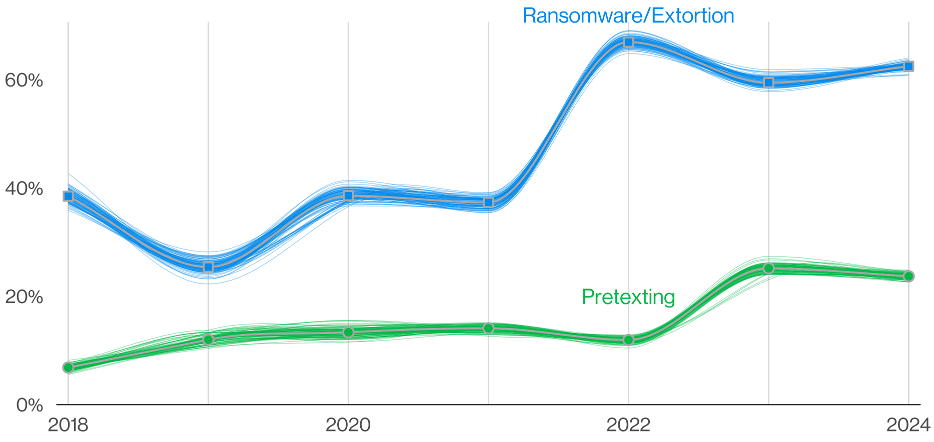


Figure 5. Select action varieties in Financial motive over time

Financially motivated threat actors will typically stick to the attack techniques that give them the most return on investment.

Over the past three years, the combination of Ransomware and other Extortion breaches have accounted for almost two-thirds (fluctuating between 59% and 66%) of those attacks. According to the FBI's Internet Crime Complaint Center (IC3) ransomware complaint data, the median loss associated with the combination of Ransomware and other Extortion breaches has been $46,000, ranging between $3 (three dollars) and $1,141,467 for 95% of cases. We also found from ransomware negotiation data contributors that the median ratio of initially requested ransom and company revenue is 1.34%, but it fluctuated between 0.13% and 8.3% for 80% of the cases.

Similarly, over the past two years, we have seen incidents involving Pretexting (the majority of which had Business Email Compromise [BEC] as the outcome) accounting for one-fourth (ranging between 24% and 25%) of financially motivated attacks. In both years, the median transaction amount of a BEC was around $50,000.

Industry highlights

As we have discussed in previous reports, what keeps one industry tossing and turning at night may not even register as a blip on another's radar. It all boils down to attack surfaces—the prime real estate for cyber malfeasance. When one factors in the nuances of specific types of threat actors, the technological infrastructures underpinning each sector, the type of data an organization handles and retains, and how folks access and use that data, you've mixed a potent cocktail of security complexities.

A tech behemoth swimming in the digital sea of mobile devices and their respective apps has a risk profile that looks markedly different from that of a boutique establishment relying on a point-of-sale system or a simple e-commerce platform supported by its vendor. At the end of the day, the threats that enterprises face vary according to industry, size and so on. Furthermore, industry findings are also influenced by reporting requirements, which means that different verticals may experience varying levels of scrutiny from that perspective. In this section, we take a high-level look at the nine industries we showcase in the report. Finally, it is important to keep in mind that we classify organizations using North American Industry Classification System (NAICS) codes.

Accommodation and Food Services

(NAICS 72)

Frequency	220 incidents, 106 with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering and Basic Web Application Attacks represent 92% of breaches
Threat actors	External (92%), Internal (9%) Multiple (1%) (breaches)
Actor motives	Financial (100%) (breaches)
Data compromised	Credentials (50%), Personal (28%), Payment (19%), System (19%), Other (16%) (breaches)
What is the same?	Ransomware and social attacks continue to be a persistent problem within this industry, accounting for 35% of incidents.
Summary	Social Engineering has increased dramatically and now accounts for 25% of incidents in this sector, with Pretexting more than doubling from the previous year and reporting 20% of incidents.

Educational Services
(NAICS 61)

Frequency	1,780 incidents, 1,537 with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering and Miscellaneous Errors represent 90% of breaches
Threat actors	External (68%), Internal (32%) (breaches)
Actor motives	Financial (98%), Espionage (2%) (breaches)
Data compromised	Personal (83%), Internal (20%), Other (18%), Credentials (9%) (breaches)
What is the same?	The same three patterns dominate this vertical as last year. External actors stealing Personal data accounts for the majority of breaches.
Summary	Errors of various types committed by internal actors and Extortion from external threat actors continue to constitute the curriculum of this industry.

Financial and Insurance
(NAICS 52)

Frequency	3,348 incidents, 1,115 with confirmed data disclosure
Top patterns	System Intrusion, Miscellaneous Errors and Social Engineering represent 78% of breaches
Threat actors	External (69%), Internal (31%) (breaches)
Actor motives	Financial (95%), Espionage (5%) (breaches)
Data compromised	Personal (75%), Other (30%), Bank (27%), Credentials (22%) (breaches)
What is the same?	Miscellaneous Errors continue to plague this industry. As it did last year, Misdelivery presents an ongoing challenge for this sector.
Summary	System Intrusion has overtaken Miscellaneous Errors and Basic Web Application Attacks as the primary threat in Financial and Insurance this year, indicating a shift toward more complex attacks, accompanied by a rise in Social Engineering. Increased visibility into the Europe, Middle East and Africa (EMEA) region shows us that Ransomware attacks are alive and well there as well.

Healthcare

(NAICS 62)

Frequency	1,378 incidents, 1,220 with confirmed data disclosure
Top patterns	Miscellaneous Errors, Privilege Misuse and System Intrusion represent 83% of breaches
Threat actors	Internal (70%), External (30%) (breaches)
Actor motives	Financial (98%), Espionage (1%) (breaches)
Data compromised	Personal (75%), Internal (51%), Other (25%), Credentials (13%) (breaches)
What is the same?	System Intrusion breaches remain in the top three attack patterns.
Summary	This year's Healthcare sector analysis reveals significant shifts compared to previous years. Insiders deliberately causing breaches have surged back into second place after a steady decline since 2018. Interestingly, Personal data has eclipsed Medical data as the preferred target for threat actors.

Information

(NAICS 51)

Frequency	1,367 incidents, 602 with confirmed data disclosure
Top patterns	System Intrusion, Basic Web Application Attacks and Social Engineering represent 79% of breaches
Threat actors	External (79%), Internal (21%), Multiple (1%) (breaches)
Actor motives	Financial (87%), Espionage (14%) (breaches)
Data compromised	Other (46%), Personal (45%), Credentials (27%), Internal (22%) (breaches)
What is the same?	The top three attack patterns remain constant since last year, and their ranked order has also not changed. The team found this somewhat interesting considering how many more breaches we had in this sector as compared to last year.
Summary	The overall breach sample size increased compared to last year, but this sector experienced substantially fewer incidents. Ransomware and Use of stolen credentials continue to dominate the System Intrusion pattern. There was a slight decrease in Phishing attacks alongside a rise in Pretexting within the Social Engineering pattern. We also saw a mild increase in Espionage motives and state-sponsored actors targeting the industry, emphasizing the need for enhanced detective controls.

Manufacturing

(NAICS 31–33)

Frequency	2,305 incidents, 849 with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering and Miscellaneous Errors represent 83% of breaches
Threat actors	External (73%), Internal (27%) (breaches)
Actor motives	Financial (97%), Espionage (3%) (breaches)
Data compromised	Personal (58%), Other (40%), Credentials (28%), Internal (25%) (breaches)
What is the same?	Two of the top patterns from last year are still in place. Financial motivation continues to be the driver behind most attacks.
Summary	Manufacturing has seen an increase in Error-related breaches. The installation of malware after hacking in via the Use of stolen credentials is also somewhat commonplace.

Professional, Scientific and Technical Services

(NAICS 54)

Frequency	2,599 incidents, 1,314 with confirmed data disclosure
Top patterns	Social Engineering, System Intrusion and Miscellaneous Errors represent 85% of breaches
Threat actors	External (75%), Internal (25%) (breaches)
Actor motives	Financial (95%), Espionage (6%) (breaches)
Data compromised	Personal (40%), Credentials (38%), Other (33%), Internal (23%) (breaches)
What is the same?	Personal data and Credentials are still the top types of data affected in this industry.
Summary	Social Engineering is one of the top threats facing this industry, accounting for 40% of breaches, with just 20% of breaches the result of Pretexting. In addition, there has been an increase in errors, specifically Misdelivery.

Public Administration

(NAICS 92)

Frequency	12,217 incidents, 1,085 with confirmed data disclosure
Top patterns	Miscellaneous Errors, System Intrusion and Social Engineering represent 78% of breaches
Threat actors	Internal (59%), External (41%) (breaches)
Actor motives	Financial (71%), Espionage (29%) (breaches)
Data compromised	Personal (72%), Internal (37%), Other (31%), Credentials (17%) (breaches)
What is the same?	System Intrusion and Social Engineering remain top attack patterns in this sector.
Summary	Miscellaneous Errors, particularly Misdelivery, have surged to the top spot in this industry, reflecting the commonality of mistakes leading to breaches. System Intrusion now ranks second, followed by Social Engineering. The predominance of internal actors underscores the potential consequences of employee carelessness, with Errors accounting for the majority of breaches.

Retail

(NAICS 44–45)

Frequency	725 incidents, 369 with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering and Basic Web Application Attacks represent 92% of breaches
Threat actors	External (96%), Internal (4%) (breaches)
Actor motives	Financial (99%), Espionage (1%) (breaches)
Data compromised	Credentials (38%), Other (31%), Payment (25%), System (20%) (breaches)
What is the same?	The three attack patterns not only remain consistent but are even in the same ranked order as last year. Threat actors with a Financial motivation continue to target this sector.
Summary	While this industry is usually the place where we see Payment card data stolen, the focus of the threat actors has shifted to Credentials. Pretexting is also increasing, while Phishing has dropped. Denial of Service attacks remain a problem for Retail organizations, causing disruption to their ability to serve their customers and make sales.

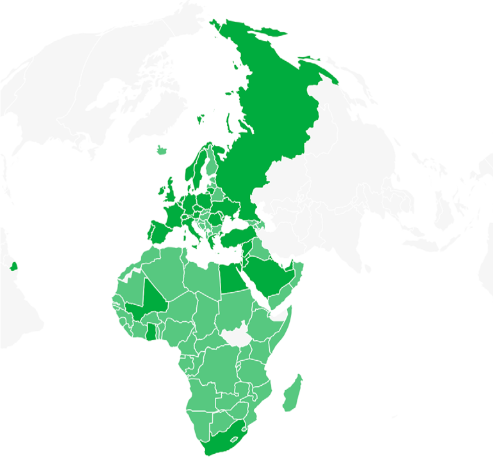
Regional findings

The 2024 DBIR once again provides a macro-regional view into the analysis of incidents and breaches in our dataset. We do this in the hope that it provides a quick and easy way for readers to learn how cybercrime trends differ and how they remain consistent from one geographical region of the world to the next. As we have mentioned in the past, we have greater or lesser visibility into a given region based on numerous factors, such as contributor presence, regional disclosure regulations and our own caseload. It is our hope that our readers find this more global view of cybercrime helpful and informative.

Asia Pacific (APAC)

Frequency	2,130 incidents, 523 with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering and Basic Web Application Attacks represent 95% of breaches
Threat actors	External (98%), Internal (2%) (breaches)
Actor motives	Financial (75%), Espionage (25%) (breaches)
Data compromised	Credentials (69%), Internal (37%), Secrets (24%), Other (17%) (breaches)

Europe, Middle East and Africa (EMEA)



Frequency	8,302 incidents, 6,005 with confirmed data disclosure
Top patterns	Miscellaneous Errors, System Intrusion and Social Engineering represent 87% of breaches
Threat actors	External (51%), Internal (49%) (breaches)
Actor motives	Financial (94%), Espionage (6%) (breaches)
Data compromised	Personal (64%), Other (36%), Internal (33%), Credentials (20%) (breaches)

Northern America (NA)

Frequency	16,619 incidents, 1,877 with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering and Basic Web Application Attacks represent 91% of breaches
Threat actors	External (93%), Internal (8%) (breaches)
Actor motives	Financial (97%), Espionage (4%) (breaches)
Data compromised	Personal (50%), Credentials (26%), Internal (19%), Other (16%) (breaches)

Stay informed and threat ready.

Facing today's threats requires intelligence from a source you can trust.

The full DBIR contains details on the actors, actions and patterns that can help you prepare your defenses and educate your organization. Get the intelligence you need to help protect your organization:

Read the full 2024 DBIR at verizon.com/dbir.

Want to make the world of cybersecurity a safer place?

If your organization aggregates incident or security data and is interested in becoming a contributor to the annual Verizon DBIR (and we hope you are), the process is very easy and straightforward. Please email us at dbircontributor@verizon.com.

Please feel free to provide us feedback for improving the DBIR at dbir@verizon.com, tweet us @VZDBIR and check out the VERIS GitHub page: https://github.com/vz-risk/veris.