12TH EDITION

2025 Data Breach Industry Forecast

Executive Summary

Global data breaches show no signs of slowing. In fact, according to the 2024 Verizon Data Breach Investigations Report, there have been 10,626 data compromises in the first three quarters of 2024, more than doubling last year's 5,199 total. Experian itself has supported more than 4,000 client data breaches in the first three quarters alone. According to our internal analytics, more than 66 million consumers globally were impacted by these data breaches from our client base in 2024—up 13 percent since last year.

No organization is immune from the fast-evolving, artificial intelligence-driven attacks from today's sophisticated fraudsters. From July's Disney's Slack messages leak to Ticketmaster and BBC in May, even the largest brands are susceptible.

One critical issue for businesses is the rising costs of data breaches. According to IBM's 2024 Cost of a Data Breach Report, the global average cost of a breach rose 10% from 2023, now standing at USD $4.88 million, the highest increase since the pandemic. Add to this the ancillary costs of lawsuits such as the $30 million settlement in September against DNA-testing company 23andMe over a genetics data breach that exposed the personal information of 6.4 million customers in 2023.

Reflecting on last year's predictions, AT&T's data breach that involved its third-party cloud service provider, Snowflake, and the theft of sensitive data from more than 70 million AT&T wireless customers is an example of our "Six Degrees of Separation" prediction. The Life360 data breach where hackers exploited a vulnerability in its back end integration with law enforcement tools is another such example. Spotlighting our "Little by little becomes a lot" prediction, the Holograph Crypto Exchange breach in June involved a small flaw in Holograph's smart contract code that enabled hackers to siphon off $26 million worth of Bitcoin and Ether.

In our 12th annual Data Breach Industry Forecast, our focus covers a wide swath of attacks from the personal (teens exploitation), corporate (increases in internal fraud), national (using dynamic identification as a fraud defense), and global (bad actors pursuing data centers). Spanning all these predictions is the dramatically accelerated speed and scaling of cyberattacks that are AI-enabled. This year's predictions come from Experian's long history of helping companies navigate breaches over the past 22 years. The following predictions represent what we see on the horizon in the world of data security incidents in 2025.

The Data Breach Industry Forecast is Experian's attempt at looking into our crystal ball and providing cybersecurity predictions for what may lie ahead. The predictions are not guaranteed, should not be relied on as formal advice and are intended for educational purposes only.

Contributors

Michael Bruemmer

Vice President, Global Data Breach Resolution

Michael Bruemmer is Vice President of Global Data Breach & Consumer Protection at Experian. The group is a leader helping businesses prepare for a data breach, manage consumer crisis response programs and mitigate consumer risk following incidents.

With more than 25 years in the industry, Michael brings a wealth of knowledge related to crisis response management from discovery to post-incident clean up. He has handled some of the nation's largest data breaches during his tenure with Experian and more than 60,000 to date. Michael has educated businesses of all sizes and sectors on pre-breach and breach response planning and delivery. This ranges from how to notify affected consumers, to call center set up and even how to implement identity theft protection services.

He is a respected speaker and presents to industry organizations across the country. He has provided insight to many trade and business media outlets including Dark Reading, IT Business, CIO, Info Security, Security Week, Health IT Security, Wall Street Journal, and American Banker among others. He has been a guest columnist for SecurityInfoWatch and has appeared on broadcast channels such as Fox Business.

He currently resides on the Ponemon Responsible Information Management (RIM) Board and NetDiligence Advisory Board.

He holds a Bachelor of Arts in Labor Economics from the University of Wisconsin-Madison.

Jim Steven

Head of Crisis & Data Response Services, UK

Jim Steven is Head of Crisis & Data Breach Response Services for Experian UK, building on the knowledge, experience and success of Experian's global data breach resolution offering.

His team works with businesses to help them manage and resource mass consumer crisis responses, including customer notification, contact center and credit/identity monitoring services for customers/employees affected by a crisis event. They also support clients in preparing and practicing readiness plans for potential incidents to mitigate the impact and speed of recovery.

Prior to joining Experian, Jim worked in the security and risk management industry providing expertise in security risk management solutions, travel risk management, aviation security and corporate security for some of the world's largest security companies.

01

Smells Like Teen Secret

According to the FBI, the **average age of someone arrested for cybercrime is 19 vs. 37 for any crime.** While findings from the Harvard School of Education say half (51%) of young people ages 14–22 reported using generative AI, and 31% said they use it to "make pictures or images." **Today, the world of cyber hacking is not confined to grown ups nor is the fallout.**

In one scenario, everyday teens are now the targets of emotional and reputation-damaging content from bad actors to harass or humiliate them or manipulate them into improper or illegal activities. Many of these bad actors are fellow teens using widely available generative AI tools to produce their deepfakes. Or we see many teens entering the world of cybercrime for fun or monetary gain. "**Across the country we're seeing increasingly sophisticated cybercrime being conducted by people who are younger and younger and younger,"** said William McKeen, a supervisory special agent with the FBI's Cyber Division, in a Wall Street Journal story. In fact, teenage cybercriminals, such as those in the *Lapsus$* group and the *Com* along with its offshoot *Scattered Spider*, have gained significant notoriety in recent years.

Sadly, many of them will have been recruited into the "business" by more sophisticated fraudsters, who reach them through online gaming, chat, and social media. As more states pass legislation against revenge porn, cyberbullying, and other forms of online fraudulent attacks, **the near future may see a dramatic increase in the number of teens prosecuted for hacking and fraud.**

02

The Enemy Within: Internal Fraud Will Rise

According to PwC, **57% of fraud is committed by company insiders** or a combination of insiders and outsiders, and insiders are behind 43% of fraud cases involving more than $100 million in losses. **The scary thing is this level of insider fraud occurred before the advent of generative AI.** An early 2024 report from Adecco Group reveals a staggering 70% adoption rate of AI in the workplace. The same report indicates that only 43% of C-suite executives believe their company's leadership team has sufficient AI skills and knowledge to understand the risks and opportunities offered by the technology. That's a lot of risk. **As more companies continue to train their employees on the responsible use of AI, we could see a marked increase in the use of that AI education by those very same employees for internal theft, sensitive information sourcing, and much more.** Next year may see at least one global brand impacted by fraud perpetrated by an insider to whom it provided educational AI training.

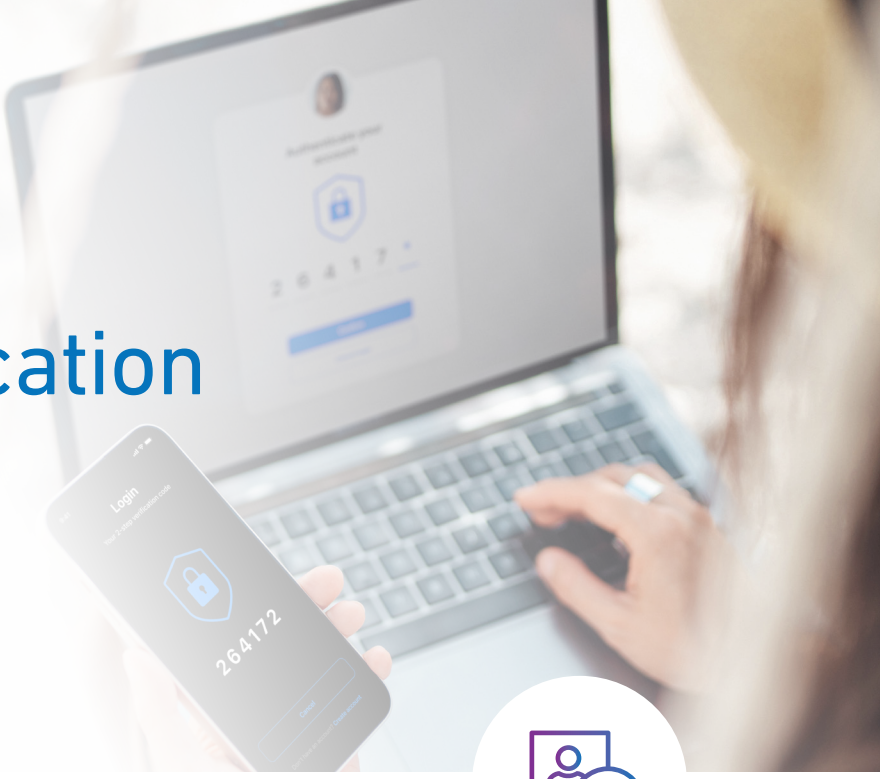
03

Eating Their Own: Predators Become Prey

A recent story of OnlyFans hackers being duped by sophisticated malware from a more malicious hacker and losing their funds points to a fast-growing trend in the highstakes world of cybercrime: the predators becoming the prey. Aspiring streaming service and social media hackers are succumbing to posts on hacker forums that – when opened – initiate harmful payloads, including attacks on their crypto wallets. Like how Ukrainian members of ransomware-as-a-service group Conti left that organization during the Russian-Ukrainian war and **eventually brought down the Russian cybercrime gang BlackCat**. The next year may see a marked increase in hacker-on-hacker attacks either for political or monetary reasons. These incidents highlight how the boundaries between predator and prey in the digital world are increasingly blurred.

04

Dynamic Identification is Next Defense Against Fraud



Normal 256 Bit Encryption is becoming obsolete, and AI-driven fraud is increasing in sophistication so quickly that **fraudsters will soon be able to create virtually undiscernible proof-of-life documents that will fool even the most discriminating eye or identification system.** To combat this evolving reality, nation-states and government agencies could move to dynamic identification that will replace static driver's licenses and social security cards with **dynamic PII that continually changes** like an online 3D barcode used for event tickets. As a result, even if an organization is hacked and its customers' or members' name and social security number are taken, consumers may be able to reset their numbers like passwords and use constantly rotating 3D barcodes on their mobile device for identification. Consider that many cybersecurity experts believe **every American's SSN has been leaked to the dark web at least once** and this approach may not be as far-fetched as one would think.

05

Power-Hungry Data Centers Become Favored Target

Global cyberattackers have had large data centers in their sights for years, but one clear attack vector has emerged with the exponential growth of consumer and business use of generative AI: power. According to Goldman Sachs, on average, a single ChatGPT query uses nearly 10 times more electricity to process than a standard Google search. The investment bank also reports that **data center power demand will grow 160% by 2030.** In related news, after meeting with executives from hyperscalers, AI companies, data center operators, and utility companies in early September, the White House announced a new task force to deal with the growing needs of building and maintaining the United States' AI infrastructure. **All these entities represent new attack surfaces that can be disrupted by bad actors.** Globally, the problem is exacerbated. Cloud infrastructure and data center technology and security vary wildly from country to country. **Within the next year, cyberattackers could successfully jeopardize a nation-state's cloud infrastructure through an attack on the power needed to run it.**

Experian® Data Breach Resolution by the numbers

Coverage
100+ Countries

2,808
Total breaches YTD through Q3 in 2024

77M
Breach notifications sent in 2024

8
Mega breaches in 2024

TOTAL BREACHES BY SECTOR:

- Healthcare 36%
- Public Sector 19%
- Financial Services 16%
- Retail 13%
- Education 10%
- Other 6%

TOP 5 COUNTRIES HIT HARDEST:

U.S.
U.K.
CANADA
AUSTRALIA
MEXICO

CONSUMERS IMPACTED:

24% Minors
76% Adults

41% of all 2024 breaches were supply chain breaches

Better outcomes, unmatched value

Count on Experian Data Breach resolution for the partnership, solutions and performance to create the best possible outcome. Gain control and confidence with the value that only Experian Partner Solutions can provide.

Contact Us

UNITED KINGDOM

08444-815-888

experian.co.uk/business/regulation-and-fraud/data-breaches/services

UNITED STATES

1-866-751-1323

experian.com/databreach

breachresponse@experian.com