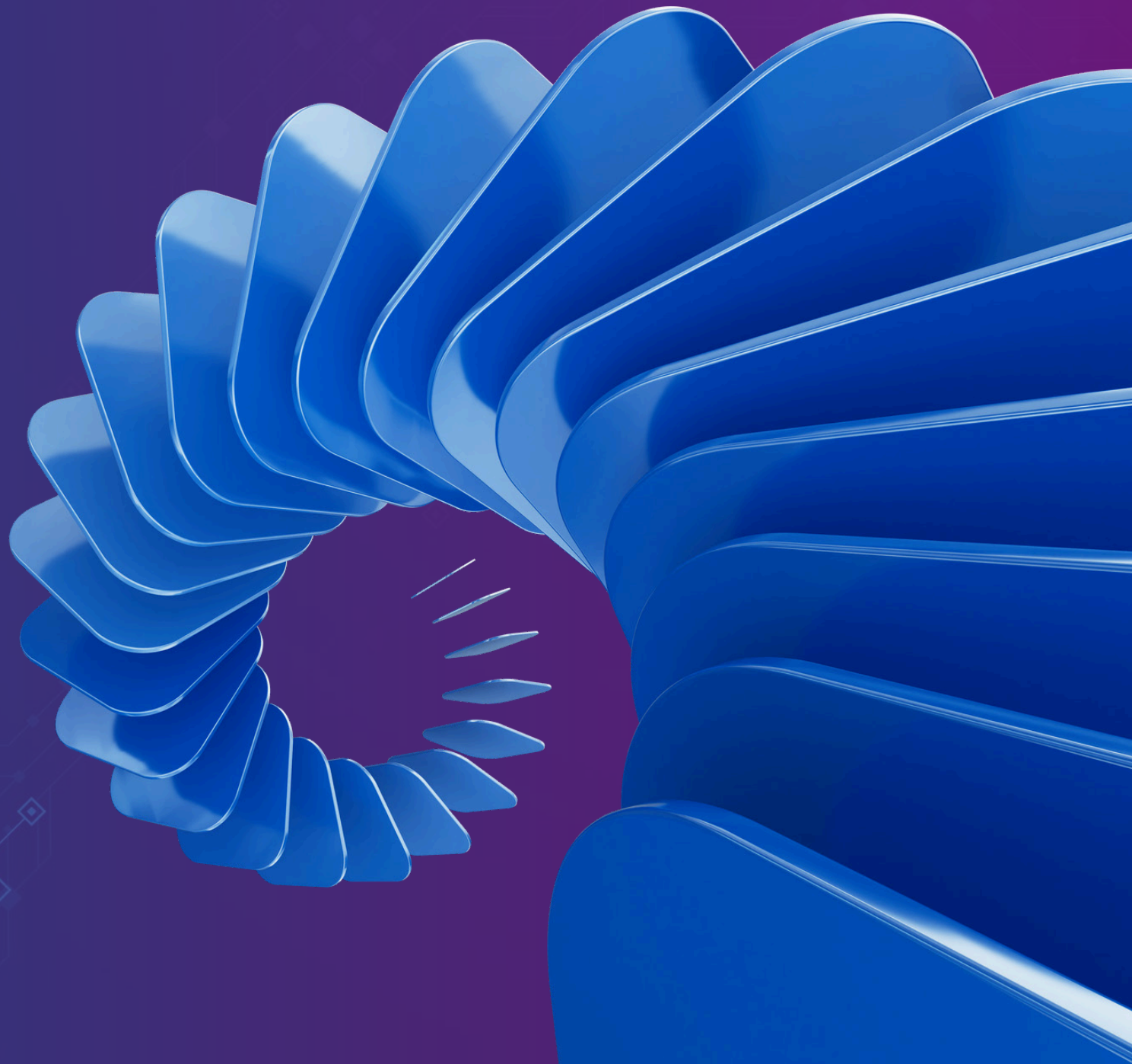
13TH EDITION

2026 Data Breach Industry Forecast



Executive Summary

There was no slowing down in 2025. The past year has seen a dramatic increase in the scope and frequency of global data breaches. Intelligence firm **Statista** reported nearly 94 million data records were leaked in data breaches during the second quarter of 2025 alone. The **2025 Verizon Data Breach Investigations Report** reported 12,195 data breaches last year, and these attacks came from 139 countries, truly demonstrating that cyberthreats know no national boundaries.

Experian has seen a continued rapid pace having supported more than 3,000 data breaches in 2025 alone. Our internal analytics show that more than 110 million consumers globally were impacted by a data breach from our client base in 2025, a 40% increase from last year.

Stateside, the costs of a data breach continue to rise. According to IBM's **2025 Cost of a Data Breach Report,** while the worldwide average cost associated with a breach shrank by a modest 9% ($4.88 million USD to $4.44 million), in the U.S., the average cost increased by 9% to $10.22 million USD, further distancing itself as the highest region globally.

Looking back at last year's predictions, a **recent report** from OPSWAT / Ponemon Institute indicates that 61% of all U.S. companies have suffered from insider data breaches in the past two years, supporting our "The Enemy Within: Internal Fraud Will Rise" prediction. It's not just large companies either. **Recent news** of an insider breach at Utah-based FinWise Bank is a perfect example.

Sadly, numerous news articles and even a recent **notice** from the FBI (Federal Bureau of Investigation) reinforce last year's "Smells Like Teen Secret" prediction about the increased number of youth getting into hacking. In 2025, **more than 26.5% of American teenagers had experienced cyberbullying** over the previous 30 days. Schools are another target, where **57% of breaches were carried out by children**.

We see 2026 as the year of AI not surprisingly. Now, new AI-driven threat vectors stand to increase the scope, frequency and cost of data breaches. The same IBM report indicates that 97% of surveyed participants reported an AI-related security incident in the last year and lacked proper AI access controls. Plus, 63% of them indicated that they lacked AI governance policies to manage AI or prevent the spread of shadow AI.

In our 13th annual Data Breach Industry Forecast, we focus on a number of AI-related predictions, such as the use of exfiltrated data to create pristine synthetic identities, AI overtaking human error as the leading cause of data breaches, and the emerging threat of AI combined with quantum computing for cyberattacks. Other interesting trends make this year's list, including the increasing use of mutating malicious code by hackers for long-game attacks, brain hacking, and the gender divide decreasing among criminal hackers. This year's predictions come from Experian's long history of helping companies navigate data breaches over the past 23 years. The following predictions represent what we see on the horizon in the world of data security incidents in 2026 and beyond.

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.

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 More Real Than Real, the Hacker's New Standard

If you thought that some of the recent mega-breaches were bad, there's something far worse that they could enable. Since January 2024, **five well-reported MOABs** (Mother of All Breaches) alone accounted for more than 60 billion comprised records and login credentials. That's more than eight times the population of the planet. And these mega-breaches touched many of the big worldwide players: Apple, Facebook, GitHub, Google, LinkedIn, Tencent QQ, WeChat, Weibo, and X, just to name a few.

Fans of the movie *Blade Runner* may remember the motto for the Tyrell Corporation's production of replicants: "More Human Than Human." In the movie, the synthetic beings were virtually indistinguishable from humans. Now, apply this standard to the hacking world.

With sophisticated AI, hackers could perform unprecedented data harvesting on these many billions of records and stitch together enriched identity profiles that are "more real than real." Imagine synthetic IDs with proof-of-life documents, voice, and video that appear so authentic, they will be indistinguishable from real people. Get ready for a potentially massive spike in identity theft. First- and third-party fraud may dramatically increase, due to enriched profiles giving hackers greater accessibility to credit applications. A **report** found that 76% of U.S. fraud and risk professionals believe their organizations are dealing with synthetic customers, with this form of fraud estimated to be growing at a rate of 17% annually. And phishing and vishing attacks work so quickly and seamlessly, even well-trained employees on security threats could be duped.

02

The Pendulum Swings to AI

In all the talk about AI replacing humans, there is one area where it could happen. Right now, human error accounts for approximately **68%** to **95%** of data breaches, depending on which industry research report you read. Common causes include social-engineering scams, phishing attacks, insider threats, and accidental misconfigurations. Make no mistake, bad actors will continue to exploit these methods to trick humans.

However, the rise of agent-based AI that can perform complex, multi-step operations may tip the scales. These AI agents carry out tasks and solve problems without frequent human intervention. Savvy hackers could exploit their target's AI-agent network by injecting their own AI agents to disrupt the orchestration or governance of the victim's AI agents. At a minimum, this disruption could impact an organization's operations or siphon money, goods, or information. Equally bad, a hacker's AI agents could perform ransomware-like actions on that network. In fact, a 2025 **IBM report** revealed that, on average, 16% of data breaches involved attackers leveraging AI—most commonly through AI-generated phishing schemes (37%) and deepfake impersonation tactics (35%).

Looking ahead to 2026, the convergence of sophisticated AI tools and motivated individuals, whether hackers or opportunistic actors, could become a major catalyst for a new wave of cyberattacks. AI agents are the next frontier for fraud and cybercrime, and we predict this may overtake human error as the leading cause of data breaches.

03

Girls Just Want to Have Fun (and Hack)

We're about to potentially see an explosion in the number of female criminal hackers, predicting the percentage may double in 2026. What's driving it? An increase of young females in STEM and coding. Well-known programs like Girls Who Code, Girls4Tech, and CyberPatriot already introduce girls to ethical hacking. All-female hacker organizations like FoundHer House are raising millions in venture capital funding, filing patents, and building products that reach mass consumers. Platforms like **HackerOne** and **Bugcrowd** have become global testing grounds where young female ethical hackers earn money for finding system vulnerabilities.

Industry data verifies the jump. Women now make up **24–25%** of the cybersecurity workforce, up from 11% in 2017. Research from Cybersecurity Ventures projects that women will make up 35% of the global workforce by 2031. Meanwhile, a **report** about cybercriminals and gender finds that at least 30% of users on cybercrime forums are women and we have already seen standout stars. In 2025 a female **Ukrainian hacker** known as "Ghost in the Shell" was revealed to have infiltrated the Securities and Exchange Commission and later became a whistleblower. Perhaps most significantly, a former Amazon engineer was found guilty for her role in the 2019 Capital One data breach.

Additionally, coding clubs, hackathons tailored for grade-school girls, and a sharp rise in the number of female mentors in tech will help build skills and contribute to possibly a dramatic increase in the number of females who become CISOs and ethical hackers as well.

The cybersecurity industry calls it polymorphic or metamorphic malware. For the layperson, it's mutating malicious code. It's a fast-rising, scary category of malware that's the code equivalent of a camouflaged leopard in a sun-streaked jungle, silently lying in wait, ready to pounce. Mutating malicious code morphs itself or data elements in real time to evade signature-based antivirus or other detection methods, then changes back to its original form or another to avoid detection.

The biggest danger with this chameleon code: it enables bad actors to play the long game, keeping the malware dormant until they're ready to strike. And activating this code can have serious consequences, such as taking someone off TSA's No Fly list to get through airport security, using visual deep fakes to evade law enforcement, engineering U.S. Census or voting results, or altering birth certificates and other proof-of-life documents in real time. We've already seen reports of threats in recent years including a **warning by BIO-ISAC** in 2021 that found this malware targeting the biotech industry.

The frightening combination of mutating malicious code being so difficult to detect and generative AI empowering its rapid spread may cause a sharp increase in injection attacks to access or fool secure networks, and that could result in a constant stream of large global data breaches.

04

Now You See It, Now You Don't

05

Brain-Hacking Still Distant, But Coming into Focus

It was 1999. The groundbreaking sci-fi film *The Matrix* introduced the world to the idea of a true brain-to-computer interface. Don't know how to fly a helicopter? No problem. Want to learn Jiu-Jitsu in less than five seconds? Easy. Just upload a program to a person's brain through a neural jack at the base of the skull.

It may not be *The Matrix*, but recent news about Elon Musk's Neuralink brain chip is a big-time first step. The chip connects to the neurons in the brain and translates electrical signals into commands to a digital device using brain-computer interfaces, or BCIs. And Neuralink has market competitors, such as Synchron or Precision Neuroscience, with their own brain-interface tech.

Right now, these early neural interfaces connect directly to the brain. But consumer BCIs worn like caps, glasses, or headphones are coming to market soon. They're perfect for a wide range of applications, like gaming, ecommerce, dating, and much more. Of course, this innovation may add a worldwide, virtually unpoliceable threat surface, as cybercriminals could use AI to develop "thought phishing" malware that detects and manipulates decision-making impulses. It'll literally be brain-hacking.

Remember when cybersecurity professionals spoke of quantum computing as an abstract concept that was a decade away? Well now, the technology is just around the corner, relatively speaking, and – when it advances from development to production mode – it stands to crack today's state-of-the-art 512-bit encryption in a matter of hours.

And that's not all. Combine generative AI with quantum computing, and you have a sobering data-breach threat that could overwhelm current, pre-quantum biometric authentication, breaking through traditional thumbprint, retinal scan, or voice print identifiers. **Industry research** indicates that currently nearly two-thirds of surveyed organizations see quantum computing as the biggest cybersecurity threat looming in the next 3-5 years. And sadly, the anticipated gains of quantum computing are already driving increased attacks. **Reports** indicate that hackers are actively collecting data with the intent to decrypt it in the future, anticipating advancements that may eventually allow them to break current encryption methods.

Fortunately, technology advancements in multi-layered AI security technology offer operational resilience for today's AI-driven attacks. Ultimately, fraud defense systems will employ quantum computing to fight quantum fraud. In the next year, we will see a quantum-computing arms race as providers of data-breach-prevention solutions accelerate development on quantum versions of their offerings to stay ahead of increasingly sophisticated and ultra-fast quantum fraud.

06

AI Meets Quantum Computing: A Dangerous Combination

Experian® Data Breach Resolution by the numbers

NUMBER OF COMPROMISES IN H1 2025 BY INDUSTRY:

- Financial Services 387
- Healthcare 283
- Professional Services 221
- Manufacturing 158
- Education 105

Source: Identity Theft Resource Center; 2025 H1 Data Breach Report

2,700
Total breaches YTD through Q3 in 2025

68M
Breach notifications sent in 2025

6
Mega breaches in 2025

Coverage
100+ Countries

TOP 5 COUNTRIES HIT HARDEST:


U.S.


U.K.


CANADA


AUSTRALIA


MEXICO

CONSUMERS IMPACTED:


22% Minors


78% Adults

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.

UNITED KINGDOM

08444-815-888

experian.co.uk/business/regulation-and-fraud/databreaches/services

UNITED STATES

1-866-751-1323

experian.com/databreach

breachresponse@experian.com