



CYBER CLAIMS THREATS INTENSIFYING AND GROWING IN NUMBER

Cyber Claims Update

2025

Contents

03

Introduction

04

The evolving cyber
threat landscape

06

Ransomware threats
expanding

08

BEC tactics
advancing

10

Social engineering
schemes becoming
more complex

12

Business interruption
costs growing

14

Privacy litigation risk
growing

20

Adapting to evolving
cyber threats

23

Contact us



Introduction

The already challenging and complex cyber risk landscape that businesses face has only become more difficult and multifaceted over the last year. Lockton's claims experience and data from industry sources both demonstrate the challenges for businesses. Threat actors are growing more sophisticated. Human error remains an immense pain point. Privacy statutes are becoming more stringent. And cyberattackers are capitalizing on the power of artificial intelligence.

The threats for businesses will not abate anytime soon, nor will cyber claims become easier and less costly to resolve. The mandate for businesses: Better understand your cyber risks, invest in cybersecurity, develop incident response and claims plans, and build effective insurance programs.

Explore our midyear 2025 cyber claims update for more insights on the biggest drivers of cyber claims activity today.



Deborah Hirschorn

Managing Director, U.S. Cyber &
Technology Claims Leader
Lockton



Meredith Ponce

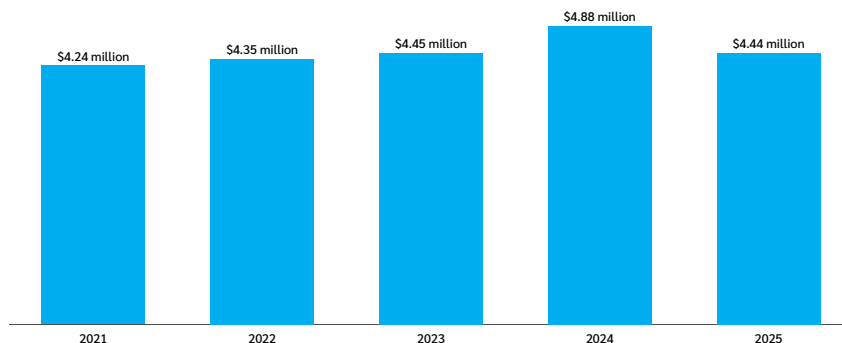
Senior Vice President,
Insurance & Claims Counsel
Lockton

The evolving cyber threat landscape

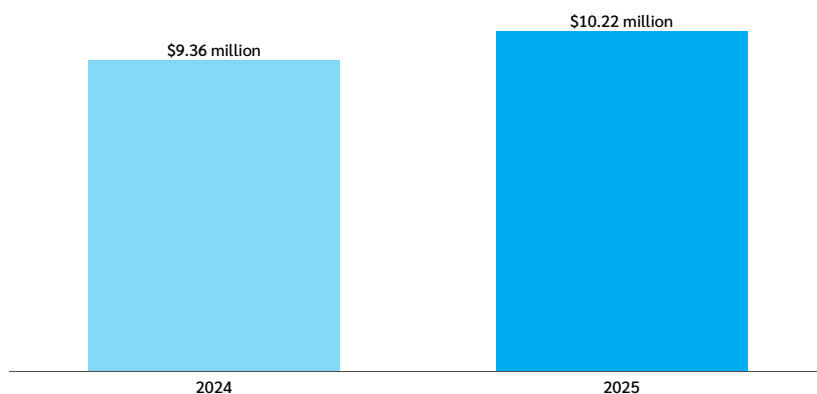
Nearly three-quarters of organizations are now using AI and automation to defend against breaches, saving an average of

\$1.9M
PER BREACH EVENT

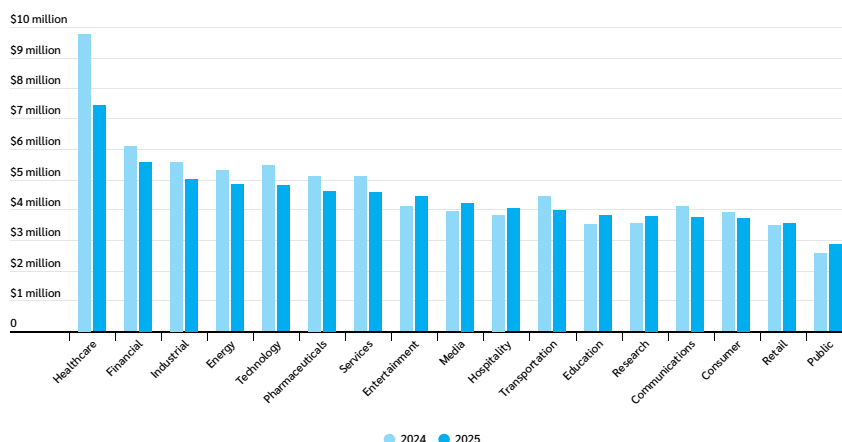
The average data breach event costs businesses more than \$4 million.



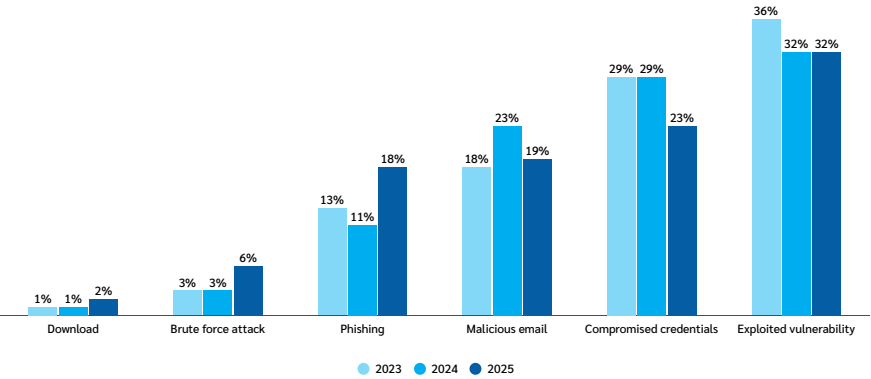
In the U.S., the average cost of a breach event is now more than \$10 million.



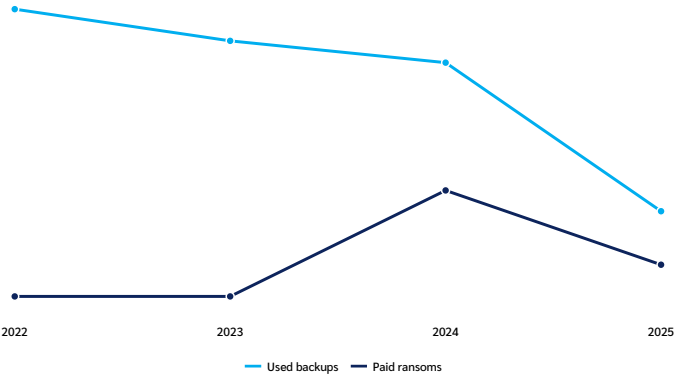
Data breach costs for healthcare continue to outpace other industries.



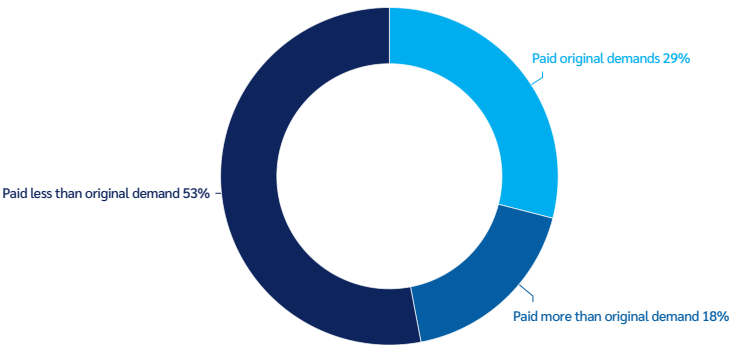
Exploited vulnerabilities remain the most common root cause of ransomware incidents.



Fewer companies are using backups to restore data after ransomware attacks, and roughly half are paying ransoms.



A majority of companies paying ransoms this year have been able to negotiate ransom amounts down from original demands.



Source: [IBM](#), [Sophos](#)



Ransomware threats expanding

Just as companies continually find ways to improve their defense against cyberattacks, those responsible for such attacks keep finding new techniques to use and weaknesses to exploit. Especially troubling: Cybercriminals are becoming faster and more efficient.

The average breakout time — how long it takes for an attacker to “move laterally from the initial foothold to high-value assets” — dropped from 62 minutes in 2023 to 48 minutes in 2024, an all-time low, according to CrowdStrike. In one particularly devastating case, an attacker broke out in just 51 seconds.

A number of cyber claims Lockton has helped to resolve in the last year highlight the wealth of opportunities presented by artificial intelligence (AI), which cyberattackers are using to carry out attacks and refine their methodologies. AI, for example, is increasingly

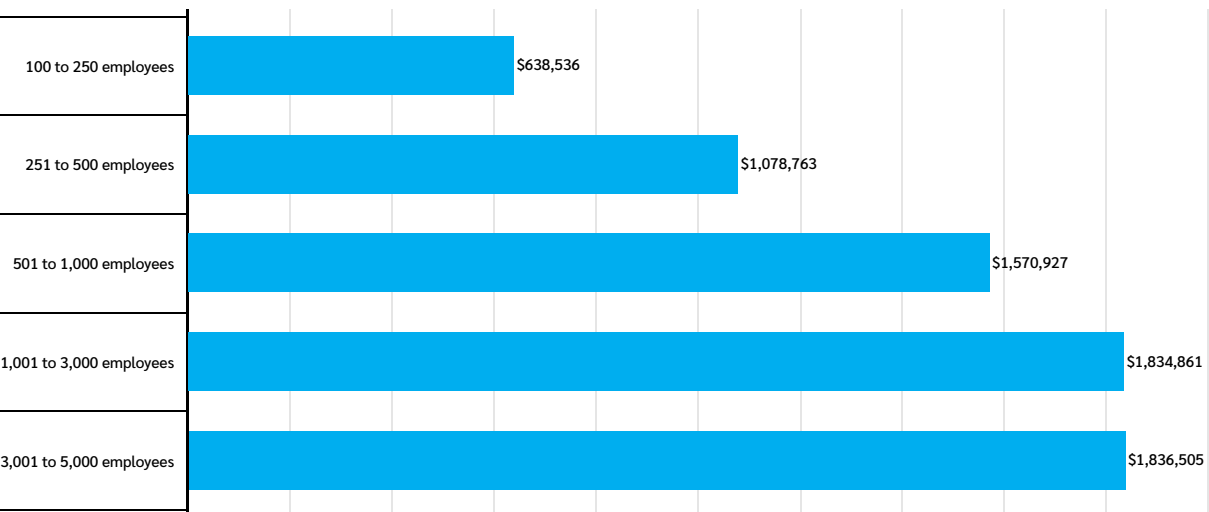
being used to prevent detection by analyzing corporate cybersecurity defenses and develop polymorphic malware that continuously adapts to defeat those defenses.

Attackers are also using AI to:

- Simulate behaviors of legitimate users, enabling greater control and access to data and assets.
- Comb the internet and social media to identify potentially lucrative targets.
- Analyze corporate websites and other content to create bespoke, personalized phishing emails.

These advanced techniques continue to fuel large ransomware payments. In 2025, the median ransomware payment is \$1 million, according to Sophos. Although this is half of the \$2 million average payment made in 2024, it’s still a sizable sum that can adversely affect many organizations’ bottom lines. Beyond ransom payments, ransomware recovery costs can also be sizable. (See Figure 1.)

Figure 1: Ransomware recovery costs can be sizable, even for smaller organizations.



Source: Sophos

BEYOND AI, ATTACKERS ARE EXPERIMENTING WITH OR GROWING MORE PROFICIENT IN USING SEVERAL OTHER TECHNIQUES. THESE INCLUDE:

Leak and shame sites.

In double extortion attacks, threat actors simultaneously encrypt data to hold for ransom and exfiltrate data they can expose on the dark web or sell to a third party. In recent years, attackers have increasingly operated dedicated websites through which they can publicly display exfiltrated personally identifiable information (PII), personal health information (PHI), and other sensitive information. The threat that sensitive data and information will appear on such sites provides attackers with more leverage against ransomware targets.

Triple extortion.

Triple extortion adds a third element beyond double extortion. Attackers could, for example, carry out a second attack on a target, such as a distributed denial-of-service attack or encrypting additional systems; attack a related organization; or blackmail individuals whose PII and PHI have been infiltrated.

Cloud computing and software as a service (SaaS) data theft.

As more companies employ cloud computing and SaaS, cybersecurity has become more complicated. Defense against attacks is the shared responsibility of both the cloud/SaaS providers and their customers. This can yield opportunities that savvy attackers can exploit.

In September 2023, for example, cybercrime group Scattered Spider gained access to MGM Resorts' network and cloud environments through an SaaS tool, after which the group deployed ransomware to encrypt the company's systems. The attack led to operations at dozens of resorts being disrupted for more than a week and the exposure of 37 million travelers' personal information. A class-action lawsuit by the victims of the breach was settled in March 2025 for \$45 million.

Decentralized ransomware as a service (RaaS) networks.

RaaS, which mimics SaaS models employed by legitimate businesses, has enabled virtually anyone to carry out ransomware attacks with relative ease, allowing individuals and groups to obtain ransomware code and malware from other hackers for a small fee. The decentralized nature of RaaS — countless individuals and affiliate groups, operating independently — makes it extremely challenging for businesses, cybersecurity consultants, and law enforcement to identify attackers and discern attack patterns.

Zero-day exploitation.

Ransomware group affiliates are increasingly taking advantage of software vulnerabilities that were previously unknown to developers and users. In mid-2023, for example, ransomware group CL0P exploited a zero-day vulnerability to steal data from 2,700 corporate users of a file transfer company, exposing the personal information of almost 100 million individuals.



BEC tactics advancing

Business email compromise (BEC) remains a potentially lucrative attack methodology for cybercriminals, who continue to refine their techniques.

In a typical BEC scam, an attacker sends an individual a message that appears to be from a known contact. This could be a coworker, a senior company leader, or an important vendor or supplier.

An attacker might send an email that uses a similar domain name — for example, ending in .co instead of .com. Attackers can also:

“Hijack” email accounts

through password theft or other means, giving them the ability to send truly authentic emails to scam targets.

Impersonate users

on internal messaging apps frequently used by companies, such as Slack and Teams.

Impersonate vendors

and executives in voicemails.



A message sent by an attacker will include what appears to be a legitimate request — for example, to make a payment to a vendor’s new bank account or a link to review a draft report written by a coworker. Scammers are counting on targets not reading emails and other messages in detail or verifying new details before making payments or clicking on links.

The result could be thousands or even millions of dollars unknowingly transferred to cybercriminals or malware being installed on corporate systems, through which attackers can gain access to PII, PHI, passwords, and more.

In July 2024, for example, a hacker obtained credentials to gain access to a Disney employee’s Slack account, and proceeded to steal 1.1 terabytes of corporate data. Meanwhile, in August 2024, chemical manufacturer Orion reported to the Securities and Exchange Commission that an employee was manipulated into wiring \$60 million to a third party in a BEC scheme.


As with ransomware, attackers are exploring new BEC tactics and delivery methods. In addition to looking to compromise supply chains such as in the example above, attackers are increasingly:

Impersonating vendors and executives using deepfakes.

Widely accessible AI tools can allow attackers to create hyper-realistic video and audio clips through which they can compel targets to make fraudulent payments or share sensitive information. In one such scheme reported by the Hong Kong police in February 2024, cybercriminals used a deepfake to pose as a multinational company’s CFO in a video conference call and induce a finance employee into making a \$25 million fraudulent payment.

Using QR codes in phishing attacks, also known as “quishing.”

Attackers are using seemingly authentic and safe QR codes to trick targets into downloading malware or visiting fraudulent websites, through which attackers can obtain PII, PHI, passwords, and other sensitive information.



Social engineering schemes becoming more complex

Cybercriminals and others have long used social engineering techniques to exploit human nature. These tactics are used to manipulate individuals into sharing sensitive and valuable information that can be lucrative for bad actors. Criminals are constantly changing methods of intrusion — and it appears their methods have again changed.

Lockton has observed that attackers are learning to personalize phishing attacks and produce more genuine-seeming content to better trick targets and entice them to take certain actions. Attackers, for example, are increasingly adding personal details to emails and other messages, which they can obtain via social media and other means.

AI is also helping attackers, who may not be native speakers of the languages their targets speak, draft messages with fewer grammatical and spelling errors. This has allowed groups to better target U.S.- and U.K.-based businesses.

In May 2025, for example, Scattered Spider launched social engineering schemes against several American and British retailers, including Harrods, Marks & Spencer, and Victoria's Secret. Using information obtained via the dark web to appear credible, attackers posed as company help desk staffers and tricked employees into providing additional credentials, which they used to infiltrate technology networks and plant ransomware. More recently, Scattered Spider has shifted to attacking insurers — including Aflac, Allianz, Erie Insurance, and Philadelphia Insurance Companies — and several airlines.



Attackers are also increasingly carrying out social engineering schemes through voice phishing, or “vishing.” A common scheme is for an attacker to call a company’s help desk posing as an employee to obtain passwords and other credentials. Attackers can also use AI tools, such as deepfakes and voice cloning, to simulate the voices of employees and supervisors, and use AI-powered chatbots to impersonate IT teams and others.

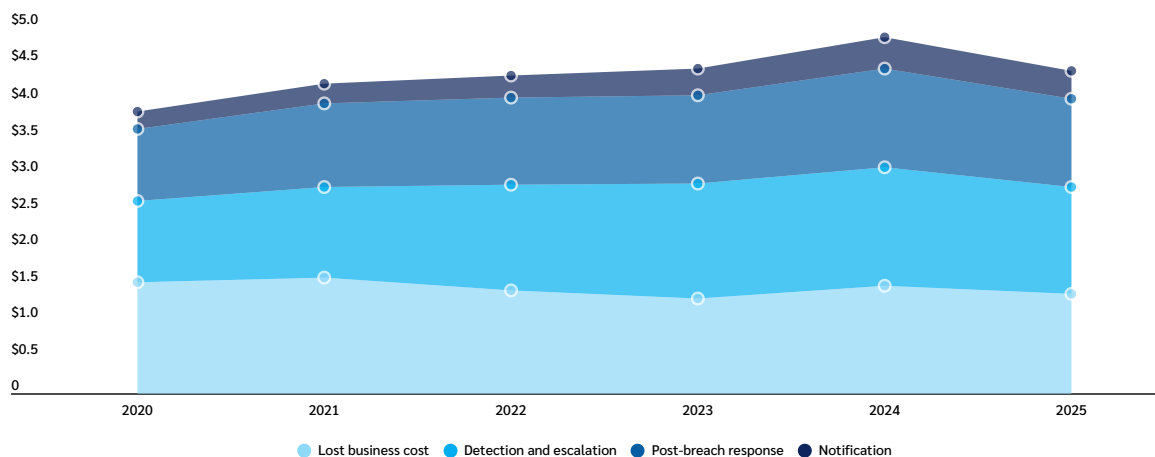
One reason why social engineering techniques are easier to carry out today than in the past is the rise of remote and hybrid work. Remote workers cannot verify suspicious requests as easily or quickly as their in-office colleagues can, making them potentially more susceptible to such schemes. More broadly, changes in how we work mean face-to-face interactions occur less frequently, which means there are fewer informal opportunities than in the past during which businesses can detect fraud.

Automation tools, meanwhile, are empowering cybercriminals to carry out large-scale attacks with greater ease. Threat actors can now create and deploy thousands of personal messages simultaneously, allowing them to test multiple vectors at once.

Business interruption costs growing

Business interruption costs stemming from ransomware attacks, data breaches, and other cyber events remain. In 2025, for example, costs from lost business and post-breach response following a data breach averaged \$4.44 million, according to IBM — 9% less than in 2024, but still a sizable number. (See Figure 2.)

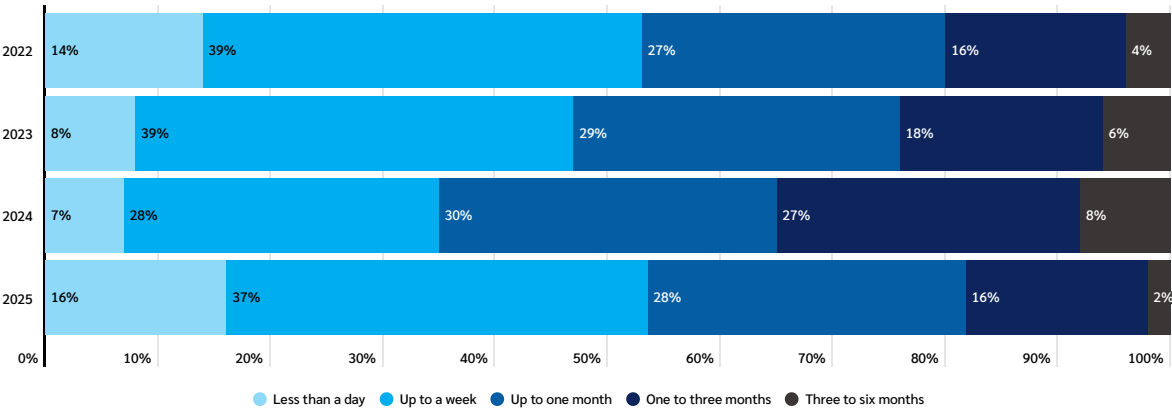
Figure 2: Lost business and post-breach response costs rose 11% in 2024.



Source: IBM
Figures in millions of dollars

Even as ransomware attackers increasingly pursue double and triple extortion schemes, business interruption accounts for 51% of all ransomware-related losses, according to Munich Re, and the mean cost to recover from a ransomware attack is \$1.53 million in 2025, according to Sophos. One bright spot for businesses in 2025: More companies have been able to recover in one week or less, according to Sophos. (See Figure 3.)

Figure 3: Recovery times following ransomware attacks have accelerated in 2025.



Source: Sophos

Recent events have demonstrated how vulnerable organizations are to disruptions involving third parties upon which they depend. “One of the most pressing cyber risks lies in the vulnerabilities of supply chains, which have been identified by criminals and state-sponsored actors alike as the ‘Achilles’ heel’ of economies and social infrastructure,” Munich Re said. “Digital bottlenecks will continue to pose major risks from software compromise, managed service provider compromise or single service disruption – to name just a few but very common supply chain risks.”

For guidance on how to take a proactive approach to cyber business interruption, explore Lockton and J.S. Held’s *Cyber Business Interruption Playbook*.

The July 2024 CrowdStrike outage, for example, was among the largest IT disruptions in history, knocking 8.5 million Windows devices offline, Microsoft said. In litigation filed against CrowdStrike in October, Delta Airlines said the outage prompted the cancellation of 7,000 flights, affecting more than 1 million passengers and resulting in a loss of more than \$500 million.

Similarly, the February 2024 ransomware attack against Change Healthcare, a leading payment processing vendor for healthcare providers, resulted in widespread outages across the industry, in addition to direct losses suffered by the company’s parent, UnitedHealth. And the June 2024 attack against auto retail technology provider CDK Global disrupted operations for some 15,000 dealers in the U.S. and Canada.



Privacy litigation risk growing

Privacy and data breach litigation remains a significant risk for businesses. In 2024, 2,529 data privacy lawsuits were filed across the U.S., a 77% increase from the number of suits filed in 2020, according to Thomson Reuters/Westlaw data analyzed by the International Association of Privacy Professionals. (See Figure 4.)

In 2024, plaintiffs continued to file suits following data breaches, relying on state statutes, such as the California Consumer Privacy Act (CCPA), and common law theories, including negligence, invasion of privacy, unjust enrichment, and breach of express or implied contract. Common law breach of contract claims often seek to leverage a company's own privacy notice, terms of service, advertisements or other public statements as contractual commitments or assurances that they will keep data secure.

With respect to negligence claims, some federal courts have recognized a duty to protect personal information where a defendant allegedly created a situation that they knew or should have known would pose a substantial risk to a plaintiff, such as intentional collection and storage of plaintiffs' information. Contract and negligence claims are more likely to survive dismissal at the pleading stage because of the factual issues that arise with the merits of these claims.

The most frequently contested issue in data breach litigation continues to be standing — whether the plaintiff has sufficiently alleged “actual or imminent” harm traceable to the defendant's conduct. In 2021, the Supreme Court held, in *TransUnion v. Ramirez*, that a risk of future harm stemming from disclosure of a data breach plaintiff's personal information does not, by itself, support standing to sue for damages. Instead, plaintiffs must identify an actual, concrete injury.



In 2024, courts continued to grapple with the types of concrete harm sufficient to confer standing. The 9th U.S. Circuit Court of Appeals held in *Greenstein v. Noblr* that a general notice to a plaintiff that their personal information may have been exposed, without confirmation that the plaintiff's information had been stolen, was not sufficient to establish a risk of future harm. The 9th Circuit left open the possibility that mitigation costs, such as identity theft monitoring services or time spent monitoring financial accounts for potential fraud, could constitute concrete injury in conjunction with an appropriately pled risk of future harm, such as confirmation that a plaintiff's personal information was, in fact, accessed during a data breach.

The past year also saw case law developments regarding whether forensic communications and analyses qualify for attorney-client privilege following a data breach. In *In re Samsung Customer Data Security Breach Litigation*, the U.S. District Court for the District of New Jersey acknowledged that attorney-client privilege must be assessed on a case-by-case basis and narrowly construed. The court established a list of factors to be used to evaluate whether attorney-client privilege should be found in the data breach litigation context:

- The type of services rendered by the third-party consulting firm to outside counsel.
- The purpose and scope of the investigation as evidenced by the investigative materials or the services contract between outside counsel and a third-party consulting firm.
- The existence of a two-track investigation commissioned by the impacted company.
- The extent of a preexisting relationship between the impacted company and the third-party consulting firm.
- The extent to which the third-party consulting firm's investigative materials were shared with members of the impacted company and/or any other outside entities, including the government.
- Whether the third-party consulting firm's investigative services assisted the law firm in providing legal advice to the impacted company.
- Corporate data breach victims should be aware of these factors as they engage in forensic investigations post-breach.

States stepping up

In 2025, the Trump administration has prioritized deregulation, including rolling back several privacy-related regulations established under the Biden administration. In May, for example, the Consumer Financial Protection Bureau announced it would not move forward with a Biden administration proposal to limit the sale of Americans' private information by data brokers. Several agencies, such as the Federal Trade Commission, are expected to focus more on enforcement of existing rules rather than additional rulemaking.

With the federal government generally taking a more hands-off approach, states are increasing enforcement. In January, new comprehensive privacy laws took effect in Delaware, Iowa, Nebraska, New Hampshire, and New Jersey. Similar laws will come into effect in Maryland, Minnesota, and Tennessee later this year.

Each of these new laws provides consumers with the right to access, delete, and opt out of sales. Each law, except Iowa's, also provides a right to opt in for sensitive data processing and a right to opt out of certain automated decision-making. Notably, none of the state laws taking effect in 2025 includes a private right of action.

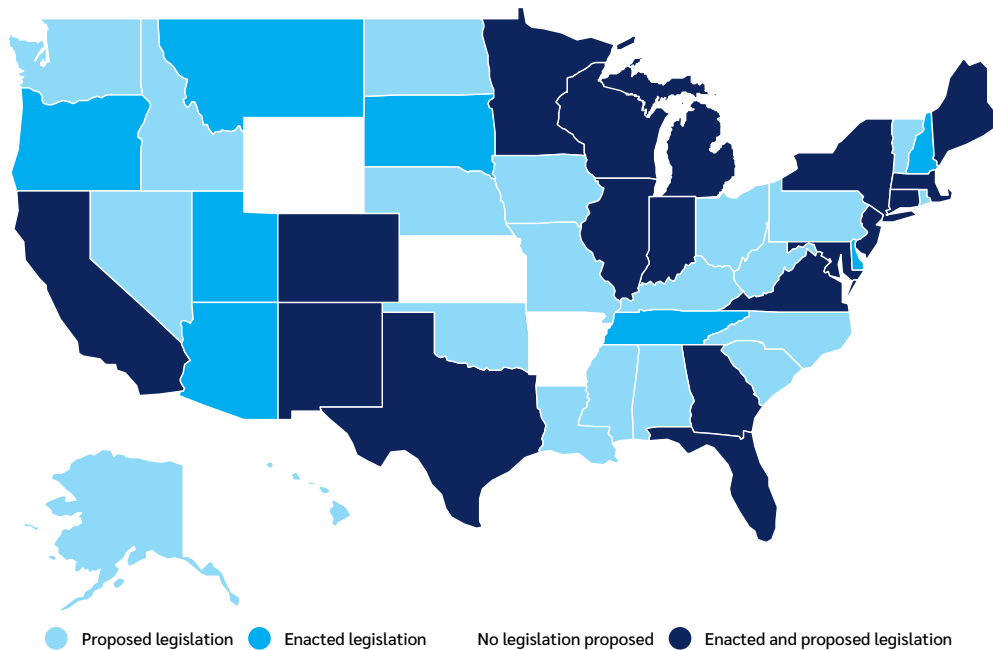
Several changes to existing state privacy laws are also taking place in 2025. Both the Colorado Privacy Act and the CCPA will include neural data as a type of sensitive personal data. The Colorado Privacy Act will expand biometric protections. Both Colorado and Virginia will also have new privacy protections for children's data.

On April 16, 2025, the California Privacy Protection Agency (CPPA) and attorneys general from seven states — California, Colorado, Connecticut, Delaware, Indiana, New Jersey, and Oregon — announced they were forming the Consortium of Privacy Regulators, a new effort to better protect consumers' privacy. The stated purpose of the consortium is to share expertise and resources and coordinate efforts to investigate potential violations of applicable laws.

Among the states, California is widely regarded as the leader in enforcement:

- In February 2024, the California attorney general fined DoorDash \$375,000 for alleged violations of the CCPA and California Online Privacy Protection Act (CalOPPA). The alleged violations included failure to comply with CCPA's opt-out requirements for business that sell personal information, and neglecting to disclose that it provided personal information to marketing co-ops.
- In May 2025, the CPPA fined a clothing retailer almost \$350,000 for alleged CCPA violations, including an improperly configured opt-out tool and requiring consumers to submit more information than necessary to process their privacy rights requests. Notably, when the CPPA announced the settlement, the agency pointed out that the company had "deferred to third-party privacy management tools without knowing their limitations or validating their operation." The head of the CPPA noted that companies should not rely solely on third-party privacy compliance tools, stating that "the buck stops with the businesses that use them,"

Figure 5: As of August 2025, 26 states had enacted AI legislation.



Source: Bryan Cave Leighton Paisner LLP

and that “using a consent management platform doesn’t get you off the hook for compliance.”

- In March 2025, the California attorney general announced an investigative sweep targeting the location data industry, specifically focusing on mobile apps, advertising networks, and data brokers. The sweep focuses on ensuring compliance with CCPA’s provisions regarding the handling of consumers’ geolocation data.

Although not part of the consortium, the Texas attorney general is also taking an active role in enforcement. In June 2024, the attorney general’s office announced an initiative focused on enforcing privacy laws in the state. Since then, the office has completed a significant settlement with a social media company relating to biometric data, launched investigations into the automotive industry for alleged surveillance and data sharing practices, issued notices to over 100 companies for failing to comply with the Texas data broker law, and

initiated a lawsuit and a large-scale probe into companies for suspected violations of the Securing Children Online through Parental Empowerment Act and the Texas Data Privacy and Security Act.

Even as the Trump administration takes a step back from privacy regulation, several bills under consideration by Congress warrant monitoring. These include proposals to update decades-old laws, such as the 1974 Privacy Act and the 1986 Electronic Communications Privacy Act.

One potential point of contention between the federal government and the states is regulation on AI. As of early August 2025, 23 states had passed specific AI legislation, and several others are considering proposed bills, according to law firm Bryan Cave Leighton Paisner LLP. (See Figure 5.) Congress considered including a 10-year moratorium on state and local AI laws in the recently passed budget and spending bill, but it was ultimately removed from the final bill.

Plaintiffs leveraging old laws

Lawsuits against consumer-facing businesses related to their use of digital tracking technologies, such as pixels and session replay tools, increased in 2024. Tracking technologies enable businesses to collect data about user interactions to refine marketing strategies and improve engagement. Plaintiffs now allege that these tracking technologies “record” or “intercept” user interactions without appropriate consent, in violation of state and federal laws originally intended to address wiretapping, pen registers, and trap-and-trace devices.

Filing suit under the federal Video Privacy Protection Act (VPPA) has proven particularly lucrative for plaintiffs’ attorneys. The VPPA, which Congress passed in 1988 in response to concerns about the privacy of consumers’ video rental history, provides for statutory damages of \$2,500 per violation. Plaintiffs have brought a surge of class-action suits against website owners with video functionality on their websites, contending that tracking pixels embedded on websites constitute an unlawful disclosure of video viewing history.

Complicating matters for businesses is a developing circuit split involving cases alleging VPPA violations. In April, the U.S. Court of Appeals for the Sixth Circuit, in *Salazar v. Paramount Global*, affirmed a lower court’s dismissal of a plaintiff’s case, narrowly interpreting the VPPA as only protecting individuals who subscribe to or purchase audio-visual materials, rather than those who consume digital content, such as newsletters. The court also held that individuals must show a direct relationship with audio-visual content (for example, subscribing to a video service) to qualify as a “consumer” and thus have standing to file suit under the VPPA.

This follows an October decision by the U.S. Court of Appeals for the Second Circuit — in *Salazar v. NBA*, involving the same plaintiff — to reverse a lower court

ruling, holding that the VPPA protects consumers regardless of the specific goods or services they subscribe to, as long as video content is involved. The Second Circuit held that subscribing to a newsletter that includes video links may qualify someone as a VPPA “consumer.”

These contrasting rulings could lead to forum shopping by plaintiffs and inconsistent outcomes depending on jurisdiction. This also sets up the potential for Supreme Court intervention to resolve the discrepancy and/or action by Congress to clarify the VPPA’s scope in the context of modern technologies.

Beyond the VPPA, plaintiffs have filed hundreds of lawsuits alleging violations of the California Invasion of Privacy Act (CIPA), a 1967 wiretapping statute providing statutory damages of \$5,000 per violation. Decades after its inception, plaintiffs are using CIPA as the basis for class actions against businesses alleging violations based on their use of website tracking tools, chatbots, and session replay software. Plaintiffs allege that tracking technologies are akin to wiretapping, allowing third parties to “eavesdrop” on users’ online activities without obtaining proper consent.

Plaintiffs have also alleged that web beacons and pixels violate the pen register provisions of CIPA by collecting data from users such as IP addresses and potential geolocation data, and such data can be used to “fingerprint” them. These allegations have had mixed success.

Other state laws that plaintiffs have used to file tracking technology claims include the Massachusetts Wiretap Act and Arizona’s Telephone, Utility and Communications Service Records Act. Inconsistent judicial rulings across the country continue to encourage plaintiffs’ attorneys to test novel legal theories regarding tracking technologies.

Global privacy regulations intensifying

International privacy laws have seen significant development since the start of 2024, reflecting a global emphasis on data protection and regulatory enforcement.

The European Union continues to set a high bar for privacy governance. In May 2025, Ireland's Data Protection Commission fined TikTok 530 million euros for inadequately protecting EU users' personal data, particularly concerning remote access by staff in China.

The rapid evolution of AI has also led the EU to establish the AI Act, which introduces a risk-based framework for AI systems, categorizing them into unacceptable, high, limited, and minimal risk levels. The act, which took effect in August 2024, subjects high-risk AI systems, such as those used in critical infrastructure and employment, to strict requirements, including data transparency, human oversight, and data governance.

The EU's stringent data protection standards have influenced global privacy practices, prompting companies to adopt GDPR-aligned measures to maintain access to the EU market. There is a growing trend toward harmonizing privacy regulations internationally aiming to facilitate data flows while safeguarding individual rights.

Australia. Meanwhile, has long been perceived as the second-most litigious country in the world, after the U.S. Class-action litigation against businesses contributed to the more difficult director and officers liability insurance market of the early 2020s, and could now drive

an uptick in cyber privacy claims. In late 2024, the Australian government passed updates to the Privacy Act 1988, which gave Australians — effective June 10, 2025 — the right to file litigation against businesses alleging serious invasions of privacy, such as the misuse of personal data.

This could lead to more litigation against businesses at the same time they face greater enforcement activity by federal regulators. The Office of the Australian Information Commissioner is more aggressively pursuing action against companies for privacy violations, including those connected to their use of AI and other emerging technologies.

Elsewhere in Asia-Pacific, new data protection laws and regulations are taking effect in China, India, Indonesia, Saudi Arabia, and Vietnam. Regulations in the region are also evolving, covering more than personal data, which makes compliance more difficult for global organizations.

Closer to home, Mexico's Law on the Protection of Personal Data Held by Private Parties (LFPDPPP) came into effect on March 21. The LFPDPPP replaces the previous 2010 federal data protection law and introduces several important changes, including broader definitions of personal data, databases, and data controllers; stricter privacy notice requirements; and enhanced individual rights over automated processing. The LFPDPPP also creates a new Secretariat of Anti-Corruption and Good Governance (SABG), which will oversee compliance with the law, conduct investigations, and impose sanctions.



Adapting to evolving cyber threats

As cyber threats grow more complex, organizations must be prepared for resultant claims that are more frequent, severe, and difficult to resolve. Here are seven ways organizations can mitigate potential losses and facilitate better claims outcomes.

01 Seek to better understand your cyber risks, including those arising out of your supply chain.

As cyber claims can take many forms and arise from several areas, it's important that businesses understand the nature of the risks they face. This includes modeling potential losses to better measure how likely they are to occur and how much they could cost businesses.

Given that vendor relationships can contribute to a variety of cyber risks, businesses should look to map their technology networks to document which vendors provide or facilitate critical processes and which vendors access or store specific data, including PII and PHI. Organizations should also try to identify which technology providers their own providers rely on, which can help to pinpoint potential dependencies and vulnerabilities.

Similarly, companies should review:

- Their use of tracking technologies — including cookies and pixels — that plaintiffs' attorneys are focusing on, and consider whether the use of such technologies outweighs their potential risk.
- Policies governing what data organizations and their partners collect and how such data is used, shared, stored, and protected.
- Contracts with key vendors to ensure their language reflects how they want risk to be managed, including via minimum insurance limits.

02 Develop and test an incident response plan.

Even with strong controls, no organization can become an impenetrable fortress. It's therefore vital that companies are prepared for potential cyber events.

Most incident response plans include three major components, which follow the sequence of how an organization will react to events. These include:

- Detection, which includes the monitoring of systems, suppliers, and environments to detect events.
- Analysis of events for their operational impact and escalation according to established criteria.
- Response activities to be executed to minimize operational impact and fully restore operations.

Organizations should identify key resources they will need to access in the event of a loss and seek to have key vendors in place before an event. This includes forensic accounting services critical to business interruption losses, ransomware consultants, and outside counsel specializing in various types of cyber losses.

As basic, generic, and/or outdated plans will not be useful during a crisis, it's important that organizations' written plans be printed, disseminated, and stored in multiple locations so they are easily accessible during an incident. Plans should also be tested and updated at least once a year, in conjunction with other elements of an organization's broader business continuity plans.

03 Maintain cyber hygiene and invest in strong cybersecurity infrastructure.

Robust cybersecurity controls and a culture focused on protecting data and systems from outside attacks represent the most effective ways for businesses to mitigate potential claims. Underwriters also now view these as minimum conditions that policyholders must meet to secure cyber insurance coverage.

Hallmarks of strong cyber hygiene include:

- Multifactor authentication (MFA), which requires users to provide two or more pieces of evidence of their identity before gaining access to corporate systems.
- Endpoint detection and response, through which user phones, laptops, and other devices are continually monitored to prevent potential intrusions.
- Regular data backups on secure offline or offsite platforms.
- Segmentation of information technology and operational technology networks to protect critical systems.

- Email filtering software to scan for malicious links or attachments.
- Privileged access and password management software.
- Timely patching of critical software and systems.
- Regular training of all employees — including C-suite executives — on key topics, including phishing, social engineering, secure use of mobile devices, videoconferencing, and more.

Managed detection and response tools (MDR) are also crucial, enabling organizations to minimize — if not eliminate — threats from entering their systems. A critical component of this is a security operations center, staffed 24 hours a day, 7 days a week, tasked with engaging and containing abnormal activity before it becomes a larger issue.

04 Optimize insurance coverage.

Even the best-prepared organizations can suffer cyber losses, which is why effective insurance coverage is essential. A well-crafted cyber insurance policy can include

First-party coverage that reimburses insured organizations for the cost of investigating a cyber event and restoring normal operations. These include costs related to incident response, defense, forensics, business interruption, and more.

Third-party coverage for liabilities to others, including damages owed to third parties, regulatory penalties, and additional costs and expenses, including legal defense costs. In some cases, policies will provide access to

specific “panel” counsel to defend policyholders from liability claims, along with vendors that can assist in incident response.

Before a cyber event occurs, organizations should work with their insurance brokers to understand what is and is not covered under their cyber insurance policies. If any gaps in existing coverage are identified, policyholders should work with brokers to seek to fill those gaps during upcoming renewal discussions. The expansion and evolution of BEC and social engineering threats also underscores the need for effective crime insurance, the procurement of which should be coordinated with the purchase of cyber insurance.

05 Prioritize data privacy and governance.

Beyond a robust cybersecurity framework, more rigorous data privacy laws in the U.S. and elsewhere require businesses to develop and maintain specific policies to protect critical data. Among other actions, organizations should:

- Develop and document guidelines for how data should be collected, stored, processed, and shared.
- Implement strategies to minimize each of these actions and ensure transparency.
- Ensure access to sensitive data is strictly limited.
- Include data privacy best practices in cybersecurity training programs.

Data-related policies and procedures should be regularly reviewed and updated to address potential gaps in cybersecurity and ensure compliance with all applicable laws.

06 Leverage threat intelligence and collaboration.

Collaborating with other cybersecurity stakeholders, including law enforcement, can enable swift and strong action against cybercriminals, which benefits all businesses. For example, the Department of Treasury's Office of Foreign Assets Control (OFAC) encourages businesses and other organizations to report and share information about ransomware attacks, which the FBI and other U.S. law enforcement entities can share with Interpol and other counterparts around the world.

Such collaboration can often enable authorities to take out attack groups and obtain ransomware decryption keys, ultimately allowing for speedier returns to normal operations and lower costs for businesses. In 2024, for example, information businesses shared about ransomware attacks helped to fuel Operation Endgame, a massive law enforcement initiative carried out by the FBI and law enforcement authorities across Europe. According to the FBI, Operation Endgame "took down or disrupted more than 100 servers to defeat multiple malware variants."

07 Develop a plan for submitting your claim.

Before a potential cyber loss, organizations should be ready to file potential claims and have key resources lined up to expedite essential processes. In the event of a claim, businesses should be prepared to:

- Notify brokers and insurers as soon as possible.
- Obtain prior consent from insurers for the use of any vendors and keep both brokers and carriers updated on any and all actions taken to mitigate losses and prepare claims.
- Identify key advisors to assist in claims preparation, loss mitigation, and legal defense, including forensic accountants, ransomware specialists, communications specialists, and outside counsel, which may be part of panels preselected by insurers.

Contact us

Click the button or scan the QR code at right to find out more around how Lockton can support your organization's cyber risk management.

[Visit our website](#)





UNCOMMONLY INDEPENDENT