CYBER THREAT REPORT: 2026

# Cybersecurity in the wake of a new wave of risks

LOCKTON®

As 2026 unfolds, the business world faces evolving technologies, new international conflicts, and growing uncertainty about the economic and regulatory landscape. Cybersecurity threats swim under the currents of all these risks. Maintaining secure network and software environments means staying on top of unpredictable, emerging threats.

In April, the artificial intelligence (AI) firm Anthropic seemed ready to release Mythos, its latest model that marked a significant improvement over existing AI applications.

But then Anthropic withheld the new model from the public, arguing Mythos' capabilities posed too great a danger to cybersecurity if it fell into the wrong hands. Instead, it gave select technology businesses a sneak preview of Mythos to get a head start at patching undiscovered network and software vulnerabilities that the model identified.

For the rest of the business world, the Mythos story sounded alarm bells. AI has already accelerated cybersecurity threats over the last year, refining and sharpening threat actors skills and methods. If a new model could quickly identify network and software weaknesses, some that had existed for years but went undetected until Mythos came along, then businesses faced new and alarming cybersecurity threats.

What loopholes could the next advanced AI model find that Mythos failed to identify? What vulnerabilities could unauthorized users who have already gained access to Mythos exploit? What if a less responsible developer released an even more powerful model without advanced cybersecurity screening?

Insurers also recognize these new AI-born risks and are beginning to analyze how policies and programs can address them. From that analysis will come new requirements that insureds must meet to mitigate risks and obtain coverage.

AI is not the sole emerging cybersecurity threat. Wrongful data collection claims, particularly those stemming from pixel tracking and other advertising technologies, have posed significant financial risks. Geopolitical tensions give rise to hackers who target government institutions, critical infrastructure, and sometimes businesses — not primarily for money, but to disrupt the enterprise.

*Lockton's 2026 Cyber Threat Report* explores new vectors of global cybersecurity threats, how carriers contemplate these risks when underwriting cyber policies and other lines, how regulations have evolved, and how policyholders can better prepare for a rapidly changing cyber risk landscape.

# Contents


**04**
What has changed in the cyber claims landscape

**08**
How cyber losses occur

**16**
Insurance coverage for cyber risks

**18**
Global regulations & considerations in cybersecurity

**24**
Reducing cyber claims severity


# Contributors


**Oliver Brew**
Head of Global Centre of Excellence, Lockton Re*

**Kegan Chan**
Senior Vice President, Risk Solutions, Greater China

**Fahed Fawal**
Privacy & Cyber Risk Advisor, Middle East/North Africa

**Michelle Faylo**
U.S. Cyber & Technology Practice Leader

**Brendan Fitzpatrick**
Privacy & Cyber Risk Consultant

**James Harris**
Claims Advocate, London Cyber & Technology Team

**Deborah Hirschorn**
Managing Director, U.S. Cyber & Technology Claims Leader

**Chuck Jainchill**
U.S. Cyber & Technology Product Leader

**Zainab Khatib**
Cyber & Technology Practice Leader, Middle East/North Africa

**Susan Leung**
Director of Business Operations, Cyber & Technology

**Brian Lewis**
Cyber Broking Leader, Lockton Re*

**Mark Luckin**
National Manager, Cyber Technology Sector, Australia

**Carlo Ramadoro**
Head of U.K. Cyber & Technology

**Mauricio dos Santos Bandeira**
Director of Financial Lines & Liability, Brazil

**James Tasnadi**
Head of Cyber & Technology, Continental Europe

**Zach Flom**
Associate Director, Threat Intelligence
Arete

**Pamela Hans**
Managing Shareholder, Philadelphia
Anderson Kill

**Lynn Peachey**
Regional Vice President, Northeast Insurance Channel
Arete

**Alfred J. Saikali**
Chair, Privacy & Cybersecurity Practice
Shook, Hardy & Bacon

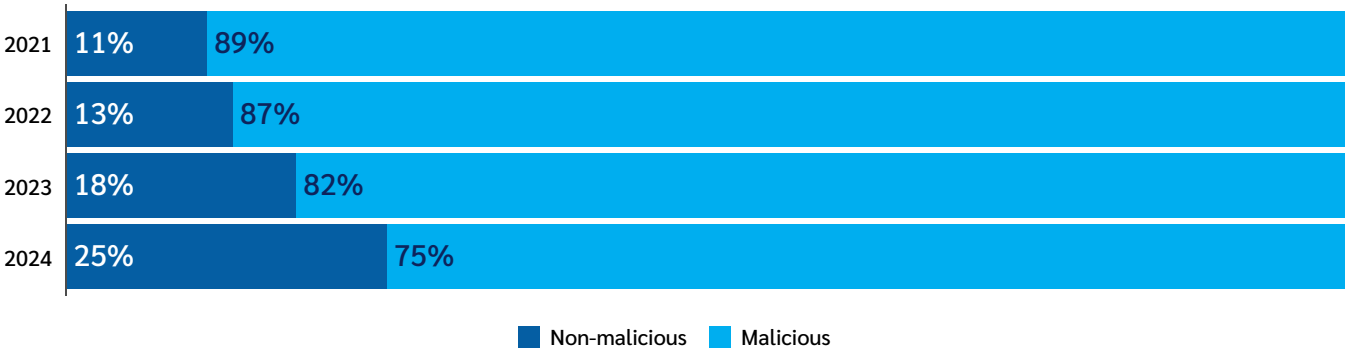
# What has changed in the cyber claims landscape

## Cyber risk is no longer just an external problem

Cybersecurity threats evoke the image of teams of ruthless and sophisticated hackers trying to break into a company's servers. That possibility remains a viable and significant threat to companies. But a growing risk to companies comes from the decisions and mistakes they make internally.

Munich Re's claims data showed that 25% of cyber incidents in 2024 were non-malicious, up from 18% the year before and 11% in 2021.

NON-MALICIOUS CYBER INCIDENTS ARE ON THE RISE.




Source: Munich Re

**Companies often incorrectly assume that traditional cyber policies cover these claims.**

For example, pixel tracking — a technology that collects behavioral and sometimes sensitive data from website visitors — can lead to accusations of wrongful data collection. As wrongful collection lawsuits have soared, particularly in 2025, carriers have pulled back on coverage for pixel tracking losses. Companies can find coverage, but insurers have grown cautious about their exposures to these claims. Cyber insurers view pixel tracking risks as the result of decisions companies make rather than as accidents or threats to businesses.

Similarly, copyright infringement — an escalating risk thanks to social media, influencers, and AI — amounts to a governance-driven loss. A policyholder accused of misappropriating another's protected work may be an accident or because of carelessness, but it was a decision made by someone nonetheless. Cyber policies in the U.S. often provide varying levels of coverage for these media-related losses. Coverage has historically been less common in international markets, but carriers have been increasingly willing to include it.

Even where external attacks occur, human decision-making is at the core of some of cybersecurity's biggest losses. An example of this is social engineering fraud (SEF). A threat actor could impersonate a corporate executive to convince an employee to transfer funds improperly. Though the employee is tricked, they still make the decision to transfer funds, which complicates coverage triggers and recovery.

## AI as a force multiplier

In 2004, the U.S. Federal Trade Commission (FTC) issued advisories and testified before Congress to warn about mysterious emails where the sender purported to be the prince of a Nigerian royal family and promised the recipient fortunes if they first sent the sender their bank account information.

Today, these types of scam emails are the butt of help desk jokes and a callback to a comparatively primitive era of cyber threats. Information technology desks used to warn company staff against clicking on links in emails that featured elementary misuse of grammar, diction, and syntax.

With AI, however, threat actors can craft phishing emails that lead to system compromises with polished English and convincing graphics that can fool even the most cautious employees.

Hackers can use AI in several ways beyond phishing emails. They can use increasingly sophisticated technology to exfiltrate data, examine it quickly to identify sensitive records, and use it for ransom or extortion or to carry out more menacing threats. Attackers can use AI to evade security controls like antivirus software and endpoint detection and response, and ransomware threat actors can use large language models (LLMs) to conduct successful payment negotiations and apply pressure to their targets.

Moreover, AI helps criminals execute cyberattacks on an industrial scale.

### AI's influence in cyberattacks manifested itself globally in 2025

**89%**

Increase in attacks from adversaries using AI.

**70%**

An average breakout time of 29 minutes — a 70% reduction since 2021 — with the fastest breakout time of 27 seconds.

**+24**

New adversaries identified and tracked by CrowdStrike, bringing the total to 281.

Source: CrowdStrike

**For businesses, AI-enhanced cybersecurity threats can lead to increased litigation risks, reputational harm, and significant losses.**

- Regulators have been slow to establish AI guardrails.
- Fierce competition among developers means there are few incentives to rein in troubling aspects of their ever-advancing models.

## Ways AI is increasing cyber threats

01

### RANSOMWARE

Whereas ransomware gangs once required considerable technical skill and tactical know-how to breach systems, purloin data, and issue ransom demands, AI allows modestly sophisticated attackers to deploy effective attacks. LLMs can craft evasive malware.

02

### PRIVACY, DATA, & ERRORS & OMISSIONS RISKS

AI increases the risk of inadvertent data and privacy disclosures. Some AI applications and LLMs are free or cheaply available for anyone to use. An employee who uses one of these applications and inadvertently uploads sensitive company data poses a significant non-data-breach privacy risk.

03

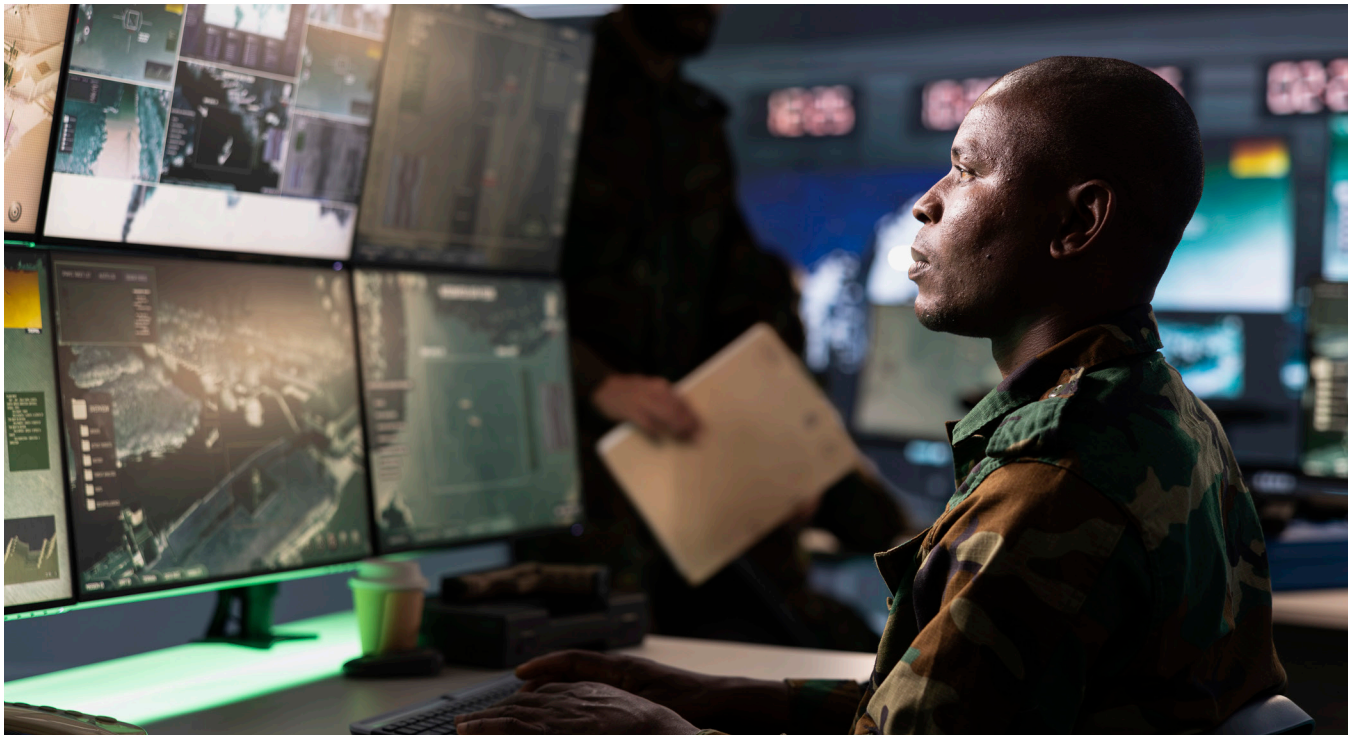
### BUSINESS EMAIL COMPROMISE (BEC) & FUNDS TRANSFER FRAUD

AI can conduct research to help attackers craft emails or voicemails that mimic a specific person's writing or voice, leading to convincing impersonations. These impersonations can instruct others within an organization to transfer funds to a criminal's account. Deepfake videos can achieve the same level of deception.

04

### MEDIA & INTELLECTUAL PROPERTY RISKS

Beyond malicious attacks, AI adds to existing intellectual property infringement and defamation risks. AI developers train LLMs on human-generated writing, videos, sounds, and imagery. Using these tools to produce content can result in unauthorized reproduction of copyrighted works, images, and likenesses, giving rise to intellectual property claims. AI models also hallucinate or turn up incorrect information, which can defame people or businesses if published without verification.



## Geopolitical tensions heightening cybersecurity risks

Geopolitical friction, strained alliances, and full-blown conflicts have destabilized the international community in recent years. International discord has led ideologically motivated hacktivists to open new frontiers in global conflicts by infiltrating corporate systems and disrupting operations, less for financial gain and more to make a point.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) warned this spring that Iran-affiliated actors targeted internet-connected operational technology devices in U.S. government critical infrastructure facilities, including energy and water facilities. CISA's advisory indicated that the threat actors targeted widely used industrial automation products developed by the Rockwell Automation brand Allen-Bradley.

Several data-wiping attacks, in which hackers erase company data to disrupt operations, have occurred alongside the U.S.-Iran conflict. A U.S. healthcare company in March had data wiped from tens of thousands of company devices. An Iran-affiliated group claimed responsibility, but the provenance of the attack has not been confirmed.

A 2025 incident illustrated the perils of ideologically driven cyberattacks. Russia-affiliated hackers took advantage of weak passwords to gain control of water valves at a Norwegian dam and increase water flow by 500 liters per second. This lasted for four hours but was brought under control before the attack posed a public safety threat.

Organizations responding to the World Economic Forum's Global Cybersecurity Outlook 2026 survey identified geopolitically motivated cyberattacks as the top factor they consider in their overall cyber risk mitigation strategies. The same report noted that 31% of respondents lack confidence in their home country's ability to respond effectively to major cyber incidents, up from 26% in 2025.

# How cyber losses occur

Cyber risk is often framed as a fight against external attackers, but most severe losses arise from a broader mix of technological dependence, human decision-making, governance failures, and vendor relationships. While ransomware remains a major liability driver, operational disruptions, social engineering fraud, privacy litigation, and even website and advertising technology are now among the most significant sources of cyber-related loss.

**Understanding how cyber losses occur, how they are litigated or remediated, and how insurers underwrite these risks can help organizations better prepare for incidents — and set realistic expectations about insurance recovery.**

01

## Operational disruption & business interruption

Some of the costliest cyber events do not hinge on ransom payments, but rather on operational shutdowns and downstream disruption. A striking example occurred in 2024, when hackers targeting Change Healthcare, a U.S. healthcare technology provider, exploited its lack of multifactor authentication on a remote-access application. After nine days inside the company's systems, attackers exfiltrated sensitive data.

Once Change Healthcare identified the intrusion, it disconnected data centers and suspended network operations. The resulting outage cost the company an estimated $867 million in business interruption losses alone, far eclipsing the $22 million ransom payment. Even then, some sensitive data was still disclosed.

The incident illustrates a key reality of modern cyber risk: Business interruption — lost revenue, additional expenses, and cascading operational impacts — often accounts for the largest share of loss.

## Why business interruption is so difficult to manage

Operational disruption following a cyber event is both common and prolonged. An IBM-Ponemon Institute study found that 86% of organizations experiencing a data breach reported operational disruption, and 76% said recovery took more than 100 days.

Dependency risk magnifies this exposure. Many organizations rely on a narrow set of vendors, platforms, or managed service providers to perform critical business functions. When a technology provider experiences an outage or breach, the effects can ripple through entire industries. During the Change Healthcare incident, pharmacies were unable to process insurance claims and healthcare providers were forced to take out loans to meet payroll, making it one of the most consequential cyberattacks on the U.S. healthcare system.

The World Economic Forum's Global Cybersecurity Outlook 2026 identified third-party and supply chain vulnerabilities as the top challenge to cyber resilience.

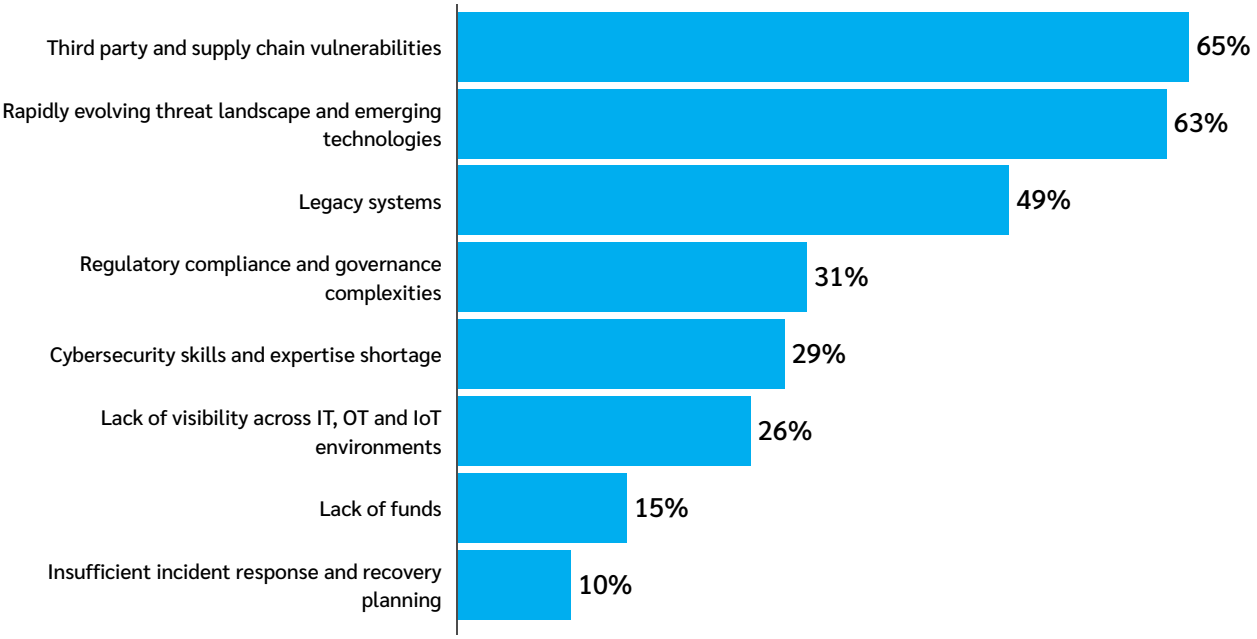
At the same time, rising geopolitical tensions in 2025 and 2026 have increased the risk of ideologically motivated attacks aimed not at extortion, but at disruption. Survey respondents cited geopolitically motivated cyberattacks as the leading factor shaping their cyber-risk mitigation strategies.

## Insurance response & pain points

Most cyber policies offer some form of business interruption coverage, but claims are closely scrutinized. Insurers focus on when an interruption began and ended, whether decisions to shut down systems were reasonable, and how policyholders calculate their losses.

Organizations that track revenue in real time — such as casinos or online retailers — may find it easier to demonstrate business interruption losses. For many others, particularly those with longer revenue cycles or intangible outputs, quantification can be significantly more challenging. To understand potential losses from business interruption events, brokers may provide modeling tools, but these require companies to realistically assess what a "worst day" looks like during a cyber event and to manage expectations about how much loss is ultimately recoverable.

THIRD-PARTY AND SUPPLY CHAIN VULNERABILITIES ARE ORGANIZATIONS' TOP CHALLENGE TO CYBER RESILIENCE.




Source: World Economic Forum/Accenture
Surveyed organizations selected up to three challenges.

02

# Ransomware's growing costs

Ransomware continues to draw public attention, but the nature of these attacks — and their financial impact — has evolved. Where attackers once focused on encrypting data and selling decryption keys, many now prioritize data theft and extortion, demanding payment to prevent publication or reuse of stolen information.

In 2025, just over 30% of ransomware victims paid a ransom, consistent with prior years, according to Arete Advisors. Median ransom demands rose to $600,000, up from $500,000 in 2024, while median payments increased only modestly to $152,750.

The higher cost often lies adjacent to the actual ransom. Sophos estimates the average enterprise recovery cost from ransomware in 2025 — excluding ransom payments — was $1.85 million, reflecting expenses tied to investigation, system restoration, legal response, and business disruption. Higher education, finance, transportation and logistics, and retail incurred particularly high recovery costs.

## Ransomware coverage challenges

Although most cyber policies cover ransomware, insurers increasingly focus on whether policyholders met baseline security and governance expectations. Identity controls, access management, backup integrity, and incident response preparedness are central to underwriting and claims decisions.

Disputes today often turn less on policy exclusions and more on compliance with conditions. Insurers are tightening scrutiny of restoration timelines, imposing or reducing business interruption sublimits, and requiring clearer dependency mapping. Because ransomware frequently involves data theft and extortion, insurers are also looking beyond ransom reimbursement and recovery costs to privacy liability, regulatory exposure, and litigation — raising complex issues around aggregation, sublimits, and allocation.

03

# Social engineering fraud & business email compromise

SEF may be the most significant cyber risk facing organizations today. Attackers can pursue these schemes quickly, cheaply, and at scale. While technology plays a role, the real vulnerability is human behavior.

In 2025 and 2026, attackers have increasingly used AI-driven deepfakes to impersonate senior executives via phone calls or voice messages, convincing employees to transfer funds or disclose sensitive information. These tactics now rival — and in some cases surpass — traditional BEC attacks involving phishing emails or bogus invoices.

SEF schemes often evade technical controls by exploiting trust, urgency, and routine business processes. Fast-paced communication, decentralized decision-making, and reliance on email and messaging platforms all increase exposure.

Large companies with good internal controls can still fall victim to theft by SEF. Some recent examples of SEF included fraudsters impersonating investors and well-known law firms in M&A transactions or other business deals. Mobile numbers set up to send genuine-looking calls and messages, along with fake portals mimicking well-known law firms to exchange documents, furthered a scheme in which multiple transactions were routed to fake bank accounts that could not be clawed back later.

This has driven some companies to question whether they are purchasing enough social engineering coverage.

Assuming the client has adequate controls in place, the Lockton U.K. crime wording offers full social engineering coverage. It works on a broader "all risk" basis, rather than the "named peril" basis that many crime wordings operate on.

These examples demonstrate the pervasiveness of cybersecurity threats, the complexity of insurance coverage, and the centrality of human error in today's most expensive claims.

## Insurance implications of SEF losses

Insurance recovery for SEF claims often depends on strict adherence to internal payment controls. Coverage may turn on whether companies enforced dual authorization, callback verification, segregation of duties, and escalation protocols. In some jurisdictions, such as many in the Middle East, stolen funds are not covered under a cyber policy but rather under a crime policy.

Insurers are increasingly denying claims where controls were bypassed — even under pressure or apparent executive urgency. As a result, claims investigations frequently resemble forensic audits of internal process compliance rather than assessments of criminal conduct.

AI-enabled impersonation has also complicated coverage. While some voice spoofing incidents may still fall under existing crime or impersonation coverage, underwriters are questioning whether traditional policy language adequately addresses synthetic identity attacks. In some cases, endorsements are being tightened to exclude "authorized" transfers, even when authorization was obtained through deception.

04

# The perils of privacy & data breaches

Although the fundamental pattern of data breaches — unauthorized access followed by theft or misuse of personal data — has remained consistent, recent years have seen an increase in third-party involvement. *Verizon's Data Breach Investigations Report* found that 48% of breaches from Nov. 1, 2024, through Oct. 31, 2025, involved third parties, up from 30% in the previous year.

Supply chain risk is especially acute for small and midsize organizations, which are targeted nearly four times as often as large enterprises. Still, human error and complacency remain the dominant contributors to data loss.

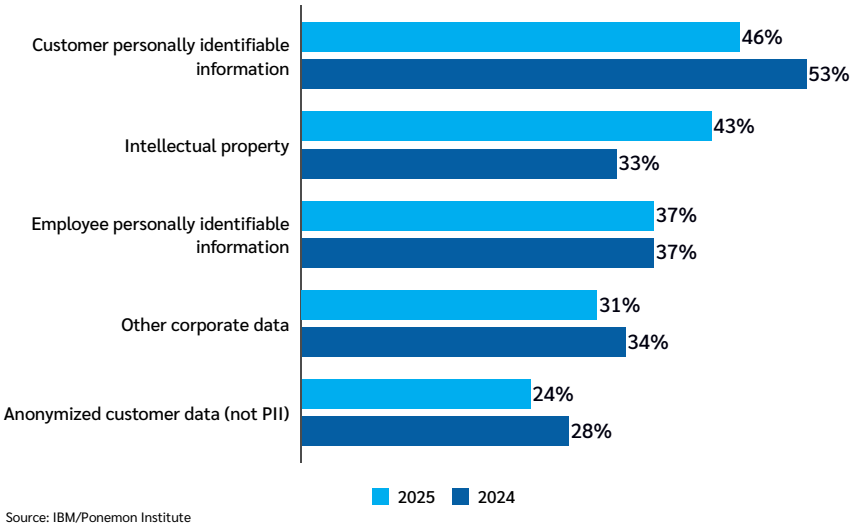
Attackers most commonly seek personally identifiable information such as tax identification numbers, addresses, and email credentials, according to IBM and the Ponemon Institute.

This data fuels downstream crimes, enabling highly targeted phishing and fraud attempts.

NEARLY HALF OF ALL DATA BREACHES IN THE YEAR ENDING OCT. 31, 2025, INVOLVED THIRD PARTIES.

Source: Verizon

PERSONALLY IDENTIFIABLE INFORMATION ABOUT CUSTOMERS WAS TARGETED IN NEARLY 50% OF BREACHES IN 2025.




Source: IBM/Ponemon Institute

The costs of data breaches include investigation and remediation, operational disruption, victim compensation, litigation, and regulatory fines. Roughly one-third of organizations that experienced a breach in 2025 paid regulatory fines, with the highest penalties reported in the United States — one reason breaches there are particularly costly. The Middle East and Benelux, a European region comprising Belgium, the Netherlands, and Luxembourg, had the second and third highest breach costs, respectively.

OUTSIDE THE U.S., THE HIGHEST DATA BREACH COSTS IN 2025 WERE IN THE MIDDLE EAST AND BENELUX.

| # | Country/region | 2025 | 2024 | # | Country/region | 2025 | 2024 |
|---|---|---|---|---|---|---|---|
| 1 | United States | $10.22 | $9.36 | 9 | ASEAN | $3.67 | $3.23 |
| 2 | Middle East | $7.29 | $8.75 | 10 | Japan | $3.65 | $4.19 |
| 3 | Benelux | $6.24 | $5.90 | 11 | Italy | $3.44 | $4.73 |
| 4 | Canada | $4.84 | $4.66 | 12 | South Korea | $2.84 | $3.62 |
| 5 | United Kingdom | $4.14 | $4.53 | 13 | Australia | $2.55 | $2.78 |
| 6 | Germany | $4.03 | $5.31 | 14 | India | $2.51 | $2.35 |
| 7 | Latin America | $3.81 | $4.16 | 15 | South Africa | $2.37 | $2.78 |
| 8 | France | $3.73 | $4.17 | 16 | Brazil | $1.22 | $1.36 |

Source: IBM/Ponemon Institute
Dollar figures in millions.

Evolving tactics by plaintiffs' attorneys have given rise to new data breach risks. Plaintiffs' attorneys in the U.S. increasingly employ technicians who surf the so-called "dark web," an obscure corner of the internet that requires specialized tools to access and where threat actors often communicate.

Technicians scan the dark web for discussions of stolen data, which plaintiffs' attorneys then use to file lawsuits quickly, sometimes before the company even knows there was an issue. This makes it challenging for a company to defend itself at the early stages of litigation.

## Insurance challenges in data breach claims

Insurers now expect demonstrable data governance, not future-looking promises. Underwriters want evidence of encryption, access control, retention policies, employee training, and vendor risk management that are already in place.

Mapping dependencies and assessing third-party risk are no longer optional. As with SEF and ransomware claims, insurers are increasingly framing coverage questions around compliance with security and governance standards rather than purely around the occurrence of a breach.

05

# Non-breach privacy risk & pixel tracking

Some of the fastest-growing cyber losses do not involve breaches at all. In 2022, Mass General Brigham settled a class-action lawsuit for $18 million over the use of cookies and pixels on its patient portal. The settlement fueled a wave of similar claims.

Pixel tracking — technology that monitors user behavior on websites — can trigger liability when data is collected without proper consent. Litigation alleging violations of wiretapping, privacy, and consumer protection statutes surged to 2,200 lawsuits in 2025, according to Fisher Phillips.

Retailers are frequent targets, but healthcare, technology, manufacturing, finance, and insurance companies also face claims, many of which settle for more than $1 million. In a high-profile case, a San Francisco jury in September 2025 awarded $425.7 million against Google for unauthorized tracking of users who had opted out. Google was also fined 325 million euros by a French regulatory agency in 2025 for displaying ads containing cookies on Gmail without obtaining account holders' consent.

## Why pixel tracking claims are so challenging

Unlike external cyberattacks, pixel tracking claims can stem from deliberate business or marketing decisions made without full awareness of legal exposure. Other times, companies hire website design firms that install these tools without the company's knowledge of their presence or understanding of what they do. Plaintiffs' attorneys can file claims cheaply and at scale, often leveraging decades-old statutes.

U.S. states such as California have expanded definitions of personal information, particularly for minors, making technical defenses less effective. Plaintiffs' attorneys have tried to push a theory that pixel tracking is intentional conduct, which opens the door to claims of willfulness or negligence, especially where executives were unaware that pixels had been deployed.

Insurers frequently exclude non-breach privacy violations and wrongful collection claims. Definitions of privacy violations, personal information, and security events have narrowed, and carriers often argue that coverage should not apply where a company chooses to deploy tracking technology.

Provisions requiring arbitration to resolve legal disputes over pixel tracking and other advertising technology can prove troublesome. Plaintiffs' attorneys can send a company a letter indicating they have hundreds or thousands of clients ready to proceed with arbitration, which can amplify legal costs for companies and their insurers.

06

# Media, marketing, & intellectual property risks

Like pixel tracking, media and intellectual property losses arise from a company's own actions rather than malicious outsiders. Cyber policies provide limited coverage, with many of these risks better suited to professional liability or media policies.

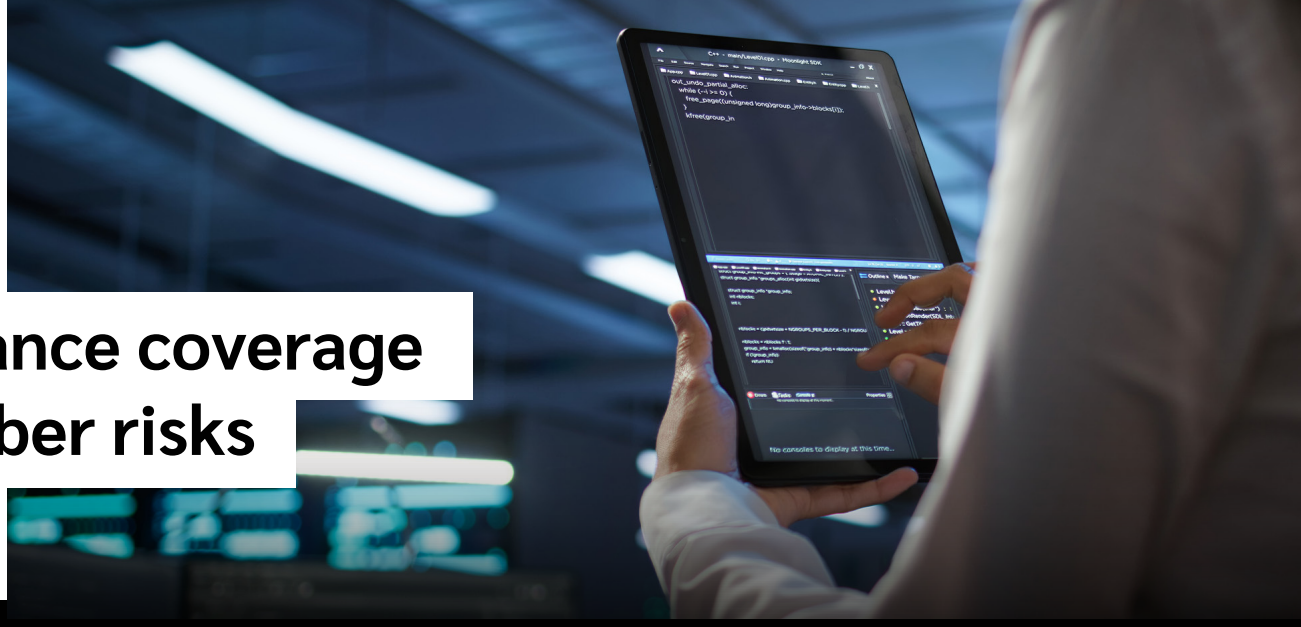
False advertising is a growing problem. Food manufacturers in particular have faced lawsuits over misleading health claims tied to ultraprocessed products. Instacart paid $60 million to settle FTC allegations that its "free delivery" and "100% satisfaction guarantee" claims were misleading. Underwriters often view false advertising as an intentional act by an insured and often exclude it from cyber policies.

Copyright infringement is another recurring risk, especially in social media marketing. Casual use of copyrighted music, images, or likenesses by brands or influencers has drawn aggressive enforcement from content owners. Defamation exposure increases when companies post provocative or inaccurate content in pursuit of online engagement.

## Preparing for the full spectrum of cyber loss

Today's cyber losses reflect more than technical failure. They arise from human judgment, operational dependencies, strategic decisions, and evolving legal standards. Insurance remains a critical tool, but recovery increasingly depends on demonstrated controls, governance discipline, and realistic planning.

Understanding how losses actually occur — and where coverage frictions emerge — allows organizations to better manage expectations, reduce exposure, and respond more effectively when incidents inevitably occur.



# Insurance coverage for cyber risks

## Overlaps & gaps in cybersecurity coverage

As cybersecurity risks expand and evolve, so does the need for a layered, sophisticated insurance program. Cyber policies have grown to incorporate many cyber-related risks but are still too narrow to cover the full gamut of cyber-related risks.

Cybersecurity failures are not straightforward incidents.

A data breach or ransomware attack requires a company to determine:

**What information was lost, who was affected, and how to restore data, which could trigger first-party cyber losses.**

**What remedies are needed for those affected by the stolen data, which could trigger third-party cyber losses.**

**Whether the attack disrupted normal operations, causing additional costs and introducing business interruption coverage.**

**How much was lost from a fraudulent funds transfer or a ransomware payment, which could trigger crime coverage.**

**Whether there was any damage to physical property as a result of the cyberattack, and whether that property belonged to the insured organization or a third party, which could trigger property or casualty coverages.**

**Who was to blame, which could implicate errors and omissions or directors and officers liability coverages.**

Clearly, these events trigger a cascade of insurance coverages, some of which may fall outside a cyber policy and others that may be covered by more than one insurance line. AI and its usefulness to threat actors can accelerate multiline losses.

The increasingly interconnected business world is another factor that will amplify this phenomenon.

The concentration of information technology services, particularly cloud vendors and software, to a handful of dominant providers, and the dependency of businesses upon these services, increases aggregation risks to primary carriers and reinsurers.

Then there are gaps in coverage. A common misconception among policyholders is that cyber policies cover anything related to computers or electronic devices.

A policyholder carrying on under this assumption may wonder why their cyber policy did not respond when an employee was duped into transferring funds to an unauthorized account by a threat actor's convincing AI-enabled deepfake ruse. Losses of this type in the $250,000 to $500,000 range may be covered under a cyber policy, but larger losses may not.

On the other hand, if the employee had been tricked into releasing employee tax documents containing highly confidential personal information to a threat actor, a cyber policy would respond. In many cases, the purloined data can impose a greater financial burden on a company than a fraudulent funds transfer, as employees may sue the organization for surrendering their private information.

## Underwriters are increasingly sharpening their pencils

Policyholders in general have recognized the peril of cybersecurity threats and adopted reasonably effective defenses against common attacks. Companies with cyber insurance have shown greater resilience than those without, partly because of the expectations policyholders must meet to receive coverage.

As AI proliferates, businesses should expect to receive increasingly detailed questions about how they use AI when renewal time comes. Underwriters want to know the company's practices, policies, and governance of AI use. Are employees trained on how to use and not use AI? Are employees only using sanctioned, enterprise-level AI applications for work purposes? How are company leaders enforcing their AI policies?

Conversely, businesses can demonstrate to underwriters how they use AI to defend against cyberattacks.

Underwriters have also placed greater emphasis and scrutiny on third-party exposures, particularly vendor concentration and supply chain dependencies that can lead to aggregation and systemic risk.

Companies should be prepared to describe the risk assessments they have conducted for their information technology vendors, particularly cloud companies, managed service providers, and software-as-a-service (SaaS) partners. Reinsurers in particular are concerned about the potential for significant losses from systemic risks and whether the primary insurance market has fully appreciated the potential for downstream effects of a major incident.

# Global regulations & considerations in cybersecurity

While the nature of cyberattacks and liabilities knows few geographic boundaries, different regions can take distinct approaches toward regulation and how insurance should respond to cyber events. Some of these differences are shaped by varying attitudes and laws that govern litigation, the degree to which critical infrastructure is exposed, and other local pressures. Corporate leaders and risk management professionals of multinational companies must navigate a maze of evolving and inconsistent standards across multiple jurisdictions.

## United States

The U.S. is the world's most litigious environment, which increases cybersecurity risks for operating within its borders.

Class-action litigation may represent a bigger headache to companies than regulations. Plaintiffs filed 1,488 data breach class-action lawsuits in 2024, a 1,265% increase since 2018, according to the Duane Morris law firm. The FTC can pursue companies for failures to reasonably safeguard consumer data. The FTC brought its first data security case under the FTC Act in 2003 and has brought 90 more cases since then.

A relatively recent federal law may lead to sweeping changes to cybersecurity reporting requirements. The Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) was passed in 2022. CIRCIA directed CISA to adopt rules governing when critical infrastructure organizations must report cyberattacks and ransomware payments.

When the rules take effect, they are expected to require covered entities in critical infrastructure sectors to report cyber incidents to CISA within 72 hours and ransom payments within 24 hours. CISA was scheduled to finalize the rule in May, but a partial government shutdown has delayed implementation.

Other sector-specific federal laws — the Health Insurance Portability and Accountability Act (HIPAA) for health information and the Gramm-Leach-Bliley Act (GLBA) for consumer financial companies — govern data privacy and breach notifications.

FTC rules imposed under the Children's Online Privacy Protection Act (COPPA) require businesses, and particularly their websites and online applications, to receive parental consent before collecting personal data on children under 13. The FTC updated COPPA-related rules in 2025 to expand the definition of personal information to include biometric data and to require parental consent for targeted advertising.

Beyond the federal government, states have enacted their own privacy and data protection laws. Many of these laws bear similarities, but some go further than others. California, for example, requires companies to notify affected individuals within 30 days of discovering a data breach under the California Consumer Privacy Act (CCPA).

Starting in 2026, CCPA also requires cybersecurity audits by independent auditors of businesses that collect consumer data to the point that its disclosure could pose a significant risk. Businesses that generate more than $100 million in revenue must submit their first audit in 2028, while companies that generate less than $100 million in revenue report their audits in subsequent years.

AI regulation in the U.S. remains limited. The White House wants the U.S. to lead in AI development and issued an executive order in December to limit states' ability to regulate the technology.

## Australia

Australia is arguably the world's second most litigious country after the U.S. But it may lead the way in terms of regulatory aggressiveness.

In the last two years, the Australian Securities and Investments Commission (ASIC) publicly sought to make an example out of a company — a test case the office can link to a breach of a director's duties — that fails to protect its cybersecurity systems.

Other sector-specific regulators, like the Australian Prudential Regulation Authority (APRA), have adopted a similar posture. The APRA successfully pursued two companies that hold financial services licenses for their failures in maintaining cyber resiliency in the last 18 months.

Another Australian company was fined $3 million for violating the Australian Privacy Act. While the fine was modest, the Office of the Australian Information Commissioner's investigation findings were scathing, citing the company for contracting with subpar vendors to remediate the violation.

## Asia-Pacific

Certain Asian countries have adopted more precise cybersecurity measures in recent years and are rapidly maturing from a general guideline stance to a more stringent, enforceable regulated environment. While major players like China and Singapore have established frameworks, other countries are in the process of implementing significant updates to align with global standards like GDPR.

### CHINA

Since coming into effect in November 2025, the Personal Information Protection Law (PIPL) requires cybersecurity incidents involving critical infrastructure to be reported within one hour and those involving non-critical infrastructure within four hours.

### HONG KONG

Following China closely, Hong Kong adopted new regulations in 2026 for critical infrastructure operators, including public infrastructure and key private industries such as banking and healthcare. Critical infrastructure organizations operating in Hong Kong must conduct regular risk assessments and security audits of their computer and network systems and maintain emergency response plans.

### INDONESIA

The Personal Data Protection (PDP) Law became fully enforceable in October 2024, imposing fines of up to 2% of annual revenue for noncompliance.

### JAPAN

Japan has shifted from a passive stance to a more proactive Active Cyber Defence Law (enacted in May 2025, operational by 2027) as well as the Act on the Protection and Use of Critical Economic Security Information (effective May 2025).

### SINGAPORE

With ambitions of becoming a regional cyber innovation center, Singapore has historically been in possession of a sophisticated set of cybersecurity laws, such as the Computer Misuse Act 1993, Spam Control Act 2007, Personal Data Protection Act 2012, and Cybersecurity Act 2018. This has equipped Singapore to move forward with developing grants for AI-infused threat detection and quantum-safe encryption.

### SOUTH KOREA

The Personal Information Protection Act was updated to levy fines of up to 10% of a company's total revenue, add rules governing decisions made by AI, and require mandatory breach notifications within 72 hours.

### THAILAND

Guidelines were updated for Data Subject Access Requests, as well as transparency for digital platform fees to protect consumer data.

### VIETNAM

Its frameworks were extended beyond cybersecurity to include legal frameworks for blockchain with strict localization requirements.

## Europe & United Kingdom

The litigation environments in Europe and the United Kingdom are more restrained than the U.S. and Australia. Class-action lawsuits, or collective actions, are rare.

Regulations often take the lead in policing cybersecurity matters in these jurisdictions.

The European Union's General Data Protection Regulation (GDPR) continues to govern how organizations maintain and handle personal data and information. Fines for violating GDPR can reach 20 million euros or 4% of an offending enterprise's global revenue, whichever is higher. A similar regulation applies in the U.K.

The EU also passed the AI Act, a comprehensive law that governs AI. The AI Act requires AI systems deemed "high risk" to be resilient against intrusions and system exploitations. The law came into force in August 2024, with specific provisions set to become effective through August 2027.

# Risk-specific considerations in different countries

## Ransomware trends around the world

Even as ransomware is universally recognized as a critical cyber risk, its significance and nature vary by geography, as do attitudes toward ransom payments.

In the highly litigious U.S., concerns about lawsuits are paramount, providing one explanation why ransom payments have not increased substantially even as demands continue to rise.

There has also been the problem of newer threat actors that inconsistently honor promises — and, in fact, are more likely to double-cross victims even after payment. The increasing prevalence of data exfiltration means companies may still face significant litigation and regulatory risks, giving ransomware targets a valid reason not to pay ransoms.

In the U.K. and Europe, ransomware is viewed primarily as a business interruption and governance issue. Senior corporate leaders are focused on regulatory expectations and resilience rather than negotiation outcomes.

In Australia, ransomware targets tend to take a pragmatic approach: Ransom payments are increasingly avoided, but regulators — including ASIC and APRA — heavily influence response strategy and costs.

In Asia, ransomware is a persistent threat but does not typically spark litigation. The consequences of attacks are primarily operational, not legal. Decisions about paying ransoms are thus driven by downtime tolerance and recovery speed, as regulatory enforcement and class-action exposure remain relatively limited.

In Latin America, ransomware remains one of the most prevalent cyber threats, particularly among small and medium enterprises with weaker cybersecurity controls. Companies tend to be more tolerant of downtime, and regulatory or litigation consequences are limited. Ransom payments are considered more often, but targets are growing more skeptical of payments due to unreliable threat actors and persistent business interruption losses.

In the Middle East and North Africa, ransomware is seen as a strategic operational and regulatory risk. Ransomware incidents often affect critical infrastructure, healthcare, energy, banking, and government-linked entities, for which continuity and public trust are paramount. Data localization laws and sector regulators strongly shape response decisions, with implicit or explicit expectations not to pay ransoms, particularly in regulated sectors. As a result, organizations frequently prioritize containment, restoration, and regulatory engagement over negotiation, even when outages are prolonged.

## The global perspective on pixel tracking

While U.S.-based companies have been the most frequent targets of pixel litigation, companies based elsewhere — notably, in the U.K. and Australia — have also been targeted in suits filed in the U.S.

Beyond litigation, pixels and other tracking technologies are governed under the EU's GDPR, its equivalent law in the U.K., and other laws in Latin America and the Middle East. These laws require that companies obtain consent from website visitors before using such technologies. Compliance is enforced through regulatory action rather than private litigation, though enforcement activity worldwide is uneven, and many regulators do not prioritize pixel tracking.

The insurance industry, however, is watching for potential developments in Australia, another litigious country that often follows the U.S. lead on legal and regulatory matters. Although pixel tracking is not currently a primary focus of Australian regulators and there currently is no mechanism for private litigation in Australian courts alleging improper use of tracking technologies, that could change in the future.

# Reducing cyber claims severity

## Governance over technology deployment

**01** | **Adopt, monitor, and enforce cybersecurity policies.** Training employees on new methods of AI-driven attacks becomes imperative in this environment. All employees should understand defenses against cyber intrusions, including multifactor authentication, and use them regularly. Additionally, company officials should regularly conduct incident response exercises, particularly to account for the speed at which cyberattackers can use AI to infiltrate and extract sensitive data.

**02** | **Expect more questions from insurers on AI.** Companies should expect to receive increasingly detailed questions about how they use AI and what policies they have adopted to address its use when renewal time comes. How are company leaders enforcing their AI policies? Conversely, businesses can demonstrate to underwriters how they use AI to defend against cyberattacks.

**03** | **Treat pixel tracking as a legal, governance, and insurance risk, not simply a marketing or IT function.** Limit who can approve website technologies, implement control group structures, and document that senior leadership does not knowingly authorize tracking tools without legal review. This is critical to preserving coverage and avoiding intent-based exclusions. Companies should communicate with outside marketing agencies and website designers to understand if pixel tracking applications or other advertising technology tools are embedded in websites.

**04** | **Treat business email compromise as a governance issue, not an IT issue.** Assign clear ownership to finance, operations, and leadership — not just cybersecurity.

## Identity & access discipline

**01** | **Strengthen identity and access controls.** Prioritize multifactor authentication, privileged access management, and credential hygiene as the most effective preventive measures.

**02** | **Assume humans are the primary attack surface.** Invest in regular, realistic employee training focused on urgency, impersonation, and authority-based manipulation.

**03** | **Do not keep old data around.** Companies should adopt, maintain, and enforce retention schedules for data and dispose of old, unneeded files regularly. Keeping unnecessary data poses a significant and avoidable risk if a breach occurs.

---

## Payment & verification controls

**01** | **Strengthen payment controls to minimize deepfake and ransomware threats.** Require dual approvals, segregation of duties, and mandatory callback verification for payment or account change requests.

**02** | **Do not rely on email alone for approvals.** Prohibit financial or vendor changes based solely on email or messaging instructions.

**03** | **Map and test response workflows.** Ensure staff members know how to pause, escalate, and validate suspicious requests without penalty.

---

## Incident response speed

**01** | **Design for speed and pressure.** Controls must hold up during peak periods (quarter end, deals, vendor changes), when fraud risk is highest.

**02** | **Align response, governance, and insurance for ransomware threats.** Establish clear ransom decision frameworks, engage experienced incident response partners early, and stress-test insurance coverage and sublimits before an event.

**03** | **Do not rely on ransom payments to resolve risk.** Payment rarely prevents data release, litigation, or regulatory action; it should not be viewed as a mitigation strategy.

**04** | **Monitor the web for discussion about stolen data.** IT teams or third-party services should examine the internet for mentions of stolen data for sale. This can be the first indication that a breach has occurred and is where plaintiffs' attorneys sometimes look for litigation opportunities. Companies should hire third-party services to examine the dark web for any discussion about stolen data.

## Preparing for losses

**01** | **Prepare for business interruption losses.** Test recovery timelines realistically, including third-party and cloud dependencies.

**02** | **Assume data exfiltration will occur.** Plan for data theft and extortion, not just system encryption. Backups alone can no longer neutralize ransomware risk.

**03** | **Regularly audit websites to inventory pixels, cookies, session-replay tools, and third-party scripts.** Apply particular scrutiny to those enabled by vendors or marketing platforms. Question whether your organization truly needs tracking tools and strongly consider eliminating unnecessary pixels to reduce exposure.

**04** | **Pay attention to different privacy and data collection consent regulations.** Implement transparent, jurisdiction-specific consent mechanisms and genuine opt-in/opt-out functionality in compliance with the most stringent regulatory regimes (particularly California).

**05** | **Prepare for deepfake and impersonation attacks.** Update controls to assume voice and identity spoofing will be credible, not obvious.

**06** | **Understand insurance limits and conditions for cyber incidents.** Confirm where coverage sits (usually crime, not cyber) and design controls to align with policy requirements.

**07** | **Train employees regularly on intellectual property risks.** Employees should receive training on applicable intellectual property and copyright laws, including what constitutes fair use and what does not. They should also understand social media risks, including what actions could give rise to allegations of defamation.

**08** | **Manage IP and defamation claims proactively.** Policyholders should immediately notify insurers and attorneys about claims or threats to initiate claims for intellectual property theft or defamation. Ignoring potential claims increases the risk of litigation and can result in a denial of coverage.

**09** | **Establish contracts with outside marketing partners, including influencers.** Terms should clarify insurance and indemnification agreements if and when claims are made.

# Together, let's overcome your cyber risk challenges

To learn more about how you can effectively manage your cyber threats, connect with a member of our Cyber & Technology team.

SCAN TO VISIT OUR CYBER PAGE

**lockton.com** | © 2026 Lockton Companies. All rights reserved.

C | 7817770 0626