CYBER AND DATA PRIVACY INSURANCE IN 2025

By Glenn E. Davis

DEM10/ISTOCK/GETTY IMAGES PLUS VIA GETTY IMAGES

Business leaders widely regard cyber threats as their number one concern in 2025.[1] Accordingly, cyber and data privacy insurance, in one form or another, is critical for most businesses in today's interconnected environment. Yet the market is fraught with risk for insurance companies and insureds alike. From the first cyber policies in the late 1990s, the market has remained fluid and evolved in fits and starts. Persistent and viral cyber threats that defy risk measurement by conventional risk assessment approaches complicate underwriting. Unlike centuries-old life, property, maritime, and auto insurance, there is no longitudinal benchmark data to support underwriting determinations.

In 2022, reported ransomware attacks fell substantially below prior levels, but starting in 2023 and throughout 2024, ransomware came back with a vengeance.[2] Cyber claims exceeding $1 million rose 14% in early 2024, with claim severity increasing 17%—after a 1% increase in 2023.[3] Data breaches now trigger complex challenges with privacy regulation, cyber insurance, and third-party liability ramifications.[4] Privacy-related class actions have tripled in value in recent years. Indeed, "nonattack" cyber and data privacy claims, such as wrongful collection, use, and processing claims, have tripled.[5] Such claims extend to data privacy regulatory cases initiated by the Federal Trade Commission (FTC), the Securities and Exchange Commission (SEC), and state regulators and attorneys general. The nature of risk and associated exposures in cyber and data privacy insurance were different in 2024 than in 2023 and are likely to change even more in 2025 and for the foreseeable future.

Accordingly, understanding and addressing increasing corporate cyber and data privacy risk is tricky and varies greatly by business sector. Careful risk assessment and alignment of governance protocols with evolving regulatory and insurance requirements are critical for organizational resilience. Effective cyber coverage must be calibrated to address specific company risks, given relevant data, operational, and interruption risks, and the financial magnitude of intrusions. Cyber insurance is a core risk transfer mechanism.

Insurance Market Risk and Price Trends

Basic cyber coverage. Cyber risk and liability insurance assists businesses with recovery from the financial impact of data breaches, malware and viruses, and other cyberattacks, by covering costs incurred by the insured (first-party claims) and expenses imposed by claims of others (third-party claims). Cyber insurance policies typically provide a mix of first-party and third-party coverages. As summarized below, the policies generally provide reimbursement for investigation expenses, business losses, legal proceedings, extortion, privacy claims, and notification costs.

First-party coverage typically includes costs related to:

- Breach response
- Cyber extortion
- Network business interruption
- Data restoration
- Funds transfer fraud
- Contingent business interruption

Thus, first-party insurance provides coverage for financial losses the insured directly incurs. In the early stages of response to a cyberattack, one of the most important grants of first-party coverage is for breach response costs. Although various cyber policies use different terms, most cyber policies provide coverage for certain costs incurred responding to a cyber breach. For example, most cyber policies provide coverage for reasonable and necessary expenses incurred by a policyholder to investigate the cause and extent of a breach. In addition, many cyber policies provide coverage for legal expenses incurred to comply with breach notification laws. Most cyber policies also provide coverage for expenses incurred to notify customers or employees whose personal information may have been taken by the attackers.

Third-party coverage typically includes expenses related to:

- Network security liability
- Privacy liability
- Privacy regulatory proceedings and fines
- Payment Card Industry Data Security Standards (PCI DSS) liability
- Media liability
- Civil damage claims, attorney fees, and settlement costs

Thus, third-party coverage protects the insured from liability actions third parties assert against them following a cyber event. This includes claims from customers and clients, consumers, vendors and suppliers, and regulators, and reimburses attorney fees, settlement costs, payment of court-ordered damages, government investigation response costs, and any resulting government fines or penalties. Third-party coverage accounted for a 62.1% share of the cyber insurance market in 2023.[6]

Types of cyber liability insurance policies. Stand-alone policies are tailored to specific businesses and the threats they face, such as data breaches and ransomware attacks. Stand-alone policies are particularly favored by large organizations in industries highly susceptible to cyber threats, such as firms in the finance and health care sectors. In 2023, it is estimated that stand-alone cyber insurance policies captured more than two-thirds (68%) of the market.[7] Packaged policies incorporate some forms of cyber coverage in other policies, such as directors and officers (D&O), comprehensive general liability (CGL), and computer risk policies. Cyber protection may be included by addenda or endorsements to the primary policy.

Although there are myriad variations, there are four principal types of cyber policy coverages: data breach, ransomware, loss of funds, and specific incident coverages.[8] Data breach coverage addresses financial loss risks flowing from a defined data breach. These policies generally include cyber liability insurance and technology errors and omissions (E&O) coverage. Ransomware

TIP: Businesses should consider working with a knowledgeable broker and building long-term relationships with insurers for better accommodations and claims outcomes.

coverage specifically protects the policyholder from ransom payments, extortion-related costs, data compromise or destruction, and response costs. This form (or policy addenda providing it) defines important ransomware exclusions. Loss of funds policy coverage addresses cybercrime, wire fraud, push payments, and social engineering fraud. Again, there is no policy uniformity as to the meaning of these terms, and policyholders and their advisers need to drill down on the specifics provided. Finally, other scenarios, such as cryptojacking, bricking, and system failure related to a breach, may require supplemental coverage attention.

Coverage limitations. Unsurprisingly, discerning the wide variations in cyber coverage limitations is a critical challenge in cyber policy selection. As discussed below, incidents attributed to nation-state attacks may be excluded due to the complexity of causation determinations and the heightened risks involved. Moreover, breaches of unencrypted data, which create significant privacy risk exposures, are often not covered unless the insured maintains specific data security protocols. Policies may also exclude third-party liabilities unless strict contractual security terms with vendors are documented, a condition that highlights insurers' focus on managing interconnected risks. These coverage restrictions necessitate that organizations implement comprehensive security measures and review their insurance policies carefully to avoid gaps in protection.

Cost of cyber coverage. Premium levels, and important policy features such as deductibles, limits, and scope of coverage, shift with changing loss trends, interest rates, macroeconomic conditions, and available capital. The primary, excess, and reinsurance levels of the insurance marketplace make underwriting and product offering decisions with longitudinally limited and variable loss data. Cyber market pricing uncertainty is driven by several factors, including:

- Increasing attack frequency and severity
- Higher ransom demands and release or destruction of exfiltrated data
- Ongoing digital transformation with proliferation of interconnected devices and systems, expanding attack surfaces
- Proliferation of cyber and privacy regulatory regimes
- Accumulation of risks (incidents impact multiple insureds)
- "Silent cyber" losses insurers may be obligated to pay on policies not intended or designed for cyber coverage
- Increasing private and regulatory privacy litigation
- Constantly evolving technology
- Effectiveness of training, enhanced awareness, and improved technical controls and defenses

For several years preceding 2022, these and other conditions led to a "hard" cyber insurance market characterized by increasing premiums, low coverage limits, high self-insured retentions and deductibles, and aggressive sublimits.[9] The global cyber insurance market saw premiums reach approximately $14 billion in 2023, with projections that the market will reach $29 billion in premiums by 2027.[10]

The total direct premium spend for cybersecurity insurance in the U.S. increased 48.2% to $9.7 billion in 2022, from $6.5 billion in 2021.[11] The increases in premiums written were driven by much higher rates as well as higher volume. Carriers paid out $4 billion in claims in 2023 in the U.S., with 400 claims exceeding $1 million in loss.[12]

Several discernible trends contributed to increased cyber and data protection exposure:

- Challenges identifying and managing burgeoning data storage volumes
- Increasing use of artificial intelligence (AI) and corresponding challenges with tracking and protecting data
- Increasing attacker sophistication
- Keeping pace with cyber and data protection requirements and regulations across jurisdictions
- Ensuring proper handling of data across supply chains and by third-party vendors
- Updating existing cyber and data protection infrastructure
- Integrating and aligning diverse systems and cyber and data protection infrastructures following acquisitions

Many observers believed that the 2021–2022 uptick in cyber premiums would continue indefinitely or at least sustain the high levels they reached.

Beginning in 2023, and continuing into 2024, the pricing trend changed. While 2024 brought record-breaking data breach costs and more pernicious forms of cyber risk, the market exhibits stable rates and ample capacity in 2025. Improved loss experience and cyber incident cost management contributed to the downward price trend. With demand outpacing supply, the markets attracted new entry and individual carriers increased capacity and capital for the cyber sector. Premiums moderated

Glenn E. Davis *is a partner at HeplerBroom LLC in St. Louis, Missouri, where he engages in complex business litigation matters, with emphasis in antitrust, cybersecurity and privacy, professional liability, intellectual property, D&O and complex insurance claims, and class action defense. He is active in the TIPS Cyber and Data Privacy and Business Litigation Committees. He may be reached at glenn.davis@heplerbroom.com.*

and even flattened in some sectors, despite a heightened level of ransomware claims.[13] And premium rate increases in 2023 did not occur at the same rate as 2022 increase levels.[14] Intense competition among cyber insurance carriers has resulted in higher limits, enhanced cyber risk management services, more flexibility in insurance applications, and increased affordability and availability. Consequently, some policyholders elect either to purchase additional limits or lower retentions when there are premium savings on renewals.

Willis Towers Watson (WTW) projects flat primary and excess cyber renewals and decreases in some areas with readily available capacity.[15] However, entities with a negative loss experience or that cannot demonstrate strong ransomware controls may not receive lower premiums or favorable coverage terms. Underwriting decisions on pricing and attachment points are heavily influenced by the security controls a company has in place. However, increased limit factors (ILFs) have come down in excess placements due to intense competition, especially on large towers with significant premium decreases.

Broker Woodruff Sawyer's 2024 annual poll of cyber insurance carriers illustrates clearly the downward pricing trend and the flattening of renewal premiums.[16] According to the client survey, most industry sectors experienced significant cost reductions for cyber liability insurance.[17] As the notable exception, in the technology E&O segment, only 50% had a decrease. Technology supply chain risk, for firms that depend on technologies provided by others, remains a challenge and threatens aggregated risk. In other sectors, 60%–70% of insured firms achieved reductions. Even with reductions, however, the poll indicates that most clients are not reducing their self-insured retentions.[18]

While carriers have increased available capacity for cyber risk, they manage risk by setting modest primary layers, generally at $5 million, with targeted limits and exclusions. Companies over $500 million in revenue may receive primary options of up to $10 million. Accordingly, most insurance companies manage the level of risk they are willing to accept by limiting the amount insured for any single risk.

As noted, the volume of claims went down in 2022 through late 2023.[19] Nevertheless, there was a sharp rise in reported ransomware events in 2023, and, according to a large survey of corporate counsel, cyber and privacy issues will be one of the more active areas anticipated for litigation in 2024, trailing only employment matters.[20]

The worldwide financial impact of cybercrime is projected to reach $10.5 trillion annually by 2025, compared to $3 trillion 10 years ago.[21] In the private litigation arena, as reflected in a recent Bloomberg Law study of cyber litigation dockets and reports, both the increasing volume and value of ransomware attacks are reflected in increased federal lawsuit filings.[22]

Regulatory and legal issues. Expanding privacy requirements, and resulting litigation, will likely increase heading into 2025, and the proliferation of data privacy laws adds layers of complexity. The California Privacy Rights Act (CPRA)[23] enforcement mechanisms became effective in May 2024. A number of other states have now enacted similar privacy enforcement regimes. These laws require data management strategies to deal with a range of rights, from opt-in consent for sensitive data to comprehensive data access and deletion options.

Biometric privacy protection for collection and retention of information without consent and other procedures has triggered class action litigation, particularly based on the Illinois Biometric Information Privacy Act (BIPA).[24] BIPA authorizes a private right of action to recover $1,000 per violation, and $5,000 per violation for reckless or intentional failure to comply, resulting in large settlements.[25] Indeed, in *Cothron v. White Castle Systems, Inc.*, the Illinois Supreme Court ruled that BIPA claims accrue and are subject to separate damages for each employee scan without informed consent.[26] Notably, on August 2, 2024, Governor Pritzker signed the Illinois legislature's bill to amend BIPA to limit damages to avoid exponential liability for repetitive incidents, such as counting each use of the same technology (e.g., fingerprint recognition software) as a separate violation.[27]

Intense competition among cyber insurance carriers has resulted in higher limits, enhanced cyber risk management services, more flexibility in insurance applications, and increased affordability and availability.

With the number of regulatory bodies and the array of potential fines and penalties, insurance companies are being more restrictive on insuring costs of regulatory investigations and settlements. On privacy claims in particular, insureds should look for exclusions tied to specific laws and regulations. Terms such as "unauthorized, "wrongful," "unlawful," or "in violation of law" merit close attention.[28]

Privacy-related breaches, often inducing high-exposure claims, significantly impact cyber insurance economics. Privacy claims—often involving sensitive customer data—have substantial financial implications, including regulatory fines

and costly settlements. As data privacy regulations grow more stringent, breaches involving protected data trigger regulatory scrutiny, class action lawsuits, brand damage, and customer loss. The 2024 Change Healthcare breach, impacting approximately 190 million consumers with compromised patient records, led to both operational downtime and extensive privacy concerns.[29] Insureds, particularly those with sensitive customer data, and their carriers must address the likelihood of multiple concurrent lawsuits after a significant data breach.

The Situation for Insureds

The underwriting process. Concurrently with pricing moderation and increased capacity trends, insureds must continue to satisfy complex underwriting requirements. Insurers are assessing robust data governance, incident response plans, and third-party security measures in underwriting decisions. Insureds confront heightened eligibility standards, as well as broadened representation and warranty requirements. Insurers are applying new underwriting criteria, mandating specific controls, and closely monitoring new business.[30] Insurers often require audits of insureds' preparedness and cyber defenses or conduct external scans of the attack surfaces of their own clients. However, to mitigate risk, insurance companies are providing more support and preventative services, as well as experienced incident response teams comprised of legal, forensic, breach coach, notification and claims management, and public relations resources. The investment in strong data privacy and governance frameworks not only reduces the impact of security incidents but also improves the likelihood of negotiating more favorable insurance terms.

Scope of coverage. Despite the improved pricing situation, many insurers have nevertheless narrowed the scope of coverage. War exclusion modifications and limits on systemic risk, as well as increased privacy and personal and biometric information collection and retention claims, lead to coverage retraction. On March 31, 2023, Lloyd's of London mandated new war exclusion provisions in part to manage systemic loss.[31] Concerns remain over potential catastrophic cyber events that would inflict widespread harm. However, the rate of reported claims, while still high, substantially declined in the first two quarters of 2023 over 2022 numbers. Industry data shows a decline in the number of insureds reporting increased claims in 2023 versus 2022, but the cost of addressing a data breach continues to rise apace.[32] The average cost of a data breach set a record in 2023 at $4.45 million, an increase of over 15% since 2020.[33] According to IBM, the global average cost of a data breach in 2024 rose 10% over 2023 to $4.88 million, the largest increase since the pandemic.[34] Post-breach customer support, remediation, and business interruption caused the increased costs.

While most cyber policies provide some coverage for cyber extortion payments (i.e., ransom), as ransomware attacks[35] have become more common many insurers have implemented ransomware sublimits to limit their exposure to such attacks. A sublimit is a lower limit that applies to a particular type of loss. Thus, a cyber policy may have a $10 million limit that applies to most losses, but a $1 million limit that applies to ransomware losses. Insurers sometimes argue that all the costs associated with a ransomware attack are subject to a ransomware sublimit even though the policy provides that only those costs arising out of a ransom event are subject to the sublimit. Policyholders should carefully review their cyber insurance policies before making a claim to determine whether costs incurred in connection with the security breach that typically precedes a ransom demand are compensable under insuring agreements that are not subject to a ransomware sublimit.

Notice. In the event of a cyber incident, insureds should consider notice to their carrier, as most policies require notice as soon as practicable after discovery of a breach. There may be time limits requiring notice to be given during the policy, or within a certain number of days after the policy period ends. This is important because an insurer may deny an otherwise valid claim based on inadequate notice. Some states require an insurer to prove that it was prejudiced by the late notice to prevail on a late-notice defense, but others do not. Policyholders should be aware of notice provisions in their cyber insurance policies (and any other policies that may provide cyber coverage) and provide timely notice in accordance with them.

Market factors. Insureds' decisions on cyber insurance may be informed by, and certainly are affected by, the sector in which they operate. Based on reported incident responses, some business and professional segments fare better on incident rates and breach costs than others, which one might expect would yield lower premiums. The health care industry faces the highest data breach costs by a large margin.[36] A number of positive and negative factors influence breach costs, which may increase or decrease costs for insureds depending on their circumstances.

Positive factors include:

- Developed security operations
- Employee training
- Tested incident response plans
- Robust encryption
- Threat intelligence and threat hunting
- Insurance protection
- Board-level involvement

Negative factors include:

- Remote workforce
- Supply chain breach
- Internet of Things (IoT) environment
- Third-party involvement
- Cloud migration
- Regulatory noncompliance
- Security system complexity

Again, worldwide demand for cyber insurance continues to grow. Currently, there is sufficient cyber insurance capacity available in the market, and cyber insurance has remained a profitable line.[37] The underlying pricing increases over the past several years have enabled insurers to sustain the quality of cyber insurance. Insureds are likely to face smaller market swings and more realistic opportunities to consider increasing limits. Accordingly, insureds may reinvest year-over-year premium savings to secure better and more comprehensive coverage. Marsh has experienced this trend of clients seeking higher limits, driven by stabilized pricing.[38]

Among potential buyers, it remains true that larger companies are more likely to secure cyber insurance than small firms. Large businesses, with larger digital infrastructure and consequently higher risk, made up nearly three-quarters (72.4%) of the value of the cyber insurance market in 2023.[39] Cybercriminals perceive larger organizations as more lucrative targets, and they face more threats, not only from employee errors but also from business partner and supplier mistakes. At the same time, they enjoy greater risk management infrastructure, defense capabilities, and financial resources. But organizations with revenues of $100 million or less are learning the hard way that they are also prime, less formidably defended targets, and cyber insurance is a key part of cyber preparedness. Attackers are prone to target firms that may have less sophisticated defenses and resources. Perhaps ironically, the debate continues as to whether the very existence of cyber coverage invites more ransomware attacks.

But it is not all bad news. Most successful ransomware attacks involve some breakdown in technological defenses or absence of controls. In Change Healthcare's situation, several security controls failed regarding its Citrix remote-access portal, lack of multifactor authentication, and inadequate backup strategy. Notably, the UnitedHealth subsidiary also lacked cyber insurance and did not receive the benefit of careful underwriting and review of practices, which may have led to incorporation of defenses sufficient to defeat the attack. The "good news" is that implementation of more robust security measures may lower cyber policy costs.[40] Firms with strong backup capabilities claimed 72% lower damages and were 2.4 times less likely to have to pay ransom.[41]

Insureds need guidance from a broker well-versed in cyber insurance to assess their risk profile and specific coverage needs. This will include careful assessment of first-party and third-party coverage potentially applicable to specific business operations, and how much risk each insured might retain. In the current environment, Marsh reports that self-insured retentions are declining.

Finally, in current conditions, insureds may find it advantageous to forge long-term relationships with a carrier. While insurers will hold insureds to the "four corners of the policy," a multiyear relationship with an insurer may improve the insured's prospects for accommodations, exceptions, and improved claims outcomes. Multiline relationships with a cyber insurer may provide even more consideration.

Common Challenges

Ransomware, in its various iterations, remains the key challenge heading into 2025. The frequency of attacks is fueled by the simple business model of cybercriminals and ease of entry through ransomware as a service (RaaS). Supply chain–enabled ransomware, as well as double or triple extortion attacks, complicate response decision-making and costs. Supply chain–based attacks are increasingly common, and insurers are focused on the connections that exist between firms in the supply chain and digital supply chains.

Cyber insurers and insureds are, like it or not, in this together. They face common threats, and their interests in minimizing risk are aligned. While insureds may dislike the demands of the underwriting process, the overall effect of detailed questionnaires and recommended or required practices has prompted higher awareness and investment in protective measures that inure to the benefit of both insurers and insureds.

While predictions on these common challenges may be difficult, some appear very likely.

Improving cyber risk analytics. Cyber risk analytics is a growing field, and quantification of potential aggregate cyber losses will be vital to address awareness, data governance gaps, and coverage issues. Analytics specialty firms, insurance associations (such as the International Underwriting Association, the Geneva Association, and the International Association of Insurance Supervisors), and carriers are partnering to focus on data-driven guidance for insurers and reinsurers on key issues such as supply chain risk, modeling systemic risk, and evaluation of threat actors. Obtaining specific, reliable data remains difficult, particularly due to a lack of uniform data governance.

Geopolitical uncertainty and state-sponsored threat actors. Nation-states (or their proxies) routinely deploy cyberattacks as tactical and strategic offensive weapons in modern warfare. The current wars in Ukraine and Gaza bring into real focus the prospect of an attack spilling outside of intended targets and impacting the broader private sector. Many carriers launched revised language this past year—spurred by a mandate from Lloyd's of London to its syndicates and the potential inclusion of ransomware cybercrime groups in the federal sanctions list, affecting ransom payments.[42] The Russia-Ukraine conflict has led many markets to reassess their war and territorial exclusions, and we are seeing various versions of a London-based exclusion but still little uniformity on the kinds of nation-state attacks that would be covered, as well as other exclusions that provide some coverage for cyberattacks tied to physical war.

Spurred by a mandate from Lloyd's to its syndicates promoting model clauses, many carriers launched revised language in 2024.[43] Lloyd's requires all stand-alone cyber policies

to exclude liability for any state-supported cyberattack, and the exclusion must: (1) exclude losses from any declared or undeclared war, (2) exclude losses from state-backed attacks that significantly impair a state's ability to function or its security capabilities, (3) require clarity as to whether coverage includes or excludes computer systems outside any state, (4) define the basis of the parties' agreement as to how any state-backed cyberattack will be attributed to one or more states, and (5) include clear definitions of key terms.

These standardization attempts remain uncertain in application. Lloyd's believes that nation-states pose the greatest threat for development of malware capable of causing catastrophic, systemic destruction. Accordingly, Lloyd's model provisions have a particular focus on nation-state cyber activity, both in the course of war or independent of any physical war. But attribution is a vexing problem, and political charges without factual support or "normal" intelligence activity may elude consistent interpretation. And questions remain as to what constitutes a "sovereign state" for purposes of the exclusions. Policy language that expansively excludes cyber warfare engaged in or sponsored by nation-states may pose unexpected consequences.

The most commonly used model exclusion—LMA5567A/B—*does not* exclude state-sponsored cyberattacks unless certain thresholds are met, the most notable of which is that the insured digital assets must be located in a state that has suffered a "major detrimental impact." The complexity and subjectivity mean that certainty will be elusive until Lloyd's requirements are applied over time to reveal what is an uninsurable loss.[44] Without clearly worded exclusionary language, insureds may believe that they are generally covered for cyberattacks, only to find that their insurers apply policy exclusions broadly to preclude coverage for losses arising from attacks indirectly sponsored by sovereign states. Parties are free to negotiate their own terms and definitions subject to underwriters' approval. Insureds need to examine this exclusion language carefully and be clear on their expectations.

SEC disclosure rule. In response to heightened cyber risks and perceived lack of adequate disclosures on material risks and governance weaknesses, the SEC implemented new rules on July 26, 2023.[45] The new disclosure rules require all public companies to make disclosures on their information security preparedness and disclose cybersecurity breaches within four days after a determination that the incident is material. Public companies must have strong cross-functional processes in place to ensure that key stakeholders can quickly make this determination and meet these new reporting obligations. The SEC regulations focus on the role (and performance) of chief information security officers (CISOs).

SEC enforcement actions and stock drop class actions related to these requirements are occurring, which will result in more loss claims and defense costs. On October 22, 2024, the SEC charged four public companies with inadequate disclosures on cybersecurity risks.[46] The SEC is aggressively pursuing these matters, and its recent seven-figure settlements reinforce the importance of disclosure and response procedures following information security incidents.[47] These developments have opened potentially large exposures for firms and individuals who require close attention in coverage evaluation and assurance that defined "insured persons" include the right people.

Insureds may mitigate this risk with insurance, but it requires close analysis of the intersection of D&O and specific cyber insurance. Care must be taken to ensure that there are no coverage gaps for violations of the SEC disclosure rule. D&O policies may have a broad cyber incident exclusion. Many cyber policies exclude coverage for securities claims arising from cyber-related securities litigation or SEC regulatory matters. If neither policy excludes coverage, priority of payment and stacking issues may result. It is also vital to consider whether the individual directors' and officers' liability typically asserted in securities claims is or is not covered by entity cyber coverage.

Systemic cyber risk. Chubb defines a "systemic" cyber event as an occurrence "that could inflict widespread harm to many [insureds] due to shared elements or commonalities—often a single point of failure that is exploited. Put simply, it's a cyber incident that impacts multiple entities in a single act."[48] Lloyd's defines systemic risk as "a low likelihood, high impact risk which affects either a systemically important global enterprise or multiple sectors, societies, or national economies. They can be global in impact, often hitting billions of people simultaneously."[49] For example, a systemic event might involve the exploitation of a vulnerability in a file transfer software utilized by thousands of businesses to deploy malware, exfiltrate data, or cause business disruption. With so many clients exposed to loss by that single exploit, aggregate losses can be catastrophic.[50] Systemic risk—a result of risks spreading across systems vulnerable to concurrent cyberattacks—remains a critical problem. "Like a pandemic, a cyber-CAT event has no geographic boundaries or temporal limitations."[51] In 2023, Lloyd's conducted a study of the impact of a hypothetical cyberattack on a major financial services payments system, which yielded estimated losses of $3.5 trillion, $1.1 trillion of which was in the U.S.[52]

Carriers and insureds alike must understand their interconnections in the digital supply chain and develop coverage, as well as defense practices, to protect those key dependencies. By combining cyber insurance, security, and claims data, market participants can learn which technologies are so critical that, if exploited directly or through third-party connections, severe financial implications for policyholders would result. To control systemic risk, some cyber carriers have divided coverage options between basic or limited impact terms and separate catastrophic or widespread impact terms. Although not yet common, this approach would allow carriers to calibrate limits, sublimits, and retentions more precisely for either scenario.

Upstream, reinsurance predominantly remains a quota share market. Primary insurers cede a share of the premium and an equal share of the losses to reinsurers. However, most contracts include a cap on reinsurers' losses, which leaves significant tail exposure with the cedent, often without the premium to pay those claims. A more efficient use of capital involves reinsurers covering cyber on an event excess of loss basis. This model resembles catastrophic event excess of loss reinsurance for property, which protects insurers from an accumulation of losses due to a single event. Reinsurers are issuing cyber catastrophic loss bonds ($75–$80 million) to diffuse risk further.

This approach offers reinsurers greater margins for assuming tail volatility with the use of proportionately less capital. Reinsurers' return on equity increases, and the overall cyber insurance market becomes more efficient. To evolve, the reinsurance market needs a clear definition of what a systemic cyber event is and a consistent approach to modeling frequency and severity of those events.

Ransomware proliferation. As noted above, ransomware methods continue to adapt to defenses, and such attacks remain the largest source of cyber insurance claims by volume and frequency.[53] LockBit has been the dominant ransomware gang for the past three years, claiming exfiltration of 33 terabytes of banking information from a single private bank ransomware attack alone.[54] This challenge will require continuous improvement in cyber threat defenses. Ransomware activity by sophisticated and organized cybercriminal groups, often state-sponsored by Russia, China, North Korea, and Iran, will continue unabated in 2025. Double and triple extortion ransomware attacks are becoming more common and more costly for victims.

Early detection, data management practices, and mitigation will be key factors in reducing risk going forward.[55] Insurance companies must also be concerned with decisions to make ransom payments. On September 21, 2021, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) issued updated guidance on sanctions risks related to ransomware payments.[56] For the foreseeable future, legal scrutiny of insureds and insurers making ransom payments will increase, as ransom money funds larger and more frequent attacks.

Privacy regulation and claims, including biometrics. U.S. data privacy laws expanded monumentally in 2023 as state and federal governments made efforts to establish something like the European Union's General Data Protection Regulation (GDPR), which was implemented in 2018.[57] With the expanded scope and complexity of statutory cyber claims, carriers constricted coverage for investigation costs, fines, and penalties from regulatory claims. While the health care sector was heavily targeted in 2023 and 2024, most observers expect more privacy lawsuits to be filed in other industries, such as retail and financial services, in 2025 and beyond. Website tracking and meta pixel class action claims, as well as biometric claims, have expanded exclusions and limits.

There are a number of state privacy laws with government enforcement or private rights of action that impose specific duties on defined entities or persons. Prime examples include:

- California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA) (private right of action)[58]
- Connecticut Data Privacy Act (CTDPA) (attorney general enforcement)[59]
- Florida Computer Abuse and Recovery Act (private right of action)[60]
- Illinois Biometric Information Privacy Act (BIPA) (private right of action)[61]
- New York Department of Financial Services Cybersecurity Regulation (private right of action)[62]
- New York Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) (private right of action)[63]

Violations of privacy rules can also lead to class actions seeking class-wide relief for disclosure of personal identifying information (PII), financial or credit information, personal health information (PHI), biometric data, and data within the protection of the Health Insurance Portability and Accountability Act (HIPAA),[64] the HIPAA Privacy Rule,[65] and the HIPAA Security Rule.[66] Even if some statutes do not provide private rights of action, they serve to define legal duties that can be used to establish the standard of care or support negligence per se claims. The CCPA, with its regulations, is perhaps the most stringent state privacy protection regime in the U.S.[67] The CCPA's private right of action holds businesses accountable directly to California residents for security breaches resulting from a business's failure to implement and maintain reasonable security measures.[68] The regulatory requirements are expanding every year, often imposing inconsistent compliance obligations.[69]

These situations are likely to increase coverage litigation as well as direct and class privacy claims.[70] For example, BIPA coverage litigation has centered around three specific policy exclusions: the statutory violation, employment-related practices, and access or disclosure exclusions.

At the federal level, Congress began consideration of a national privacy protection law, the American Data Privacy and Protection Act (ADPPA), in 2022 with bipartisan support. The ADPPA proposes national standards for protection of personal information, including corporate and individual executive accountability provisions, with FTC, state attorney general, and private right of action enforcement mechanisms.[71] The ADPPA is now stalled, but the American Privacy Rights Act (APRA),[72] which incorporates some of the ADPPA concepts, is under consideration. While uniformity of standards would be helpful for compliance and assessment of risk, if adopted the APRA may or may not preempt state laws. APRA does authorize a private right of action for injunctive relief, actual damages, and attorney fees.

In the final days of his administration, President Biden issued a sweeping executive order on January 16, 2025, calling for enhanced measures for securing federal agencies and contractors and giving the federal government enhanced ability to sanction hackers who target critical infrastructure.[73] Vendors of software and computers will have to prove secure development practices to secure federal contracts. The National Institute of Standards and Technology (NIST) is to define standards for verifying compliance.

If implemented, both of these federal measures portend additional risks and potential claims that implicate cyber insurance coverage.

Artificial intelligence. In 2025, AI and predictive analytics' role in cybersecurity will expand as preventive measures. AI will be used to anticipate future cyber threats by analyzing historical data and current trends, extracting meaningful insights from vast and diverse datasets. AI's use in cybersecurity will expand to encompass automated response mechanisms and predictive analytics. Integrating AI into cybersecurity applications shows promise to improve threat detection and incident response. For instance, AI can identify anomalies or deviations that may indicate potential security threats and detect previously unidentified attacks.[74] AI excels in extracting meaningful insights from vast and diverse datasets. As the complexity of data and connectivity grows, AI will improve both effectiveness and efficiency in addressing new challenges. The coming year will likely show more innovation and automation in both back-office and front-office applications due to the increased adoption of AI and generative AI.

Conversely, AI may be leveraged to create more convincing and effective social engineering or phishing threats. Many expect politically motivated disinformation campaigns created through AI and coordinated with data breaches of fake information. The creation of large language models (LLMs) and AI has led to more convincing phishing messages, and the use of these LLMs to push malicious agendas will continue to ramp up in 2025. Obvious syntax and typographical errors may become a thing of the past. They can also be used to impersonate organizations or individuals and create fictitious engagement on social media platforms.

Integration of generative AI into business functions creates unprecedented opportunities and risks. Cybercriminals may target AI systems, which, if not properly secured, can result in data breaches and other information security events. As businesses increasingly rely on technology, the dependencies on these systems create vulnerabilities. Accidental system outages, data poisoning, and extraction attacks are some of the risks associated with AI technology. The breakneck speed of AI development complicates the industry's ability to anticipate and respond to challenges.

There are already over 200 cases pending involving AI and machine learning on a range of theories beyond cyber insurance.[75] There is no leading authority on whether AI claims are covered under cyber or other policies yet, but the industry is paying attention. Some carriers are developing specific AI policies or endorsements for AI developer and user coverage. These will likely need to be assessed in conjunction with any insureds' other policies.

Standardization of cyber and privacy risk standards. Cybersecurity and data privacy are related but distinct areas of concern. Cybersecurity may be defined as "[p]revention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation."[76] The Department of Homeland Security offers another comprehensive cybersecurity definition: "[t]he activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation."[77]

Data privacy,[78] although there are many definitions, generally refers to the ability of an individual to determine when, how, and to what extent their personal information is shared with or communicated to others. Stated another way, data or information privacy is concerned with the proper handling of data—consent, notice, and regulatory obligations. Data privacy, with variations in domestic and international legal frameworks, typically involves practices to secure personal data or PII, such as names, addresses, Social Security numbers, and credit card numbers from unauthorized access, corruption, or theft. It also extends to other valuable or confidential data, including financial data, intellectual property, and PHI. In addition to regulatory requirements, industry guidelines often govern data privacy and data protection initiatives.

Accordingly, there is a dizzying array of cyber and privacy risk standards domestically and internationally, which complicate cyber and privacy insurance underwriting. In February 2024, NIST issued its updated and expanded NIST Cybersecurity Framework (CSF) 2.0.[79] The International Standards Organization (ISO) has published its information security, cybersecurity, and privacy protection standards, which it promotes as the "world's best-known standard for information security management systems."[80] Harmonization of these requirements would help underwriting assessments and reduce the threat of exposure or noncompliance and the cost of compliance.

Adapting to an Evolving Cyber Threat Landscape

No one expects cyber insurance to complete maturation or resolve all challenges in 2025. The trends and volatility of the cyber landscape are likely to continue for years to come. Despite best efforts to stop them, threat actors will pivot, develop new tactics, and identify new vulnerabilities as attack surfaces grow. Insurers, however, are poised to gain a deeper understanding of the risks their insureds face, including insights into how vulnerabilities expose clients to loss, how

threat actors behave, and how internet exposures contribute to cyberattacks.

Together, in 2025 and beyond, carriers and insureds will confront more sophisticated cyber threats and attacks while adapting to the evolving regulatory environment and increasing financial impact of cyber incidents, despite growing awareness and understanding of cyber risks. This will require insureds to prioritize using their capital to fight cyber threats, meeting certification requirements that demonstrate resilience (e.g., ISO 27001, HITRUST, Baldrige, NIST), and carefully balancing primary, excess, and self-insured components of their insurance protection to address their specific needs. Insureds must keep their incident response plans updated, strengthen vendor oversight, and align data governance with stricter underwriting requirements.

Despite the changing cyber threat landscape, the cyber insurance market will likely continue to expand in 2025, as the industry gains insight into how threats become claims and how to prevent and mitigate their effects. For their part, insurers must continue to provide effective resources to help insureds by offering holistic management services that enable organizations to manage cyber risks proactively and contain the impact of any breach. These include cybersecurity assessments, threat intelligence, incident response planning and capabilities, and employee training.

At the underwriting level, insurance companies and allied data analytics firms must continue to drill down on data-driven risk assessments to make cyber insurance more efficient and less costly over time. Further, carriers must tailor policies for specific industries, such as health care, finance, or manufacturing, to address their unique risks and compliance requirements. Market offerings and pricing must be profitable but accessible to provide what policyholders need as part of a meaningful risk management program. ◄

Notes

1. Roxanne Libatique, *Cyber Tops Business Threats in 2025—Allianz*, Ins. Bus. (Jan. 16, 2025), https://www.insurancebusinessmag.com/ca/news/catastrophe/cyber-tops-business-threats-in-2025--allianz-520741.aspx.

2. Verizon, 2024 Data Breach Investigations Report (2024), https://www.verizon.com/business/resources/reports/2024-dbir-executive-summary.pdf.

3. Press Release, Allianz, New Data Privacy Trends Help Drive Growth in Frequency and Severity of Large Cyber Claims (Oct. 9, 2024), https://commercial.allianz.com/news-and-insights/news/cyber-risk-trends-2024.html.

4. Allianz, Cyber Security Resilience in 2024 (2024), https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/cyber-security-trends-2024.pdf.

5. *Id.* at 12.

6. James Coker, *Cyber Insurance Market to Be Worth Over $90bn by 2033*, Infosecurity Mag. (Jan. 10, 2024), https://www.infosecurity-magazine.com/news/cyber-insurance-market-worth/.

7. *Id.*

8. Laura Bohnert, *The Anatomy of a Cyber Insurance Policy*, Beyond Tr. (July 20, 2023), https://www.beyondtrust.com/blog/entry/anatomy-of-a-cyber-insurance-policy.

9. *Reality Check on the Future of the Cyber Insurance Market*, Swiss Re (Nov. 18, 2024), https://www.swissre.com/risk-knowledge/advancing-societal-benefits-digitalisation/about-cyber-insurance-market.html.

10. John Farley, Gallagher, 2025 Cyber Insurance Market Conditions Outlook: Cyber Market Stabilization as Cyber Risks Evolve (2025), https://www.ajg.com/-/media/files/gallagher/us/news-and-insights/2025/2025-cyber-insurance-market-conditions-outlook.pdf; *Cyber Insurance Market to Expand as Risks Evolve: Gallagher*, Ins. J. (Jan. 17, 2025), https://www.insurancejournal.com/news/national/2025/01/17/808663.htm.

11. Aon, U.S. Cyber Market Update: 2023 U.S. Cyber Insurance Profits and Performance (2024), https://www.aon.com/getmedia/4afa8654-6534-48c3-91c1-b27d57170cdb/20240806-US-Cyber-Market-Update.pdf.

12. David Anderson, *Does Cyber Insurance Pay Out?*, Woodruff Sawyer (Dec. 11, 2024), https://woodruffsawyer.com/insights/cyber-insurance-pay-out.

13. Gavin Souter, *Insurers, Brokers Forecast More Rate Hikes*, Bus. Ins., Nov. 2023, at 11, https://www.businessinsurance.com/insurers-brokers-forecast-more-rate-hikes/.

14. *Special Report: Cyber Risk & Professional Liability*, Bus. Ins., Nov. 2023, at 26.

15. *Insurance Marketplace Realities 2025—CyberRisk*, WTW (Oct. 4, 2024), https://www.wtwco.com/en-us/insights/2024/10/insurance-marketplace-realities-2025-cyber-risk.

16. Woodruff Sawyer, Looking Ahead: Cyber Insurance Trends for 2024 (2024).

17. *Id.* at 8.

18. *Id.* at 10.

19. *Special Report*, *supra* note 14, at 26.

20. Norton Rose Fulbright, 2024 Annual Litigation Trends Survey 7 (2024), https://www.nortonrosefulbright.com/-/media/files/nrf/nrfweb/knowledge-pdfs/norton-rose-fulbright---2024-annual-litigation-trends-survey.pdf (annual survey of corporate counsel).

21. Press Release, *supra* note 3.

22. Press Release, Bloomberg L., New Report from Bloomberg Law Highlights Surge in Ransomware Litigation (July 29, 2024), https://pro.bloomberglaw.com/insights/company-news/new-report-from-bloomberg-law-highlights-surge-in-ransomware-litigation.

23. Cal. Civ. Code § 1798.115.

24. 740 Ill. Comp. Stat. 14/20.

25. *See, e.g.*, Fredric D. Bellamy & Ashley N. Fernandez, *Illinois Court Decisions Acknowledge Biometric Privacy Act's Damages a Potential Business Killer*, Reuters (Apr. 17, 2023), https://www.reuters.com/legal/legalindustry/illinois-court-decisions-acknowledge-biometric-privacy-acts-damages-potential-2023-04-17/.

26. 216 N.E.3d 918 (Ill. 2023).

27. S. 2979, 103d Gen. Assemb. (Ill. 2024) (Pub. Act 103-0769).

28. Farley, *supra* note 10.

29. Steve Alder, *UHG Increases Change Healthcare Data Breach Victim Count to 190 Million*, HIPAA J. (Jan. 25, 2025), https://www.hipaajournal.com/change-healthcare-responding-to-cyberattack/ (UnitedHealth Group's updated numbers make the breach 2.5 times the largest prior health care breach experienced by Anthem).

30. Robert Lemos, *Insurers Use Claims Data to Recommend Cybersecurity Technologies*, Dark Reading (Feb. 22, 2024), https://www.darkreading.com/cyber-risk/insurers-claims-data-recommend-cybersecurity-technologies.

31. *Market Bulletin: State-Backed Cyber Attack Exclusions*, Lloyd's of London (Aug. 16, 2022), https://assets.lloyds.com/media/35926dc8-c885-497b-aed8-6d2f87c1415d/Y5381%20Market%20Bulletin%20-%20Cyber-attack%20exclusions.pdf.

32. IBM, 2023 Cost of a Data Breach Report (2023) [hereinafter 2023 IBM Report].

33. *Id.* at 5.

34. IBM, Cost of a Data Breach Report 2024 (2024), https://table.media/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf.

35. Ransomware is often defined as a threat or series of threats to commit or continue an attack unless the policyholder pays a ransom.

36. 2023 IBM Report, *supra* note 32, at 13.

37. *Cyber Insurance Market Size, Share & Industry Trends Analysis, by Insurance Type (Standalone and Tailored), by Coverage Type (First-Party and Liability Coverage), by Enterprise Size (SMEs and Large Enterprise), by End-User (Healthcare, Retail, BFSI, IT & Telecom, Manufacturing, and Others), and Regional Forecast, 2024–2032*, Fortune Bus. Insights (Jan. 20, 2025), https://www.fortunebusinessinsights.com/cyber-insurance-market-106287 (the compound annual growth rate is forecast to be 26% for 2023 to 2030).

38. *US Insurance Market Rates*, Marsh (2024), https://www.marsh.com/en/services/international-placement-services/insights/us-insurance-rates.html (lower rates in 2024; approximately 20% of clients purchased additional limits).

39. Coker, *supra* note 6.

40. Robert Lemos, *Cyber Insurance: A Few Security Technologies, a Big Difference in Premiums*, Dark Reading (Aug. 29, 2024), https://www.darkreading.com/threat-intelligence/cyber-insurance-security-technologies-premiums (listing key cybersecurity technologies that prevent loss).

41. *Id.*

42. OFAC, in particular, has raised the potential for firms and individuals paying ransom to risk potential civil and criminal sanctions for facilitating ransomware payments. *See Cyber-Related Sanctions*, Off. of Foreign Assets Control, https://ofac.treasury.gov/sanctions-programs-and-country-information/sanctions-related-to-significant-malicious-cyber-enabled-activities (last visited Feb. 1, 2025).

43. *Market Bulletin*, *supra* note 31.

44. Lloyd's published updated versions of its clauses in January 2023. *Cyber War & Cyber Operation Clauses Updated*, Lloyd's Mkt. Ass'n (Jan. 20, 2023), https://www.lmalloyds.com/LMA/News/LMA_bulletins/LMA_Bulletins/LMA23-002-PD.aspx. Current versions of all Lloyd's approved policy language may be found in its Wordings Repository (http://www.lloydswordings.com/).

45. Press Release, U.S. Sec. & Exch. Comm'n, SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies (July 26, 2023), https://www.sec.gov/newsroom/press-releases/2023-139; Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 88 Fed. Reg. 51896 (Aug. 4, 2023).

46. Christian Auty et al., *The SEC Is Watching: Four Companies Charged for Misleading Cyber Disclosures*, JD Supra (Nov. 7, 2024), https://www.jdsupra.com/legalnews/the-sec-is-watching-four-companies-4902861/.

47. Jennifer Lee et al., *Key Takeaways from Recent SEC Cybersecurity Enforcement Actions*, Harv. L. Sch. F. on Corp. Governance (Oct. 29, 2024), https://corpgov.law.harvard.edu/2024/10/29/key-takeaways-from-recent-sec-cybersecurity-enforcement-actions/.

48. *A Better Way to Define and Insure Systemic Cyber Events*, Chubb, https://www.chubb.com/uk-en/businesses/resources/a-better-way-to-define-and-insure-systemic-cyber-events.html (last visited Feb. 1, 2025).

49. Press Release, Lloyds, Lloyd's Systemic Risk Scenario Reveals Global Economy Exposed to $3.5trn from Major Cyber Attack (Oct. 18, 2023), https://www.lloyds.com/about-lloyds/media-centre/press-releases/lloyds-systemic-risk-scenario-reveals-global-economy-exposed-to-3.5trn-from-major-cyber-attack.

50. Major events such as WannaCry and SolarWinds, and the CrowdStrike and CDK Global episodes, are analogous to a major tropical storm, and risk ratings are difficult as the differences in each event and resulting losses are complex.

51. *A Better Way to Define and Insure Systemic Cyber Events*, *supra* note 48.

52. Press Release, *supra* note 49.

53. Bloomberg L., Ransomware Attacks: Litigating a Growing Threat 9 (2024).

54. Press Release, U.S. Dep't of the Treasury, United States Sanctions Affiliates of Russia-Based LockBit Ransomware Group (Feb. 20, 2024), https://home.treasury.gov/news/press-releases/jy2114.

55. Michelle Drolet, *Eight Cybersecurity Trends to Watch for 2024*, Forbes (Dec. 26, 2023), https://www.forbes.com/sites/forbestechcouncil/2023/12/26/eight-cybersecurity-trends-to-watch-for-2024/.

56. Press Release, U.S. Dep't of the Treasury, Treasury Takes Robust Actions to Counter Ransomware (Sept. 21, 2021), https://home.treasury.gov/news/press-releases/jy0364.

57. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46 EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.

58. Cal. Civ. Code §§ 1798.100 *et seq.*, 1798.145.

59. Conn. Gen. Stat. § 42-516-522.

60. Fla. Stat. §§ 668.801–.805.

61. 740 Ill. Comp. Stat. 14/1 *et seq.*

62. N.Y. Comp. Codes R. & Regs. tit. 23, §§ 500.0 *et seq*.

63. N.Y. Gen. Bus. Law § 899-bb.

64. 42 U.S.C. §§ 1320d *et seq*.

65. 45 C.F.R. pts. 160, 164.

66. *Id*. pt. 164.

67. Cal. Civ. Code § 1798.192; Cal. Code Regs. tit. 11, § 7000.

68. Cal. Civ. Code § 1798.150(a)(1).

69. The National Conference of State Legislatures (NCSL) publishes an annual survey of cybersecurity legislation. *See, e.g.*, *Cybersecurity 2024 Legislation*, Nat'l Conf. of State Legislatures, https://www.ncsl.org/technology-and-communication/cybersecurity-2024-legislation (last updated Jan. 30, 2025). The International Association of Privacy Professionals (IAPP) maintains developments in state data privacy laws and proposed legislation. *US State Privacy Legislation Tracker*, Int'l Ass'n of Priv. Pros., https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ (last updated Feb. 3, 2025).

70. Lisa Burden, *Biometric Privacy Settlements Spark Insurance Coverage Battles*, Legal Dive (Feb. 26, 2024), https://www.legaldive.com/news/biometric-privacy-settlements-spark-insurance-coverage-battles-BIPA-Wilson-Elser-anderson-kill/708562/.

71. H.R. 8152, 117th Cong. (2022).

72. H.R. 8818, 118th Cong. (2024).

73. Jenna McLaughlin, *Biden Issues an 11th Hour Executive Order Aimed at Strengthening U.S. Cybersecurity*, WUSF (Jan. 16, 2025), https://www.wusf.org/2025-01-16/biden-issues-an-11th-hour-executive-order-aimed-at-strengthening-u-s-cybersecurity.

74. Danielle Braff, *How to Combat Cybersecurity Threats When Using Artificial Intelligence*, A.B.A. J. (Aug. 26, 2024), https://www.abajournal.com/web/article/using-ai-heres-how-to-combat-cybersecurity-threats (according to Cornell University researchers, if properly trained, AI can detect network intrusion with 99.9% accuracy and corrupted emails with 98% accuracy).

75. Farley, *supra* note 10.

76. *Cybersecurity*, NIST Comput. Sec. Res. Ctr., https://csrc.nist.gov/glossary/term/cybersecurity (last visited Feb. 1, 2025).

77. *Vocabulary*, Nat'l Initiative for Cybersecurity Careers & Stud., http://niccs.us-cert.gov/glossary (last visited Feb. 1, 2025).

78. According to the IAPP, in 2025, 19 states have some form of state consumer privacy protection laws. *US State Privacy Legislation Tracker*, *supra* note 69; *see also Which States Have Consumer Data Privacy Laws?*, Bloomberg L. (Sept. 10, 2024), https://pro.bloomberglaw.com/insights/privacy/state-privacy-legislation-tracker/.

79. Press Release, Nat'l Inst. of Standards & Tech., NIST Releases Version 2.0 of Landmark Cybersecurity Framework (Feb. 26, 2024), https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework.

80. *ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements*, ISO (Oct. 2022), https://www.iso.org/standard/27001.