



Cyber Solutions for Insurance Professionals: BUILDING RESILIENCE AGAINST EMERGING THREATS

Authors: **Richard W. Boone Jr.** | October 2026

The magnitude and nature of the cyber risks that businesses face, and the types of coverage available for them, continue to grow. In less than a decade, insurance coverage for cyber risk evolved from an add-on product to a core coverage for nearly every type of business. It has continued to evolve since. The cyber landscape in 2026 is now defined by a convergence of emerging threats and evolving coverage challenges that demand attention from insurance professionals at every level.

Agentic artificial intelligence, quantum computing vulnerabilities, deepfakes, and regulatory volatility are reshaping the threat environment. At the same time, insurers are adapting their underwriting strategies, claims handling practices, and policy language to close AI-related coverage gaps and respond to new patterns of cyber litigation. For insurance professionals, understanding these developments is essential because the emerging threats and coverage questions have direct implications for policy design, pricing, claims management, and the long-term sustainability of cyber portfolios.

THE 2026 CYBER LANDSCAPE

The magnitude of the cyber threats faced by insureds continues to intensify. Several widely cited statistics illustrate the scope of the challenge. The International Monetary Fund forecasts that global cybercrime costs will reach \$23 trillion by 2027, representing a 175 percent increase from 2022.¹ While most reported losses from individual cyberattacks remain relatively small, the risk of extreme losses caused by cyber incidents has been growing.² NordStellar has reported that the frequency of ransomware attacks increased approximately 45 percent in 2025 from the prior year, with December 2025 setting a two-year record of 1,004 incidents in a single month.³

Global cyber insurance premiums reached approximately \$15.3 billion at year-end in 2024, according to Munich Re, and the market is projected to continue growing significantly, reflecting both increased demand and an expanding universe of covered risks.⁴ Perhaps most telling is a January 2026 Allianz survey of more than 3,300 risk management professionals. It found that AI-related risk jumped from the number ten business risk concern to the number two concern in just one year. Both cyber risk and AI now rank as top five concerns for companies in almost every industry sector.⁵

These figures build on a trajectory that has been apparent for several years. Indeed, cyber risk has consistently been rated as the top concern in nearly every insurance industry survey, driven in large part by the tremendous increase in ransomware incidents, the rising number of business email compromise scams, and the expanding cost of each individual incident. The average global cost of a data breach was \$4.45 million in 2023, the highest average on record at that time and a 15 percent increase over the prior three years.⁶ That number has risen further to \$4.99 million in 2025.⁷

I. THE BIG SHIFTS: WHAT IS NEW IN 2026

Against the overall backdrop of ever-expanding risks, several significant developments have emerged as defining factors in 2026. Agentic AI, quantum computing threats, increasingly sophisticated deepfakes, and a volatile regulatory environment are each creating new exposures that insurers and reinsurers must account for in their underwriting and claims strategies.

Cyber Solutions for Insurance Professionals: Building Resilience Against Emerging Threats

A. AGENTIC AI AND SHADOW AI

Until recently, much of the industry's attention was focused on the risks of generative AI. With generative AI now widespread in the workplace, the conversation in 2026 has moved to what is known as "agentic AI," a term that refers to autonomous AI systems capable of taking actions, making decisions, and interacting with other systems without direct human oversight. An additional threat is the growing phenomenon of "Shadow AI," where employees, in an effort to increase productivity, adopt AI tools that can autonomously access systems, modify data, or send emails without the knowledge or approval of IT or data security departments. These result in new, unmonitored vulnerabilities and potential regulatory issues about which insured companies may not even be aware.

The fundamental concern has always been that the greater the use of AI, the greater the potential risk for cyber insurers. Agentic AI heightens that concern because these systems operate with a degree of autonomy that traditional cybersecurity controls were not designed to address. Indeed, one of the most significant risks posed by generative AI has been its authorized and unauthorized use in the workplace. Many companies and employees do not fully understand these tools or how they work. Risks include uploading sensitive company data into platforms like ChatGPT, unwitting copyright infringement when AI generates content derived from protected works, and the danger of employees producing fictitious work product. Well-publicized instances of attorneys submitting AI-generated briefs citing nonexistent cases illustrate the potential consequences. Shadow AI is the natural extension of that problem, now compounded by the fact that the tools themselves can take independent action.

B. ADVANCEMENTS IN QUANTUM COMPUTING

Quantum computing is a type of technology that uses the principles of atomic physics to solve complex problems exponentially faster than traditional computers. Instead of standard "bits," which store information as either a zero or a one, quantum computers use "qubits" that can represent multiple states at once, allowing them to process vast amounts of data simultaneously. Experts now predict that advances in quantum computing will break the encryption methods organizations currently rely on to secure data and systems by 2032, and possibly sooner.⁸

The threat may be even more imminent than that timeline suggests, because so-called "harvest now, decrypt later" attacks are already believed to be happening. In these attacks, threat actors steal encrypted data today with the intention of decrypting it once quantum computing matures sufficiently. A report from the Federal Reserve Board has examined this precise risk in the context of distributed ledger networks (like Bitcoin) and other sensitive data infrastructure.⁹ For the insurance industry, the implication is that data stolen in a breach today could become a source of liability years from now, once quantum decryption becomes feasible.

C. DEEPFAKE AND VOICE-CLONING ESCALATION

AI-powered deepfakes, which are fabricated videos and audio recordings generated by artificial intelligence, are a rapidly growing threat. Cybercriminals are using increasingly accessible AI tools to create convincing fake videos and audio recordings for use in social engineering schemes. One source reports that deepfake files surged from 500,000 in 2023 to an estimated 8 million by 2025, and that there were more deepfake incidents in the first quarter of 2025 alone (179) than in all of 2024 (150).¹⁰

Cyber Solutions for Insurance Professionals: Building Resilience Against Emerging Threats

The potential for real-world financial harm is already well established. In one high-profile case from 2024, the Hong Kong office of a UK engineering firm lost \$25 million when an employee was tricked by a multi-person videoconference involving deepfake impersonations of several company executives.¹¹ Deepfakes represent a particularly dangerous subset of social engineering fraud because AI-powered tools can now impersonate people on live audio and video calls, and these tools are expected to become more sophisticated and accessible over time.

D. REGULATORY VOLATILITY

The cyber regulatory landscape has shifted significantly in the past year. The SEC's November 2025 decision to drop its landmark civil fraud case against SolarWinds was widely seen as a shift in the agency's enforcement approach. However, its enforcement of cybersecurity disclosure rules on Form 8-K and in annual reports apparently remains a priority.¹²

In this regard, the SEC announced the establishment of its Cyber and Emerging Technologies Unit in February 2025, which listed compliance with cybersecurity rules and regulations as a priority area. Globally, provisions of the EU AI Act took effect in 2026, with potential fines of up to €35 million or 7 percent of global turnover.¹³ This regulatory environment creates a complex compliance landscape for multinational insureds and, by extension, for the carriers who cover them.

II. CONTINUING TRENDS

While the threat environment continues to evolve, several persistent trends remain central to the cyber risk landscape in 2026. Business email compromise, ransomware, the expanding patchwork of state privacy laws, supply chain vulnerabilities, and heightened regulatory enforcement continue to drive claim frequency and severity across the market.

A. BUSINESS EMAIL COMPROMISE AND FUNDS TRANSFER FRAUD

Business email compromise, commonly known as BEC, and funds transfer fraud remain some of the most financially damaging cyber threats facing organizations. The FBI reports that BEC attacks resulted in close to \$2.8 billion in losses in 2024¹⁴ and have caused over \$55 billion in domestic and international losses over the past decade.¹⁵ The frequency of BEC attacks has continued to increase, with a reported 33 percent increase in losses from 2023.¹⁶ On the claims side, Coalition's 2025 Cyber Claims Report indicates that BEC and funds transfer fraud events accounted for 60 percent of all cyber insurance claims, a trend that has generally held steady for the past three years.¹⁷

A key development is that ever-improving generative AI tools are being used to increase the sophistication of BEC schemes, allowing attackers to create more convincing phishing emails. This reflects a broader trend in which generative AI fuels more sophisticated social engineering and phishing attempts, making the fraud harder to identify because cybercriminals can craft more convincing emails and messages that appear to come from trusted sources. The scale of this shift is striking: one industry source reported that phishing attacks increased by 1,265 percent, driven largely by the growth of generative AI,¹⁸ while cloud intrusions rose by 75 percent,¹⁹ and distributed denial of service attacks increased by 31 percent in the final quarter of 2025 alone,²⁰ with cybercriminals launching an average of 44,000 such attacks daily.²¹

Cyber Solutions for Insurance Professionals: Building Resilience Against Emerging Threats

B. RANSOMWARE EVOLUTION

Ransomware continues to be the leading factor driving claim severity in the cyber insurance market.²² Ransomware groups have broadened their target base from large corporations to mid-size and even small companies. Anecdotally, threat actors appear to be getting better at covering their tracks, making it increasingly difficult for forensic investigators to determine how a system was breached. Recent data shows ransomware still present in approximately 44 percent of reported breaches,²³ and total ransomware payments were predicted and likely to exceed \$900 million in 2025, up slightly from \$892 million in 2024.²⁴ However, average ransom demands fell 22 percent, though the average demand is still approximately \$1.1 million.²⁵

A notable shift is that, according to Coalition, only 44 percent of its policyholders chose to pay a ransom in 2025, and the insurer successfully negotiated a 60 percent reduction in payment based on the initial demand.²⁶ Additionally, attackers are increasingly moving from encrypting data to simply exfiltrating it and threatening publication.²⁷ Ransomware remains the primary driver of business interruption loss, accounting for roughly 81 percent of those claims and averaging \$1.1 million per loss event for small- to medium-sized companies with under \$2 billion in revenue.²⁸

C. THE EXPANDING STATE PRIVACY LAW PATCHWORK

The proliferation of comprehensive privacy laws at the state level continues unabated. As of January 2026, 20 states now have comprehensive privacy laws in effect.²⁹ California remains at the forefront, with new California Consumer Privacy Act (CCPA) regulations that took effect on January 1, 2026, covering cybersecurity audits, risk assessments, and automated decision-making technology.³⁰ Connecticut lowered the applicability threshold for its data privacy law from businesses with data for 100,000 consumers to 35,000 consumers.³¹ Colorado also eliminated the 60-day cure in its data privacy law, meaning that the Colorado Attorney General and District Attorneys now have the discretion to immediately enforce penalties for violations without first providing businesses an opportunity to correct noncompliance.³² These amendments mean that thousands of additional businesses are now within the scope of state privacy obligations, and each new state law creates potential sources of regulatory investigation, civil litigation, and cyber policy claims.

The state privacy patchwork exists alongside a complex framework of federal laws that may also be implicated by a cyber incident, including the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act (FCRA), the Electronic Communications Privacy Act (ECPA), the Children's Online Privacy Protection Rule, and the Video Privacy Protection Act (VPPA), among others. Globally, multinational insureds must also contend with Europe's General Data Protection Regulation (GDPR), which requires companies to obtain certain permissions before sharing data and gives individuals rights to access, delete, or control the use of their data. The protections afforded under the GDPR are generally more extensive than those provided under any U.S. state or federal law, and noncompliance can give rise to significant fines and enforcement actions that may trigger coverage obligations under cyber and other liability policies.

The California Privacy Protection Agency's enforcement actions have resulted in record settlements, including a \$2.75 million settlement with Disney in early 2026 for failure to provide compliant opt-out rights.³³ Some of the largest areas of concern for cyber class actions involve statutes like BIPA in Illinois and the CCPA in California, because both provide for statutory damages that can produce staggering potential recoveries for a class of any size. For example, one BIPA case resulted in a verdict against railroad company BNSF for \$228 million, based on just 45,600 alleged violations at \$5,000 per violation. Although BIPA was since amended (in August 2024)

Cyber Solutions for Insurance Professionals: Building Resilience Against Emerging Threats

to cap statutory damages to a “per-person” rather than “per-scan/violation” basis (meaning an entity is liable for at most one recovery per person, regardless of how many times they scan or disclose a person’s biometric data), potential liability remains significant.

D. SUPPLY CHAIN AND THIRD-PARTY VENDOR RISK

Supply chain attacks have become a central concern in cyber insurance, with attackers increasingly bypassing direct defenses to exploit vulnerabilities in vendors, suppliers, and service providers. The Verizon 2025 Data Breach Investigations Report found that 30 percent of breaches involved a third party, doubling from 15 percent the prior year.³⁴ Other research indicates that 35.5 percent of all data breaches now originate from third-party compromises.³⁵

The retail, hospitality, and consumer goods sector is especially exposed, with 54.2 percent of breaches in those industries linked to third-party vendors.³⁶ Third-party breaches cost an average of \$4.91 million, exceeding the global breach cost average.³⁷ Cybercriminals have long targeted third-party vendors as entry points into larger, more secure networks. Complicating defensive efforts is an increasing reliance on third-party code and AI-assisted development tools, which create new vulnerabilities that can make supply chain attacks easier to execute, harder to detect, and more costly when they occur.

E. EXPANDING REGULATORY ENFORCEMENT

Beyond the SEC developments discussed above, several other regulatory bodies have significantly increased their enforcement of cybersecurity obligations in recent years, creating additional compliance exposure for insureds and, by extension, for their carriers. The Federal Trade Commission has become increasingly active in regulating cybersecurity practices, having settled enforcement actions against companies including GoodRx and BetterHelp for pixel tracking violations,³⁸ and against Chegg and Drizly for inadequate cybersecurity practices that led to data breaches.³⁹

The New York Department of Financial Services Cybersecurity Regulation, which requires New York insurance companies, banks, and other regulated financial services institutions to assess their cybersecurity risk profiles, was also amended in November 2023, imposing heightened requirements on the largest institutions and additional notice obligations in the event of an incident.⁴⁰

AI-specific legislation has also accelerated rapidly at the state level. In the 2024 legislative session alone, at least 45 states introduced AI-related bills, and 31 states adopted resolutions or enacted legislation, including Colorado’s statute protecting consumers from algorithmic discrimination in high-risk AI systems and New Hampshire’s law criminalizing the fraudulent use of deepfakes.⁴¹ These regulatory developments create potential sources of enforcement actions, civil litigation, and insurance claims that insurers must account for in their underwriting and claims handling.

F. INTERNET OF THINGS VULNERABILITIES

The proliferation of Internet-connected devices, commonly referred to as the “Internet of Things” or “IoT,” continues to expand the cyber threat surface for businesses across industries. IoT devices include everything from networked security cameras and electronic access systems to industrial sensors and smart building controls. These devices are embedded with software that connects them to the Internet and allows them to exchange data with other systems. They often have significant security flaws, including weak default

Cyber Solutions for Insurance Professionals: Building Resilience Against Emerging Threats

credentials, infrequent software updates, and limited encryption, which can serve as entry points for attackers seeking access to broader corporate networks.

Real-world incidents have demonstrated the severity of this risk. In one widely reported case, hackers accessed the systems of an Austrian hotel through its electronic key system, locking the hotel out of its computers and guests out of their rooms while demanding a ransom.⁴² In another, an explosion at a Turkish pipeline was potentially linked to hackers who gained access to critical infrastructure systems through surveillance camera software.⁴³ As organizations deploy more connected devices without corresponding security controls, IoT vulnerabilities are likely to generate an increasing number of cyber insurance claims, particularly in sectors like healthcare, manufacturing, and hospitality where IoT adoption is most advanced.

G. THREAT ACTORS WEAPONIZING REGULATORY OBLIGATIONS

A trend that has grown more pronounced in recent years is the use of growing cyber regulations by threat actors themselves. In ransomware and data exfiltration attacks, threat actors increasingly threaten to report the breach to regulators, notify affected individuals, or publicize the incident if the victim does not pay.⁴⁴ The proliferation of mandatory disclosure requirements at the state, federal, and international levels gives these threats real teeth, because a delayed or mishandled regulatory response can compound the financial and reputational harm of the underlying incident. Insurers should be aware that this tactic can accelerate the timeline from breach to regulatory exposure and litigation, increasing the overall cost of a claim.

H. EMERGING SOCIAL ENGINEERING SCHEMES

While business email compromise and deepfake fraud continue to dominate the social engineering threat landscape, newer schemes are also emerging. One such scheme, colloquially known as “pig butchering,” involves threat actors building trust with victims over extended periods, often through social media or messaging platforms, before inducing them to transfer substantial sums of money, typically under the guise of a fraudulent investment opportunity.⁴⁵

Some threat actors have also returned to older techniques, including traditional mail, to initiate fraud schemes that ultimately lead to cyber-related losses.⁴⁶ These evolving tactics underscore the importance of comprehensive social engineering coverage and the need for underwriters to assess not only an insured’s technical cyber defenses but also its employee training and awareness programs.

PROACTIVE UNDERWRITING AND CLAIMS STRATEGIES

Effective management of cyber risk requires more than reactive claims handling. It demands a proactive approach that begins at the underwriting stage, where gathering better risk information can materially improve portfolio outcomes, and extends through incident response readiness, litigation preparedness, and the pursuit of recoveries when third-party failures contribute to a loss.

I. UPDATING THE UNDERWRITING APPLICATION

One of the most impactful things insurers can do to address the evolving cyber risk is gather better information during the underwriting process regarding the risks faced by each prospective insured. The underwriting application is critical in this regard. Asking the right questions on the application not only ensures

Cyber Solutions for Insurance Professionals: Building Resilience Against Emerging Threats

that important issues are addressed but also provides a potential basis to void coverage if the insured's representations later prove false.

In 2026, AI-related representations may be the most important ones on the application. This heightened focus reflects the reality that AI adoption is transforming how insurers evaluate cyber risk, with underwriters increasingly examining whether organizations have robust AI governance frameworks and oversight mechanisms in place. Applications should now include targeted questions about an insured's use of AI, including whether the insured has deployed agentic AI, what governance frameworks are in place, and whether the insured has a policy addressing unauthorized or Shadow AI use by employees.

Sophisticated practitioners have for some time been asking more detailed questions on their applications regarding cyber risks, and representations on those applications are becoming more critical. Insurers are also making increased use of third-party verification services to independently assess an applicant's cybersecurity posture, rather than relying solely on self-reported information in the application.

Forward-thinking underwriters should also begin asking about planning for post-quantum cryptography. In August 2024, the National Institute of Standards and Technology finalized its first post-quantum cryptography standards (designated FIPS 203, 204, and 205),⁴⁷ and federal guidance now calls for migration from quantum-vulnerable algorithms by 2035.⁴⁸ Even if migration to these new standards is years away, underwriters may wish to inquire whether insureds have begun conducting cryptographic inventories, developing migration roadmaps, or coordinating with vendors regarding post-quantum readiness. This signals a proactive approach to managing an evolving risk that, if left unaddressed, could expose organizations to significant future liability.

Given the persistent and growing threat of supply chain attacks, underwriters should also ask detailed questions about how insureds vet, monitor, and contractually allocate risk with their vendors. Specific areas of inquiry may include whether the insured maintains a current inventory of critical technology vendors, what due diligence processes are conducted during vendor onboarding, how the insured monitors the security posture of key suppliers on an ongoing basis, and whether vendor contracts include provisions addressing incident notifications, audit rights, security requirements, and indemnification.

Insurers should also consider whether the insured has developed contingency plans for potential vendor outages or compromises, as the ability to respond quickly to a supply chain incident can significantly reduce the ultimate cost of a claim.

II. CLAIMS HANDLING: STAYING AHEAD OF THE CURVE

While robust underwriting can help select better risks, even the best-underwritten policies will generate claims. The speed and effectiveness of the claims response often determines whether a manageable incident becomes a catastrophic loss.

The claims handling response in the first 24 to 72 hours of a ransomware event can significantly affect the ultimate cost of the incident. Most major insurers maintain pre-approved panels of forensic investigators, breach counsel, crisis communications firms, and ransom negotiators ready to deploy. However, these resources are only effective if insureds know they exist and how to engage them. Insurers should provide policyholders with a clear incident response guide at policy inception that identifies available panel vendors, explains how to engage them quickly, and clarifies any approval processes or coverage considerations. An insured who learns about available resources for the first time during a crisis is already behind.

Cyber Solutions for Insurance Professionals: Building Resilience Against Emerging Threats

Targeted phishing simulations and resilience tabletop exercises are no longer optional; they are essential for both insureds and the carriers that insure them. These exercises help everyone involved understand how they will respond when, not if, an event occurs. Insurers should encourage and, where possible, facilitate tabletop exercises that include not only the insured's internal team but also the insurer's claims personnel and panel vendors, so that all parties understand their roles and can coordinate seamlessly during an actual incident.

One issue that continues to arise is how to protect the forensic investigation report of a cyber event as attorney work product. Insurers and experienced breach counsel understand how to maintain the privilege, but the challenge is communicating that knowledge to insureds and involving counsel in the incident response from the very beginning. The critical workflow is for the insured to contact breach response counsel first, before conducting any internal investigation or remediation, so that counsel can coordinate all forensic and remediation efforts under the protection of attorney-client privilege and work product doctrine.

If an insured begins investigating or remediating on its own before counsel is engaged, the resulting reports and communications may not be protected. They then become a roadmap for plaintiffs in subsequent litigation. Understanding how to protect the investigation report as attorney work product is one of the hallmarks of sophisticated cyber practice.

III. PREPARING FOR LITIGATION AND PURSUING RECOVERIES

A significant data security incident will frequently give rise to class action litigation, and the cost of defending and resolving that litigation often exceeds the cost of the breach response itself. The scope of this litigation trend is considerable. The number of reported data security events in the United States reached an all-time high in 2023,⁴⁹ and litigation following the disclosure of a data security event has become the norm, ranging from large-scale class actions brought by national plaintiffs' firms to smaller class actions brought against smaller businesses on behalf of state-specific classes. Notably, despite the growing ubiquity of data breach litigation, no data breach class action has ever been tried to verdict.

In 2023 alone, a number of major putative class actions were filed, including lawsuits against mortgage provider Mr. Cooper (14.6 million impacted individuals),⁵⁰ hospital system HCA Healthcare (11.3 million impacted individuals),⁵¹ and DNA testing company 23andMe (6.9 million impacted individuals).⁵² Several large cybersecurity litigations were also resolved, including the second-largest data breach settlement ever, a \$350 million settlement by T-Mobile,⁵³ and a \$49.5 million settlement by software company Blackbaud with the Attorneys General of 49 states and the District of Columbia regarding a 2020 ransomware incident.⁵⁴ Blackbaud had previously agreed to pay \$3 million to the SEC for failing to properly disclose the ransomware attack,⁵⁵ underscoring the growing level of regulatory scrutiny for data incidents.

Because data breach class actions frequently span multiple jurisdictions and may be consolidated through the Multidistrict Litigation process, there is significant value in coordinating with a single national law firm that has the resources and experience to handle complex, multi-jurisdictional defense. Litigation counsel should be involved as early as possible in the claims process, ideally before a complaint is filed, so that counsel can help shape the breach response narrative, preserve evidence, and prepare the insured for discovery and motion practice.

In response to the rise in third-party vendor risk, more carriers are pursuing subrogation actions against the vendors and software providers whose failures caused the breach. A leading example is the *Ace American v. Progress Software* case, where two insurers filed suit seeking to recover payments made to their insureds

Cyber Solutions for Insurance Professionals: Building Resilience Against Emerging Threats

arising from the May 2023 MOVEit file transfer software breach, which affected thousands of organizations worldwide and has been consolidated into a multidistrict litigation in the District of Massachusetts.⁵⁶ Insurers should consider whether they are adequately preserving and pursuing subrogation rights, as recoveries can materially reduce net losses.

Finally, it bears emphasis that cyber losses frequently implicate multiple lines of coverage, including directors and officers, errors and omissions, employment practices liability, media, crime, and general liability. For example, a data breach that triggers an SEC investigation might give rise to securities litigation. Insureds are also increasingly seeking coverage for cyber-related losses under non-cyber policies, including media liability endorsements added to general liability policies and cyber liability coverage provided as an add-on to technology errors and omissions or private equity insurance policies.

Despite the obvious need for coordination, even major, well-resourced insurers can find it challenging to manage exposures across coverage lines well. Siloed underwriting teams, separate claims units with their own leadership and priorities, differing renewal cycles, and internal competition between business units all contribute to gaps. The result can be unanticipated exposures, higher claims costs, and coverage disputes that only become apparent after a loss occurs. For this reason, coordination between lines, which is paramount at the claims stage, should actually begin at the underwriting stage. Because a cyber loss can potentially impact multiple lines of coverage, insurers must understand how the evolving cyber landscape affects each line of risk they are underwriting.

EVOLVING POLICY LANGUAGE: CLOSING GAPS BEFORE THEY BECOME DISPUTES

As cyber risks evolve, so must the policy language designed to address them. Insurers are actively updating coverage terms and exclusions across several key areas: from AI-related exposures and business interruption calculations to war exclusions for state-sponsored attacks and the growing wave of wrongful collection claims.

I. AI-RELATED COVERAGE AND EXCLUSION LANGUAGE

The insurance market has reached a point where specific AI language in policies is not optional, yet the market has not standardized its approach. Carriers are beginning to move, but their approaches vary considerably.

Some carriers have introduced affirmative AI endorsements. One insurer, for example, announced an endorsement that expands the definition of a security failure or data breach to include an AI security event, and expands the trigger for a funds transfer fraud event to include fraudulent instructions transmitted through the use of deepfakes or other AI technology.⁵⁷

At the other end of the spectrum, some carriers are considering AI-specific exclusions. One insurer has introduced the first so-called “absolute” AI exclusion in several specialty lines of liability coverage.⁵⁸ Because violations of emerging AI regulations like the EU AI Act may arise absent a traditional cyber event or data breach, resulting losses may fall outside the scope of a standard cyber policy regardless, but it is better to be explicit.

Insurers should also consider whether policy language adequately addresses losses arising from an insured’s employees using unsanctioned AI tools. If an employee uploads sensitive company data into a public AI platform and that data is compromised, is that a covered security failure? The answer may depend entirely on the policy language and may require an AI endorsement or exclusion, depending on the insurer’s intent.

Cyber Solutions for Insurance Professionals: Building Resilience Against Emerging Threats

II. BUSINESS INTERRUPTION LOSS

If there is one area of cyber coverage litigation that has dominated the landscape over the past few years, it is disputes over business interruption loss. These disputes are potentially the biggest trend in cyber claims, with insureds pushing to expand the coverage available to them beyond what the parties may have originally contemplated. These cases are only going to increase, and clear, unambiguous language defining the measurement period, the triggering event, and the methodology for calculating loss is essential.

This point is illustrated by *Heritage Co. v. Hudson Excess Insurance*, where a telemarketing company sought coverage under a cyber policy following a ransomware attack that disrupted its operations for months.⁵⁹ The parties disputed both the duration of the interruption period and the proper methodology for calculating business income loss. The court ultimately held that business interruption coverage is not intended to result in a windfall and that the insured could only recover normal operating expenses to the extent they were not paid using revenue earned during the interruption period.

III. WAR AND GEOPOLITICAL EXCLUSIONS

The *ViaSat v. Lloyd's* case, which involved an insurer's denial of coverage for a cyberattack during the Russian invasion of Ukraine based on a "War and Civil War Exclusion," was voluntarily dismissed but highlighted the importance of clear exclusionary language for state-sponsored cyberattacks.⁶⁰

The cyberattack in that case, attributed to Russia by U.S. and European governments, disabled tens of thousands of modems across Ukraine and Europe in advance of Russia's invasion. The case exposed how traditional war exclusions, typically drafted with armed military conflict in mind, may not address key questions raised by state-sponsored cyber operations: whether a cyberattack launched hours before a ground invasion constitutes an "act of war," whether collateral damage to civilian commercial systems in third-party countries falls within the exclusion's scope, and whether attribution to a nation-state alone is sufficient to trigger the exclusion absent a formal declaration of war.

With geopolitical tensions continuing to drive sophisticated cyber operations by China, Russia, Iran, and North Korea, insurers should ensure that war exclusions in underlying policies are drafted with cyberattacks specifically in mind, if that is the intent. Government-backed threat actors from these countries are actively using AI tools to research targets and vulnerabilities, making the intersection of geopolitical risk and cyber risk increasingly significant.

IV. WRONGFUL COLLECTION AND PIXEL TRACKING

Pixel tracking, BIPA, and other wrongful collection lawsuits have not gone away, and insurers are growing increasingly wary of extending coverage for privacy exposures arising from the use of tracking technologies and other data collection issues.

Wrongful collection lawsuits include both BIPA claims and the current wave of pixel tracking litigation, where plaintiffs have repurposed older privacy, wiretap, and anti-hacking statutes, such as the California Invasion of Privacy Act (CIPA) and the Video Privacy Protection Act (VPPA), to turn common website tracking software into a potentially huge liability for many businesses. Approximately 70 percent of wrongful collection claims reported to leading cyber insurers have been tied to CIPA,⁶¹ a 1967 statute originally designed to regulate wiretapping that is now being deployed against companies using tracking pixels, session replay tools, and AI-

Cyber Solutions for Insurance Professionals: Building Resilience Against Emerging Threats

powered chatbots. Four plaintiffs' law firms have alone been responsible for more than 70 percent of all these claims,⁶² often using templated demand letters to drive pre-litigation settlements at scale.

Insurers can potentially leverage several existing exclusions to deny coverage for wrongful collection claims. Invasion of privacy exclusions have proven particularly effective. In *Twin City v. Vonachen Services*, the court held that a broadly worded invasion of privacy exclusion barred directors and officers coverage for BIPA claims, rejecting the insured's argument that mere "procedural violations" did not implicate privacy rights.⁶³ Statutory violation exclusions have also been invoked against BIPA and related claims, though there have been some unfavorable rulings in this regard.⁶⁴ Insurers have also asserted wrongful collection exclusions against BIPA and related claims.⁶⁵

Beyond leveraging existing exclusions, insurers are implementing targeted policy changes. Many carriers are adding BIPA-specific or pixel tracking exclusions to eliminate ambiguity.⁶⁶ In *Tony's Finer Foods v. Certain Underwriters at Lloyd's*, an Illinois appellate court upheld a cyber policy exclusion barring coverage for claims based on collection of information by the insured without the knowledge or permission of the persons to whom such information relates, finding that such language plainly excluded BIPA claims.⁶⁷ Additionally, where affirmative wrongful collection coverage remains available, insurers are imposing sublimits well below full policy limits.⁶⁸

PREDICTIONS: CYBER RISKS BEYOND 2026

AI will be at the center of cyber risk for the foreseeable future, with agentic AI and Shadow AI creating new and often unmonitored vulnerabilities, while AI-powered deepfakes and voice cloning enable increasingly sophisticated social engineering attacks. The carriers who develop effective frameworks for underwriting and pricing AI risk will have a significant competitive advantage.

Ransomware will remain the dominant driver of claim severity; while improved controls and declining payment rates are encouraging, large-scale events will continue to expand the risk. A significant AI-related loss event, whether arising from an agentic AI failure, a deepfake-induced funds transfer, or an AI governance breakdown, appears likely in the near term. When it materializes, it will reshape underwriting approaches across the market. Wrongful collection litigation will also continue to expand, with pixel tracking, BIPA, and CIPA claims showing no signs of abating, and plaintiffs' counsel increasingly targeting new industries and technologies.

Cyber coverage disputes will increase, particularly over business interruption calculations, war exclusion applicability, and the scope of wrongful collection exclusions. Clear, unambiguous policy language drafted today will prevent costly disputes tomorrow. Finally, 2026 remains a favorable time for insurers to pursue meaningful coverage innovations, whether through AI endorsements, refined exclusionary language, or improved underwriting data, while market conditions support such investments.

The cyber risk landscape beyond 2026 will be more complex, more dynamic, and more consequential than ever. But for those who approach it carefully, the tools and strategies to manage that risk are available. The insurance professionals who engage proactively with these issues, rather than waiting for the next headline or the next lawsuit to force their hand, will be the ones best positioned to lead their organizations and better serve their policyholders.

Cyber Solutions for Insurance Professionals: Building Resilience Against Emerging Threats

Endnotes

- 1 See, e.g., SentinelOne, Key Cyber Security Statistics for 2026 (Mar. 12, 2026), available at: <https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-statistics/>; Kroll, A New Era of Financial Cybercrime Is Here (Mar. 18, 2025), available at: <https://www.kroll.com/en/publications/financial-crime-report-2025/new-era-financial-cybercrime>.
- 2 International Monetary Fund, Global Financial Stability Report: The Last Mile: Financial Vulnerabilities and Risks, p. 83 (Apr. 2024), available at: <https://www.imf.org/-/media/files/publications/gfsr/2024/april/english/text.pdf>.
- 3 TheCannataReport, Ransomware Attacks Soar with a 45% Increase in 2025, available at: <https://www.thecannatareport.com/ransomware-attacks-soar-by-45-percent/>.
- 4 S&P Global, Cyber Insurance Market Outlook 2026: Resilient Earnings, Tougher Competition, Pockets of Growth (Dec. 9, 2025), available at: <https://www.spglobal.com/ratings/en/regulatory/article/cyber-insurance-market-outlook-2026-resilient-earnings-tougher-competition-pockets-of-growth-s101658506>.
- 5 Allianz Risk Barometer: Identifying the Major Business Risks for 2026, p. 4 (2026), available at: <https://commercial.allianz.com/news-and-insights/news/allianz-risk-barometer-2026.html>.
- 6 IBM Report: Half of Breached Organizations Unwilling to Increase Security Spend Despite Soaring Breach Costs, available at: <https://newsroom.ibm.com/2023-07-24-IBM-Report-Half-of-Breached-Organizations-Unwilling-to-Increase-Security-Spend-Despite-Soaring-Breach-Costs>.
- 7 IBM, Cost of a Data Breach Report 2026: The AI Tipping Point, available at: <https://www.ibm.com/reports/data-breach>.
- 8 Federal Reserve Board, “Harvest Now Decrypt Later”: Examining Post-Quantum Cryptography and the Data Privacy Risks for Distributed Ledger Networks, p. 7 (2025), available at: <https://www.federalreserve.gov/econres/feds/files/2025093pap.pdf>.
- 9 Jillian Mascelli and Megan Rodden, Federal Reserve Board, “Harvest Now Decrypt Later”: Examining Post-Quantum Cryptography and the Data Privacy Risks for Distributed Ledger Networks (September 2025), available at: <https://www.federalreserve.gov/econres/feds/harvest-now-decrypt-later-examining-post-quantum-cryptography-and-the-data-privacy-risks-for-distributed-ledger-networks.htm>.
- 10 Keepnet, Deepfake Statistics & Trends 2026: Growth, Risks, and Future Insights, available at: <https://keepnetlabs.com/blog/deep-fake-statistics-and-trends>.
- 11 The Guardian, UK engineering firm Arup falls victim to £20m deepfake scam (May 17, 2024), available at: <https://www.theguardian.com/technology/article/2024/may/17/uk-engineering-arup-deepfake-scam-hong-kong-ai-video>.
- 12 Harvard Law School Forum on Corporate Governance, SolarWinds Dismissed: What the SEC’s U-turn Signals for Cyber Enforcement (Dec. 7, 2025), available at: <https://corpgov.law.harvard.edu/2025/12/07/solarwinds-dismissed-what-the-secs-u-turn-signals-for-cyber-enforcement/>.
- 13 White & Case, Long awaited EU AI Act becomes law after publication in the EU’s Official Journal (Jul. 16, 2024), available at: <https://www.whitecase.com/insight-alert/long-awaited-eu-ai-act-becomes-law-after-publication-eus-official-journal>.
- 14 Federal Bureau of Investigation, Internet Crime Report 2024, p. 10 (April 23, 2024), available at: https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.
- 15 Federal Bureau of Investigation, Business Email Compromise: The \$55 Billion Scam, available at: <https://www.ic3.gov/PSA/2024/PSA240911>.
- 16 Federal Bureau of Investigation, FBI Releases Annual Internet Crime Report, available at: <https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report>.
- 17 Coalition, 2025 Cyber Claims Report, p. 6, available at: https://cdn.intelligencebank.com/us/share/NMXD/aP6w/1413d/original/Coalition_2025-Cyber-Claims-Report.
- 18 Brightside, AI-Generated Phishing vs Human Attacks: 2025 Risk Analysis, available at: <https://www.brside.com/blog/ai-generated-phishing-vs-human-attacks-2025-risk-analysis>.
- 19 CrowdStrike, 2024 Global Threat Report, available at: <https://github.com/jacobdjwilson/awesome-annual-security-reports/blob/main/Annual%20Security%20Reports/2024/Crowdstrike-Global-Threat-Report-2024.pdf>.
- 20 Cloudflare, 2025 Q4 DDoS threat report: A record-setting 31.4 Tbps attack caps a year of massive DDoS assaults (Feb. 5, 2026), available at: <https://blog.cloudflare.com/ddos-threat-report-2025-q4/>.
- 21 SentinelOne, DDoS Attack Statistics 2026: 41 Key Facts and Trends (May 6, 2026), available at: <https://www.sentinelone.com/cybersecurity-101/cybersecurity/ddos-attack-statistics/>.
- 22 *Id.*, p. 5.
- 23 Verizon, 2025 Data Breach Investigations Report, p. 10 (Apr. 22, 2025), available at: <https://www.verizon.com/business/resources/Td5c/reports/2025-dbir-data-breach-investigations-report.pdf>.

Cyber Solutions for Insurance Professionals: Building Resilience Against Emerging Threats

- 24 See Chainalysis, The 2026 Crypto Crime Report, p. 60 (Feb. 26, 2026), available at: <https://www.chainalysis.com/wp-content/uploads/2026/03/the-2026-crypto-crime-report-3-17-release.pdf>.
- 25 *Id.*, p. 17.
- 26 Coalition, 2025 Cyber Claims Report, p. 18, available at: https://cdn.intelligencebank.com/us/share/NMXD/aP6w/1413d/original/Coalition_2025-Cyber-Claims-Report.
- 27 Arctic Wolf, 2026 Threat Report, p. 3 (Feb. 17, 2026), available at: <https://arcticwolf.com/resource/aw/arctic-wolf-threat-report-2026>.
- 28 NetDiligence, Cyber Claims Study 2025 Report, p. 17 (Sep. 17, 2025), available at: <https://netdiligence.com/wp-content/uploads/2025/12/NetDiligence-Cyber-Claims-Study-2025-Report-V1.1.pdf>.
- 29 Multistate, All of the Comprehensive Privacy Laws That Take Effect in 2026 (Feb. 4, 2026), available at: <https://www.multistate.us/insider/2026/2/4/all-of-the-comprehensive-privacy-laws-that-take-effect-in-2026>.
- 30 See California Privacy Protection Agency, California Finalizes Regulations to Strengthen Consumers' Privacy (Sep. 23, 2025), available at: <https://coppa.ca.gov/announcements/2025/20250923.html>.
- 31 TrueVault, Extensive Changes to Connecticut's Privacy Law (Aug. 5, 2025), available at: <https://www.truevault.com/learn/extensive-changes-to-connecticuts-privacy-law>.
- 32 Ketch, Colorado Privacy Act (CPA): What you need to know in 2026, available at: <https://www.ketch.com/regulatory-compliance/colorado-privacy-act-cpa>.
- 33 State of California Department of Justice, California Won't Let It Go: Attorney General Bonta Announces \$2.75 Million Settlement with Disney, Largest CCPA Settlement in California History (Feb. 11, 2026) <https://oag.ca.gov/news/press-releases/california-wont-let-it-go-attorney-general-bonta-announces-275-million>.
- 34 Verizon, 2025 Data Breach Investigations Report, p. 11 (Apr. 22, 2025), available at: <https://www.verizon.com/business/resources/Td5c/reports/2025-dbir-data-breach-investigations-report.pdf>.
- 35 SecurityScorecard, 2025 SecurityScorecard Global Third-Party Breach Report (Mar. 2025), p. 2, available at: https://securityscorecard.com/wp-content/uploads/2025/03/SSC-Third-Party-Breach-Report_031225_03.pdf.
- 36 *Id.*, p. 10.
- 37 IBM, Cost of a Data Breach Report 2025: The AI Oversight Gap, p. 7 (Jul. 30, 2025), available at: <https://www.ibm.com/downloads/documents/us-en/131cf87b20b31c91>.
- 38 FTC, Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking, available at: <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/lurking-beneath-surface-hidden-impacts-pixel-tracking>.
- 39 FTC, FTC Brings Action Against Ed Tech Provider Chegg for Careless Security that Exposed Personal Data of Millions of Customers, available at: <https://www.ftc.gov/news-events/news/press-releases/2022/10/ftc-brings-action-against-ed-tech-provider-chegg-careless-security-exposed-personal-data-millions>.
- 40 NYDFS, Governor Hochul Announces Updates To New York's Nation-Leading Cybersecurity Regulations as Part of Sweeping Effort to Protect Businesses and Consumers from Cyber Threat, available at: https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202311011.
- 41 NCSL, Artificial Intelligence 2024 Legislation, available at: <https://www.ncsl.org/technology-and-communication/artificial-intelligence-2024-legislation>.
- 42 Dan Bilefsky, New York Times, Hackers Use New Tactic at Austrian Hotel: Locking the Doors, available at: <https://www.nytimes.com/2017/01/30/world/europe/hotel-austria-bitcoin-ransom.html>.
- 43 Ariel Bogle, Slate, A Cyber Attack May Have Caused a Turkish Oil Pipeline to Catch Fire in 2008, available at: <https://slate.com/technology/2014/12/bloomberg-reports-a-cyber-attack-may-have-made-a-turkish-oil-pipeline-catch-fire.html>.
- 44 See, e.g., Dan Goodin, ARS Technica, Ransomware group reports victim it breached to SEC regulators, available at: <https://arstechnica.com/security/2023/11/ransomware-group-reports-victim-it-breached-to-sec-regulators/>.
- 45 See, e.g., Rajvardhan Oak and Zubair Shafiq, "Hello, is this Anna?": Unpacking the Lifecycle of Pig-Butchering Scams, available at: <https://arxiv.org/html/2503.20821v2#bib.bib16>.
- 46 See, e.g., Campus CISO, Old-School Mail Brings New Ransomware Threats to Higher Education, available at: <https://www.campusciso.com/blogs/old-school-mail-brings-new-ransomware-threats-to-higher-education>.
- 47 National Institute of Standards and Technology, NIST Releases First 3 Finalized Post-Quantum Encryption Standards (Aug. 13, 2024), available at: <https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards>.
- 48 National Institute of Standards and Technology, Post-Quantum Cryptography (Dec. 11, 2025), available at: <https://csrc.nist.gov/projects/post-quantum-cryptography>.
- 49 Matt Kapko, Cybersecurity Dive, US data compromises surged to record high in 2023, available at: <https://www.cybersecuritydive.com/news/data-compromises-surge/705549/>.

Cyber Solutions for Insurance Professionals: Building Resilience Against Emerging Threats

- 50 Christopher Brown, Bloomberg, Mr. Cooper Customers Advance Class Action Over 2023 Data Breach, available at: <https://news.bloomberglaw.com/privacy-and-data-security/mr-cooper-customers-advance-class-action-over-2023-data-breach>.
- 51 Steve Alder, The HIPAA Journal, 11.27 Million HCA Healthcare Patients Affected by Recent Cyberattack, available at: <https://www.hipaajournal.com/hca-healthcare-cyberattack-data-breach-2023/>.
- 52 Steve Alder, The HIPAA Journal, 6.9 Million 23andMe Users Affected by Data Breach, available at: <https://www.hipaajournal.com/6-9-million-23andme-users-affected-by-data-breach/>.
- 53 Samantha Kelly, CNET, T-Mobile Sued Again Over Massive 2021 Data Breach, available at: <https://www.cnet.com/tech/t-mobile-sued-again-over-massive-2021-data-breach/>.
- 54 Blackbaud, Blackbaud Resolves Multi-State Attorneys General Investigation of 2020 Security Incident, available at: <https://www.blackbaud.com/newsroom/article/blackbaud-resolves-multi-state-attorneys-general-investigation-of-2020-security-incident>.
- 55 SEC, SEC Charges Software Company Blackbaud Inc. for Misleading Disclosures About Ransomware Attack That Impacted Charitable Donors, available at: <https://www.sec.gov/newsroom/press-releases/2023-48>.
- 56 See *Ace Am. Ins. Co. v. Progress Software Corp.*, No. 1:24-cv-10140-ADB (D. Mass.), consolidated in *In re MOVEit Customer Data Sec. Breach Litig.*, No. 1:23-md-03083-ADB (D. Mass.). See also *Great American Fidelity Ins. Co. v. Keystone Management Grp., LLC*, No. 3:24-cv-00426-WWB-LLL (M.D. Fla.) (subrogation action against third-party vendor of the insured to recoup losses resulting from data breach).
- 57 Coalition, Coalition Adds New Affirmative Artificial Intelligence Endorsement to Cyber Insurance Policies (Mar. 26, 2024), available at: <https://www.coalitioninc.com/announcements/coalition-adds-new-affirmative-ai-endorsement-to-cyber-policies>.
- 58 Hunton, The Continued Proliferation of AI Exclusions (May 28, 2025), available at: <https://www.hunton.com/hunton-insurance-recovery-blog/the-continued-proliferation-of-ai-exclusions>.
- 59 *Heritage Co. v. Hudson Excess Ins. Co.*, No. 4:22-cv-82-JM, 2024 U.S. Dist. LEXIS 91714 (E.D. Ark. May 22, 2024).
- 60 *ViaSat Inc. v. Lloyd's*, No. 3:22-cv-01169-JAH-DDL (S.D. Cal.) (insurer denied coverage for cyberattack which occurred in Europe at the time of the Russian invasion of Ukraine based, in part, on a "War and Civil War Exclusion") (voluntarily dismissed).
- 61 Insurance Business, Wrongful collection claims escalate as CIPA drives new wave of cyber lawsuits (Oct. 20, 2025) <https://www.insurancebusinessmag.com/us/news/cyber/wrongful-collection-claims-escalate-as-cipa-drives-new-wave-of-cyber-lawsuits-553582.aspx>.
- 62 *Id.*
- 63 *Twin City Fire Ins. Co. v. Vonachen Servs.*, 567 F Supp 3d 979 (C.D. Ill. 2021).
- 64 See, e.g., *Thermoflex Waukegan, LLC v. Mitsui Sumitomo Ins. USA, Inc.*, 102 F.4th 438, 442 (7th Cir. 2024) (holding statutory violation exclusion inapplicable to BIPA claim based on Illinois Supreme Court precedent).
- 65 See, e.g., *Rempres, LLC v. Certain Underwriters at Lloyd's London*, 228 N.E.3d 321, 343 (Ill. App. Ct. 2023) (finding wrongful collection exclusion applicable but holding that the insured had a duty to defend under a specific carveout for defense costs).
- 66 Bloomberg, Web Tracking Suits Draw Pushback from Cyber, Liability Insurers (Sep. 11, 2025), available at: <https://news.bloomberglaw.com/insurance/web-tracking-suits-draw-pushback-from-cyber-liability-insurers>.
- 67 *Tony's Finer Foods Enters., Inc. v. Certain Underwriters at Lloyd's, London*, 263 N.E.3d 579, 586 (Ill. App. Ct. 2024).
- 68 See, e.g., ERRRA.com, Files Cyber 'Bolt-On' Coverage for Small Businesses (Oct. 5, 2025) (noting regulatory filings by U.S. Specialty Insurance Company which included, among other things, a "Biometric Claims Sublimit" and a "Pixel Tracking Exclusion"), available at: <https://errra.com/files-cyber-bolt-on-coverage-for-small-businesses/>; CharityFirst, Cyber Market Comparison (noting \$100,000 BIPA sublimit on BCS policies), available at: https://www.charityfirst.com/media/zwghxuo/cf_cybermktcomparison_031722-1.pdf.

For more information about Wilson Elser's Insurance & Reinsurance Coverage practice, visit our [website](#).



Richard W. Boone Jr.

Partner - New York, NY

212.915.5972

richard.boone@wilsonelser.com