RT ProExec

The Importance of Cyber Insurance and How to Get Full Value Out of a Cyber Policy

CONTACT
RT ProExec
rtproexecinfo@rtspecialty.com

Or contact your local RT ProExec broker at rtspecialty.com

Cyber insurance has evolved significantly since its inception in the late 1990s, becoming beneficial for businesses of all sizes to help protect against growing cyber threats such as hacking, or stealing personally identifiable information both intentionally and unintentionally (when an employee inadvertently sends out private information for example). It is known by a number of different terms such as – Privacy and Network Security Insurance; Data Breach Insurance; Information Security & Privacy Insurance; or a combination of the above - most typically though, just Cyber Insurance / Liability. Mention of privacy, network security or of course the term cyber will tip you off. There are also a lot of synonymous terms for coverage grants within Cyber Insurance Policies that I have summarized below. This document outlines the history, current landscape, policy components, exclusions, requirements, and recommendations for maximizing the value of cyber insurance.

History

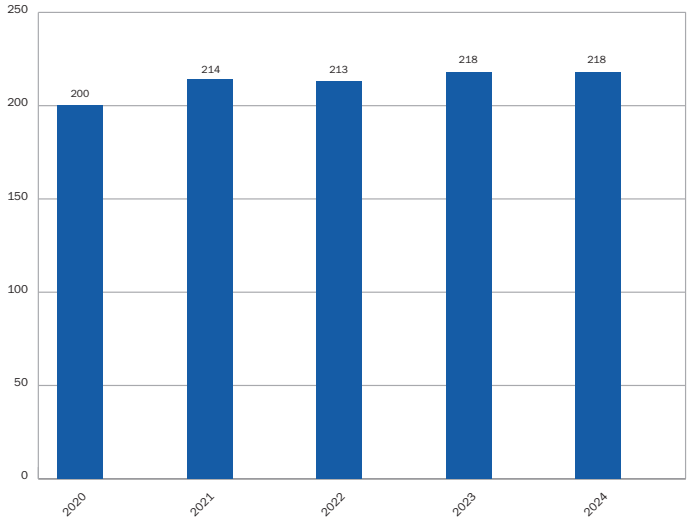
Cyber insurance first emerged in the late 1990s, following the public release of the World Wide Web in 1993. The earliest dedicated policy, known as the Internet Security Liability policy, was launched by American International Group (AIG) in April 1997. Initially, adoption was slow due to limited awareness of cyber risks and the distraction caused by the Y2K bug. However, the industry began to gain momentum in the early 2000s.

Mass adoption of cyber insurance accelerated between 2003 and 2005, largely due to California's groundbreaking breach notification law, CalOPPA. This legislation triggered a domino effect, prompting businesses to consider liability insurance for data loss and pushing cyber insurance into the mainstream. The market continued to grow as regulatory pressures increased, and major data breaches became more frequent.

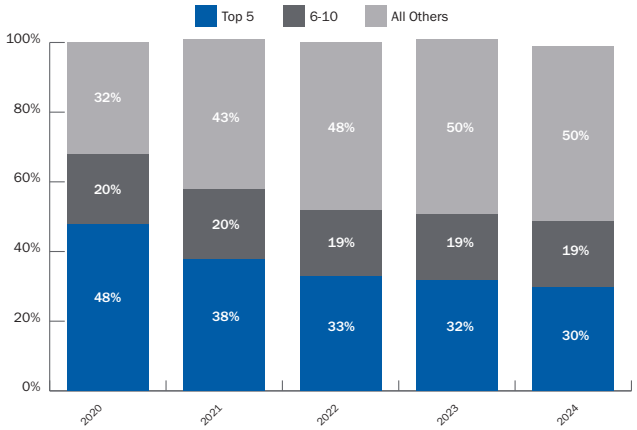
Between 2010 and 2015, the industry saw rapid expansion, fueled by high-profile data breaches and evolving regulations such as Health Insurance Portability and Accountability Act (HIPAA). During this period, cyber insurance shifted from a niche product to a standard business insurance offering. By 2015, the market was generating more than $2 billion in premiums, with growth driven by rising ransomware incidents and business interruptions related to cyber threats.

From 2021 onward, a surge in ransomware attacks pushed the market into a "hard market," where demand for cyber insurance was at an all-time high and coverage became critical for businesses. By 2020, the number of cyber insurance providers grew considerably, with the market softening in recent years due to increased capacity and lower claims levels. As of 2024, cyber insurance remains an essential tool for businesses seeking protection against evolving cyber risks.

U.S. Number of U.S. Chamber Insurers, 2020-2024



Total Cyber Written Premium Distribution by Insurer Size, 2020-2024

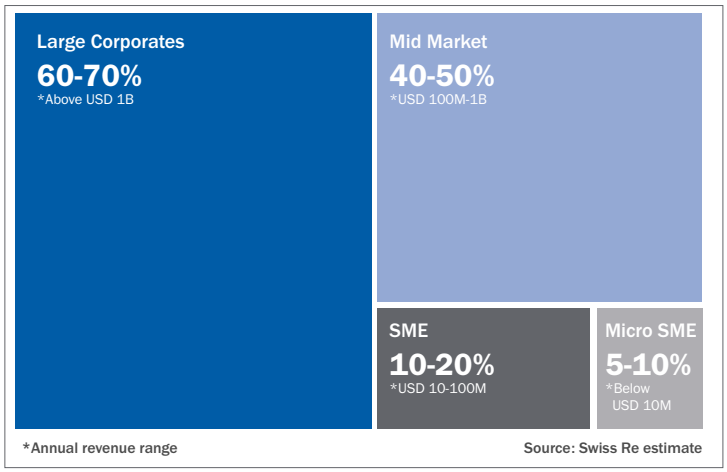


The Importance of Cyber Insurance and How to Get Full Value Out of a Cyber Policy

Current Landscape

Now today, we are seeing not just the largest companies buy cyber, but also smaller insureds taking up larger portion of the market segment. Threat actors go for the lowest hanging fruit so smaller revenue insureds are less likely to have decent controls in place and thus become easier targets. Some insureds are catching on and collaborating with the insurance industry to put protections in place. You may have to, for example, an insured or potential insured may need to implement Multi Factor Authentication if they do not already have in place. But this and other controls Cyber Insurers are seeking all serve to reduce risk helping all parties involved defend themselves from these newer and evolving threats.

What Percentage of Each Customer Segment is Buying Cyber Insurance?



CORE COMPONENTS OF A CYBER INSURANCE POLICY

First-Party Coverage (Expenses):

- **Incident Response & Forensics:** Covers costs to hire experts to investigate and contain the breach. (synonymous terms - Cyber Incident Mitigation; Breach Management/Response; Intrusion Response; Cybersecurity Emergency Response; Damage Containment and Recovery)
  - **Commonly Covered Events:** AI-Enhanced Phishing and Social Engineering; Ransomware and Data Extortion; API and Cloud Native Vulnerabilities; Supply Chain Compromise; Account Takeover & Business Email Compromise; Living Off the Cloud/Land Attacks.
- **Data Recovery & Restoration:** This coverage part pertains to restoring lost or encrypted data. (Synonymous terms: Data Asset Restoration; Data Reconstitution; Data Recreation; System Restoration/Rebuilding; Data Remediation)
  - **Commonly Covered Events:** External Specialists; Re-keying/Inputting; Software/System Rebuilding; Data Validation.
  - **Case Example:** A hacker has whipped an insured's system. There are costs associated with recovering and restoring that lost or missing data. In some cases, the whole system may have to be rebuilt.
- **Business Interruption:** This coverage grants responds to lost income and operating expenses if systems go down. (Synonymous terms: Network Interruption; Contingent/Dependent Business Interruption; Business Income Insurance; System Failure; Consequential Loss)
  - **Commonly Covered Events:** Ransomware/Malware; Denial of Service (DDoS); Network Security Failure; Third-Party Vendor Outage
  - **Case Example:** A ransomeware attack takes down an e-commerce platform for five days. They are not able to accept orders at this time which causes lost revenue.
  - **Note:** Dependent Business Interruption (also known as Contingent Business Interruption) is a type of insurance coverage that compensates a business for lost income and extra expenses caused by an interruption to a key third-party provider or customer. It covers disruptions at suppliers, manufacturers, or customers, rather than damage the insured's own property. If offered, this is typically sublimited. Some carriers limit it to IT/cloud vendor failures, while others extend it to a broader set of dependent entities. For retailers placing accounts with heavy vendor dependencies (healthcare, manufacturing, fintech), that distinction can be the difference between coverage and no coverage on a dependent claim.
- **Cyber Extortion:** Covers ransom payments and negotiator fees. (Synonymous terms: Ransomware; Data Kidnapping; Digital Blackmail; Double Extortion; DDoS Extortion; Sextortion; Protesware; Extortionware)
  - **Commonly Covered Events:** Ransomware Attacks; Doxing/Data Breach Extortion; DDoS Attack; Social Engineering / Business Email Compromise; Software Vulnerability Extortion.
  - **Typical Costs Covered:** Extortion Payments; Incident Response; Negotiation Expenses; Public Relations; Business Interruption.
- **Crisis Management/PR:** Grants coverage for costs to restore company reputation. (Synonymous terms: Reputation Management; Issues Management; Crisis Communications Strategy; Contingency Planning; Corporate Reputation Defense; Emergency Communication Plan; Crisis Response Protocol)

- **Commonly Covered Events:** PR Consultation & Strategy; Notification Services; Customer Support; Credit Monitoring; Social Media Monitoring.**Notification Costs:** Coverage grant that expenses for informing affected customers of a breach (postage, call centers). (Synonymous terms: Breach Response)
- **Commonly Covered Events:** Postage for notifying affected customers, and call centers for the same reason

Third-Party Coverage (Liability):

- **Data Privacy Liability:** Legal liability for lawsuits from customers whose data was stolen (think the liability of insured's vendors as well).
  - **Commonly Covered Events:** Data breaches of vendor systems; Supply Chain Attacks (i.e. SolarWinds); Ransomeware of Vendors; Pixels of vendors; Email compromise of vendors or clients; Lost of stolen data of vendors
- **Regulatory Fines/Penalties:** Covers fines from government entities, such as GDPR or HIPAA violations.
  - **Commonly Covered Events:** Data Breaches and PII Theft; Regulatory Investigations; Privacy Law Violations; PCI DSS Assessments; Third-Party Vendor Breaches; Delayed Disclosure; Non-Material Violations (certain policies now offer coverage for regulatory actions even if a breach or security incident did not occur, such as penalties for failing to properly respond to consumer privacy requests).

Additional Coverages for Added Protection:

- **Media Liability:** Covers defamation or intellectual property infringement.
  - **Coverages:** Defamation, libel, slander, product disparagement; violations of the right to privacy, such as false light and intrusion upon seclusion; invasion of an individual's right of publicity; plagiarism; improper deep linking; false arrest; and the invasion of the right to private occupancy, such as trespassing or wrongful eviction.
  - **Note:** Media and the way it is used have changed significantly over the years. Media liability becomes intertwined with cyber liability, particularly with content disseminated through electronic means.
  - **Case Example:** Defamation from social media: A retail business has an online presence, including a website and numerous social media pages. A hacker accesses their social media account and defames a competitor's business, resulting in a lawsuit initiated by the competitor claiming lost revenues as a result of this defamation. Is this a cyber claim or a media claim?
  - **Case Example:** Privacy violation by an employee: A PR business has several high-profile clients. A rogue employee takes information meant to be private for a client and posts it on the PR business's website. Is this privacy liability or media liability?
- **Tech Errors & Omissions (Tech E&O):** Protects against financial losses caused by a failure of technology products or services to perform as intended.
  - **Coverages:** Glitches caused by a breach; botched migration; other software glitches.
- **Crime:** There is some gray area between what constitutes a cyber claim vs. a crime claim. The coverages listed below are not typically provided in a cyber policy; therefore, a crime policy can be purchased to supplement the coverage.
  - **Coverages:** Social engineering; theft of client funds; callback and authentication provisions.
  - **Note:** The Cyber Insurance market has evolved to offer sublimits on Social Engineering coverage, but typically only up to $100k-$250k. For larger companies that may require higher limits, a crime policy and or offshore excess Social Engineering only programs can be put together.
- **(Affirmative) AI Coverage:** This growing exposure is typically not contemplated in the aforementioned coverages. Some carriers may be silent on it, leaving it to the courts to decide if coverage will be afforded. For insureds looking to ensure claims stemming from the use of AI technology are covered, considering a dedicated AI policy is recommended.

COMMON EXCLUSIONS (WHAT IS NOT COVERED)

- **Prior Breaches:** Events that occurred before the policy start date.
- **Human Error/Negligence:** Incidents caused by employees failing to follow security protocols. What is typically excluded here is gross negligence or willful misconduct.
- **Physical Asset Damage:** Damage to physical infrastructure (usually covered by commercial property insurance).
- **Betterment:** Costs to improve or upgrade security systems after a breach.

- **Act of War:** State-sponsored cyber warfare. This has been a hot topic in the Cyber world for a while, but especially now when Iranian hacker groups are going on the offensive targeting US and Israeli companies. Since the mid to late 2000s, China, Russia, Iran, and North Korea have made up 77% of all state sponsored cyber operations. They all have different goals which are important to keep in mind. China has been known to be focused on information warfare and espionage. North Korea is often more focused on either destructive attacks or hacks that increase their finances. And Russia is known to go on the offensive like their 2007 cyber attack on Estonia, and a year later in the Russo-Georgian War.

KEY REQUIREMENTS TO QUALIFY

Insurers often require companies to have robust security in place before issuing a policy.

- **Multi-Factor Authentication (MFA):** Mandatory for remote access. Multi-factor authentication (MFA) is critical because it adds essential layers of security beyond passwords, making users 99% less likely to be hacked. By requiring at least two forms of verification (e.g., password + mobile code), it stops attackers from accessing accounts even if they steal credentials through phishing or data breaches.
- **Endpoint Detection and Response (EDR):** Security software installed on all devices. Endpoint Detection and Response (EDR) is critical for modern cybersecurity because it provides continuous, real-time monitoring and visibility across endpoints (laptops, servers, mobile devices) to detect, investigate, and mitigate advanced threats that evade traditional antivirus software. EDR enables rapid incident response, forensic analysis, and behavioral, AI-driven threat detection.
- **Data Backups:** Regular, encrypted backups that are secure from ransomware. Regularly backing up ensures business continuity, preventing significant financial losses and reputational damage while allowing for rapid recovery of critical information.

IMPORTANT DISTINCTIONS

- **Social Engineering Fraud:** This is frequently excluded unless specifically purchased as an add-on. Typically, would need a specialist crime market that can include the coverage.
- **"Bricking":** Some insurers offer specific coverage for when hardware is destroyed (bricked). Many cyber insurance forms have evolved to cover this exposure. But there is some gray area when it comes to covering physical damage. So, it is important to affirm this coverage is granted in a policy.

Cyber insurance has evolved a lot to respond to the new and emerging threats. The bad actors are getting more sophisticated with the use of AI – spelling errors are rarer now, and hacking kits can be purchased on the dark web for minimal fees. So now almost anyone with the desire can become involved as a bad cyber actor.

Phishing remains a top threat. Therefore, regular phishing training can do a lot to help significantly reduce this risk. Business email compromise and funds transfer fraud remain as large exposures as well. Ransomware is also continuing to surge. Meta Pixels is also a growing exposure we are discussing in the insurance industry – alleging improper sharing of data with third parties. This is often not covered by a cyber insurance policy.

It is a complicated industry, but we are here to help! Cyber insurance now does not only respond in the time of a claim, but many carriers are adapting to find other ways of interacting with the insureds during the life cycle of the policy. That a lot of times also includes monitoring and outreach when dark web activity is detected that is tied to an insured's company. Other important value adds could include an incident response plan, so that roles are assigned during the toughest time of many insureds' careers. This is very important and can help a lot during a breach event when tensions are high, and chances for mistakes are elevated. A Cyber Insurance policy can in some cases also include a dedicated hot line to a law firm who can help navigate and give advice during a claim.

In conclusion, cyber insurance is often structured alongside Technology E&O, Media Liability, and Crime coverage to address a range of related risks. And for those utilizing AI, a dedicated AI policy could help supplement coverage. This will increase the likelihood of a filed claim being covered. With a soft market and more options than ever, it is a great time for insureds to consider their risk management options and purchase their first cyber insurance policy if they do not already have one. If you are a retailer looking to implement this for your clients, please don't hesitate to reach out!

SOURCES AND CITATIONS

The factual assertions in this article are based on the following publicly available sources and the author's analysis of cyber insurance coverage structures.

Sam Tashima."Cyber Insurance Nears an Inflection Point." April 2026. https://actuary.org/article/cyber-insurance-nears-an-inflection-point/.

Privacy Notification and Crisis Management Expense Coverage. Apr. 2026. https://www.irmi.com/term/insurance-definitions/privacy-notification-and-crisis-management-expense-coverage#:~:text=Home%20Term%20Insurance%20Definitions%20privacy,personal%20auto%20policy%20(PAP)).

Security, Pivot Point. "How Should Crisis Management Connect with Incident Response?" Pivot Point Security. July 2024. https://www.pivotpointsecurity.com/how-should-crisis-management-connect-with-incident-response/.

"What Is Cyber Extortion?" Fortinet, Apr. 2026. https://www.fortinet.com/resources/cyberglossary/cyber-extortion.

"2026 Unit 42 Global Incident Response Report." Palo Alto Networks, Apr. 2026. https://www.paloaltonetworks.com/resources/research/unit-42-incident-response-report.

Modern Cybersecurity Threats and How to Detect Them. Apr. 2026. https://www.vectra.ai/topics/cybersecurity-threat.

What Is Digital Forensics and Incident Response (DFIR)? | IBM. Feb. 2023, https://www.ibm.com/think/topics/dfir.

"What Is Exposure Management in Cybersecurity? | CrowdStrike." CrowdStrike.Com, Apr. 2026. https://www.crowdstrike.com/en-us/cybersecurity-101/exposure-management/.

"Expert Digital Forensics & Incident Response Services." eSentire, Apr. 2026. https://www.esentire.com/what-we-do/digital-forensics-and-incident-response.

The Birth of the Web | CERN. Apr. 2026. https://home.cern/science/computing/birth-web#:~:text=On%2030%20April%201993%2C%20CERN%20put%20the,These%20actions%20allowed%20the%20web%20to%20flourish.

"Media Liability Coverage in a Cyber Policy." Insurance Training Center, Apr. 2026. https://insurancetrainingcenter.com/resource/media-liability-coverage-in-a-cyber-policy/.

Cyber Insurance Claims Studies | NetDiligence. Mar. 2020, https://netdiligence.com/cyber-insurance-claims-study/.

2026 Cyber Claims Report | Coalition. Apr. 2026. https://www.coalitioninc.com/claims-report/2026.

Cyber Operations Tracker. Apr. 2026. https://www.cfr.org/cyber-operations/.

Nation-State Threats | Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors