Cybersecurity insurance – a beginner's guide

The better the question. The better the answer.
The better the world works.

Shape the future with confidence

Table of contents

1. Introduction

In today's rapidly evolving landscape of cybersecurity, cyber insurance is emerging as a strategic tool within the organization's broader risk management strategy. Rather than simply accepting off-the-shelf coverage, businesses are increasingly taking a more deliberate approach to align cyber insurance decisions with their overall risk posture and defined thresholds for loss. As organizations digitally transform, and cyber threats continue to intensify, this shift enables businesses to balance mitigation, transfer and acceptance of risk in a way that reflects their unique business priorities. In this article, we explore the foundational concepts of cyber insurance and the role insurance plays in managing financial exposure and enabling informed business-driven risk decisions.

2. What is cyber insurance?

Cyber insurance provides financial protection and support services against online risks and IT threats, covering direct costs from cyber events, third-party claims and assisting with regulatory compliance. It helps mitigate the financial impact of incidents such as data breaches, ransomware and business interruptions. Essential coverage includes the following:

First-party coverage:

- **Data breach response:** Expenses for breach management, such as notifications and public relations
- **Business interruption:** Lost income from disrupted operations after a cyber attack
- **Data recovery:** Costs to restore or replace lost or corrupted data
- **Extortion:** Payments for ransomware or cyber extortion
- **Network damage:** Repair or replacement of damaged hardware or software

Third-party coverage:

- **Privacy liability:** Lawsuit protection for exposing sensitive third-party data
- **Regulatory fines:** Penalties for data protection failures or noncompliance
- **Media liability:** Issues from electronic content, like intellectual property (IP) infringement or defamation

3. What is D&O insurance (directors and officers)?

- **Purpose and coverage** — Protects corporate leaders and board members from lawsuits related to negligence, mismanagement and breaches of fiduciary duties
- **Who is it for?** Executives, board members and officers of corporations or nonprofits
- **Claim examples** — A board or individual members are named by a shareholder or a derivative suit for a decision that negatively affected the company's stock value
- **Reason to purchase** — Attract and retain qualified senior leaders by safeguarding their personal assets from potential lawsuits

4. What is E&O insurance (errors and omissions)?

- **Purpose and coverage** — Protects professionals (e.g., lawyers, doctors, accountants) against claims of negligence, breach of contract, fraud/misrepresentation and professional malpractice
- **Who is it for?** Anyone providing professional services, from real estate agents and financial consultants to IT professionals and architects
- **Claim examples** — Software company negligently releases corrupted software update and causes system outages that result in lost sales and suits from software customers
- **Reason to purchase** — Keep your business from shouldering the steep financial costs of handling a claim and paying legal fees (and possibly a settlement) due to professional negligence

5. How does cyber insurance relate to D&O and E&O policies?

Cyber insurance can be an important consideration for both D&O and E&O insurance, as it can fill in coverage gaps and provide specialized protection against the financial and reputational impacts of cyber incidents. Businesses should work with their insurance brokers or legal advisors to assess their coverage needs and make sure that they have reasonable protection across all relevant areas of risk. As an example, a cyber incident could lead to a lawsuit against directors and officers for failing to implement adequate cybersecurity measures, potentially triggering both cyber insurance and D&O insurance. Similarly, a cyber incident resulting from a professional service error could involve both cyber insurance and E&O insurance.

6. Would cyber insurance cover business interruption due to a cybersecurity breach?

Each policy has its own exclusions and sub-limitations, but business interruption resulting from a cyber attack could be covered within a cybersecurity policy. There are also insurance policies exclusively focusing on business interruption, and those could cover a cyber event unless explicitly excluded.

7. What are some considerations that may influence cyber insurance premiums?

The insurance industry has seen a significant shift in underwriting, moving from simple questionnaires to detailed 30+ page documents and on-site audits. Cyber insurance is increasingly shifting toward data-driven decisions, enabling better negotiation of premiums and policy terms. Quantifying risk facilitates transparent discussions about coverage and risk transfer between insurers and organizations. This shift is crucial as cyber insurance policies adapt to the growing complexity of cyber threats. This change stems from the need to better assess complex risks and provide customized insurance offerings. Initially, underwriters used a limited number of questions to determine risk and premiums. However, as cyber breaches increased and resulting claims grew, the need for in-depth information led to more detailed and objective evaluations covering various risk factors. On-site evaluations and data driven approaches provide underwriters a more direct view of business operations and the chance to advise on risk management. This thorough approach to underwriting allows for more precise risk assessment, accurate premiums, appropriate coverage limits and improved sustainability in the insurance sector. Here are some considerations that may influence cyber insurance premiums:

1. **Patch systems regularly** — Regularly patching your systems can lead to lower cyber insurance premiums, as it demonstrates proactive management of security vulnerabilities.
2. **Strengthen identity access management (IAM) systems/processes** — Implementing privileged access management (PAM) and multi-factor authentication (MFA) practices and conducting regular access review campaigns can positively affect premiums by making sure only necessary personnel have access to critical systems. In addition, protecting your active directory can lead to lower insurance costs, as it is a critical component in preventing widespread network compromise.
3. **Use encryption** — Using encryption protects sensitive data, potentially decreasing cyber insurance costs by lowering the risk of data breaches.
4. **Create redundant and reliable backups** — Creating redundant and reliable backups may influence insurers to offer lower premiums due to the reduced impact of data loss incidents.
5. **Implement network segmentation (secure remote desktop protocol (RDP), virtual private network (VPN), operational technology/information technology (OT/IT))** — Implementing network segmentation, including secure RDP and VPNs, can reduce premiums by limiting the spread of breaches within networks.
6. **Conduct regular penetration testing** — Regular penetration testing can lead to reduced cyber insurance premiums by identifying and allowing for the remediation of security weaknesses.
7. **Establish an incident response plan** — Establishing a written incident response plan can influence insurers to lower Premiums, because it shows preparedness to effectively handle security incidents.
8. **Implement vendor/supply chain risk management** — Implementing vendor/supply chain risk management can result in lower premiums by mitigating risks associated with third-party service providers.

9. **Cyber training and education** — Cyber training and education for employees can reduce the likelihood of user-related security incidents, potentially lowering insurance premiums.
10. **Background checks** — Conducting recurring background checks helps in minimizing insider threats, which can be a factor in negotiating lower cyber insurance premiums.

8. What are the common exclusions in cyber insurance?

- **Patent, software and copyright** — Cyber insurance policies often exclude patent-, software- and copyright-related scenarios. However, an IP insurance policy can cover patent, software and copyright.
- **Cyber warfare** — Business losses stemming from cyber warfare and attacks potentially tied to specific countries or governments are often excluded from coverage, as the risks are immense and exceed the capabilities of individual insurers.
- **Critical national infrastructure** — Losses resulting from disruptions or breakdowns in essential national infrastructure, including power, gas, water, satellite or telecommunications services, are not covered. Like war and terrorism exclusions, the magnitude of the risk surpasses what individual insurers can handle.

9. Recent developments and trends in cyber insurance

- A large life science company was hit by the NotPetya cyber attack, affecting 40,000 of its computers were wiped by NotPetya malware. The pharmaceutical company's $1.4 billion insurance claim from their insurance company was initially denied citing an "acts of war" exclusion. The pharmaceutical company sued the insurance provider and won in court, with the decision upheld in 2023. The ruling may influence future interpretations of war exclusions in cyber insurance policies.
- An American multinational confectionery, food and beverage company was hit by the same NotPetya ransomware attack, affecting 1,700 servers and 24,000 laptops, disrupting supply chains, and causing significant operational and financial damage. The company sought over $100 million from its insurance for recovery expenses. The parties reached a confidential settlement with specific terms undisclosed, highlighting potential gaps in cyber insurance policies regarding war exclusions.
- A mortgage company sued its insurance providers for $30 million over denied cyber insurance claims following a significant cyber attack. The insurers denied the claims, leading to the lawsuit. The dispute centers on policy coverage and exclusions. The case is ongoing, with potential implications for the interpretation of cyber insurance policies and coverage terms.
- Over the years, organizations have significantly enhanced their preparedness levels. It has been observed that many organizations now prefer to recover from backups rather than paying ransoms. This shift is driven by stricter insurance requirements and increased premiums, which have prompted companies to adopt robust measures such as air-gapped backups and thoroughly tested Business Continuity Plans.

10. What is the significance of cyber insurance?

The significance of cyber insurance in today's digital age cannot be overstated. As cyber threats proliferate, the scrutiny of cyber insurance policies has intensified, leading to a substantial rise in premiums. Consequently, organizations must enhance their security measures to become insurable and potentially reduce their premiums. Implementing measures, such as encryption, privileged access management, regular backups and network segmentation, can mitigate risks and demonstrate a proactive approach to cybersecurity, influencing insurance premiums positively.

For chief information security officers (CISOs) and senior security leaders, understanding the intricacies of cyber insurance is crucial. A robust security framework can lead to significant financial savings, particularly for large enterprises where premiums can run into millions of dollars. Moreover, the personal liability of CISOs in the wake of cyber incidents has become a pressing concern, with high-profile cases underscoring the potential legal ramifications.

In conclusion, the landscape of cyber insurance is complex and ever-changing. By enhancing their organization's security posture, CISOs can secure better insurance terms and safeguard their professional and personal interests. The insights provided aim to equip security leaders with the knowledge needed to navigate this challenging environment effectively, contributing to a more secure and resilient organizational framework.

Companies are re-evaluating the benefits they derive from cyber insurance policies. They are closely examining the extent of coverage these policies offer, particularly in the event of a cyber incident. Additionally, businesses are exploring alternative methods to manage their risk exposure, beyond solely relying on cyber insurance. This indicates a shift toward a more comprehensive approach to risk management in the face of evolving cyber threats.

Disclaimers-

- It is increasingly important for policyholders to thoroughly discuss exceptions to common exclusions with their insurers. Verifying that coverage meets unique needs requires detailed conversations to understand these exclusions and address any potential coverage gaps. This trend highlights the necessity for proactive engagement with insurers to secure comprehensive cyber insurance protection.
- EY does not take an official position on whether to include cyber insurance as a risk management strategy. The decision to purchase cyber insurance should be based on the organization's specific posture, business goals and strategic aspirations.

Contact us

Bill Fryberger
EY US Cybersecurity Advisory Leader
Ernst & Young LLP
bill.fryberger@ey.com
https://www.linkedin.com/in/wfryberger

Brian DePersiis
EY Americas Cybersecurity Strategy Leader
Ernst & Young LLP
brian.depersiis@ey.com
https://www.linkedin.com/in/briandepersiis

Special thanks to Abhijit Das, Brandon Bapst and John Bates for contributions to this content

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

SCORE US SCORE no. 25899-251US
2501-10598-CS
ED None

ey.com