AIATrust
Where smart architects manage risk®

An Architect's Guide to Buying Cyber Liability Coverage

By Insurance Buyers' Council, Inc.

2021 Update

Cyber Liability (also known as "cyber insurance," "privacy breach insurance" and "network security insurance") has become a hot topic over the past couple of years due to several high-profile cyber attacks. Almost every type of business has some exposure to cyber and privacy risk which makes this a universal concern for insureds.

This increasing awareness has fueled demand for cyber liability insurance. Becoming a buyer of cyber liability insurance starts with understanding the insurance product and how it addresses your cyber related risks as an architect. But first it's important to know what information to ask to become an educated and informed buyer.

Coverage Overview

As companies rely more and more on technology, they are also exposing themselves to both first party and third party cyber risks[1] which include:

- Identity theft as a result of security breaches where sensitive information is stolen by a hacker or inadvertently disclosed, including such data elements as Social Security numbers, credit card numbers, employee identification numbers, drivers' license numbers, birth dates, passwords, and PIN numbers.
- Business interruption from a hacker shutting down a network.
- Damage to the firm's reputation.
- Costs associated with damage to data records caused by a hacker.
- Theft of valuable digital assets, including customer lists, business trade secrets and other similar electronic business assets.
- Introduction of malware/ransomware, worms and other malicious computer code.
- Human error leading to inadvertent disclosure of sensitive information, such as an email from an employee to unintended recipients containing sensitive business information or personal identifying information.
- The cost of credit monitoring services for people impacted by a security breach.
- Lawsuits alleging trademark or copyright infringement (media liability related to website content).

Risk transfer via insurance is becoming a more prevalent method of managing cyber risk. This is one tool for insureds to consider in addition to establishing risk control measures. Cyber and privacy policies cover a business' liability for a data breach in which the customers' (or employees') personal information, such as Social Security or credit card numbers, is exposed or stolen by a hacker or other criminal who has gained access to the firm's electronic network. The policies cover a variety of expenses associated with data breaches, including: notification costs, credit monitoring, costs to defend claims by state regulators, fines and penalties, and loss resulting from identity theft[2].

Cyber insurance has adapted over the years to meet technology changes and advances as well as the evolving regulatory environment. This has led to many extensions and broadening of coverage on cyber policies to meet customer's needs.

Published by the AIA Trust, TheAIATrust.com

Typical coverage components:

- Privacy Liability – theft, loss and unauthorized disclosure of confidential information
- Network Security Liability - Unauthorized access or use of computer systems; denial-of-service attack against computer systems; infection by malicious code or transmission of malicious code
- Data Breach Expenses / Privacy Breach Response Services – such as:
    - Computer forensics
    - Expenses to comply with privacy regulations – including notifications
    - Voluntary notifications
    - Public relations firm / crisis management firm
    - Legal services
    - Credit monitoring
- Regulatory Defense and Penalties
- Network Extortion, including ransomware
- Social Engineering Fraud coverage
- Loss of income coverage
- Payment Card Industry (PCI) Fines, Expenses and Costs
- Website Media Content Liability

Coverage Evaluation

Factors beyond strict premium considerations should weigh in your cyber insurance purchase decision. Scope of coverage as well as insurer services are also vital.

As the cyber insurance product has gained popularity, the number of insurance carriers writing the coverage has also increased. However, as with any emerging insurance product, there is no standardized policy form. Therefore, comparing the policy forms to identify key coverage differences is needed before a potential buyer can make an educated decision.

The limit and retention structure play a large role in whether a proposal is competitive.

Coverage for data breach expenses is one of the most beneficial coverage elements of this type of policy. Some insurers offer breach expense limit structure options – of either a straight dollar limit or a per person approach subject to a maximum of affected individuals.

Most cyber insurance policies impose sub-limits in certain areas, such as crisis management expenses, notification costs or regulatory investigations. A breach response coverage sublimit could apply not just to credit monitoring and privacy liability but also to ransom negotiation and forensics services which means the sublimit could quickly become eroded. It is important to pay special attention to these sub-limits to make sure that they meet your needs.

It is also important to look for any objectionable exclusion or limitation included in the policy form and endorsements and to seek their removal. Remember that *purchasing insurance is a negotiation*.

Below are some areas that are important to delve into when comparing policy forms:

- Identify the limit structure (coverage limits; aggregate policy limit; sub-limits being imposed)
- Identify the coverage components being offered

- Are Data Breach expenses inside or outside the policy limit?
- What types of expenses are included for a data breach?
- Does the insured have choice of counsel and vendors or does the insurer select?
- Is there coverage for inadvertent disclosures (i.e., loss of thumb drive or laptop with unencrypted data)?
- What are the claims-made triggers (i.e., is there a retroactive date – from policy inception or full prior acts)?
- Is there coverage for violation of insured's own privacy or data handling policies?
- What coverage restrictions are being imposed?
- What are the proposal's subjectivities or conditions (underwriting requirements)?
- Does the application contain a warranty statement?
- Available Services: What loss prevention tools are available? Any fees associated with these services?

NOTE: Many insurers also offer a checklist of coverage items to compare against their competitors.

Claims and Risk Management Services

Understanding the claim process of the insurer that you select is critical since timely response to a breach event is essential to helping to mitigate the severity of the claim. Insurers have their 'preferred vendors' which offer the services outlined in the insurer's policy form. Since claim services are heavily dependent on these vendors, it is important to understand the role of the insurer and the vendor(s) during a breach event.

Before a breach event occurs, you should know what service providers are available for assistance so you can contact them soon as possible. Below are some examples of services that may be offered:

- 24/7 access to call center for claim reporting and guidance.
- Initial breach investigation and consulting such as access to a panel of domestic and international attorneys with local expertise in handling cyber claims as well as computer forensic services.
- Access to a risk management portal that provides educational and loss control information relating to compliance with applicable laws, safeguarding information, preparing to respond to breach incidents and best practices.
- Consultation with a breach coach and access to a breach response team to prepare for a cyber attack.
- Access to a network vulnerability assessment tool.

Recent Claim Trends

Ransomware attacks have increased year over year and are the top cyber related risk. Ransomware cost organizations around the world approximately $11.5 billion in 2019. These types of attacks have increased in 2020.[3]

There could be legal implications for ransomware payments. On October 1, 2020, the US Treasury Department's Office of Foreign Assets Control (OFAC) published an advisory reiterating the prohibition against US businesses and persons conducting business or paying funds to any person on the "Specially Designated Nationals and Blocked Persons" list.[4]

The pandemic has heighted problems with ransomware attacks. These types of attacks are preying on people's heightened anxiety and tricking them into sharing information. Also, with the shift to a remote workforce, work-from-home setups may have weaker security than corporate networks.[5]

Current State of the Cyber Insurance Market

In response to the increased frequency of ransomware attacks, insurers are raising rates and making coverage form changes. According to a recent cyber market report from a leading broker, cyber insurance rate hikes are anticipated at +10% to +30%, up from +10% to +15% earlier this year.[6]

During the underwriting process, insurers are asking about what cybersecurity controls an insured/potential insured has in place. The responses gathered by a company often is a great indicator of how strong or weak a company's protections are against cyber threats.

According to recent research conducted by Cowbell Cyber, 65% of small and medium-size businesses are planning to spend more on cyber insurance as part of their cyber resilience plan in the next two years.[7]

Conclusion

The unique exposures and liabilities associated with privacy breaches and cyber attacks are not properly addressed in traditional general liability and professional liability coverages. To help transfer the cyber risks identified above, you can evaluate the cyber policy options available to you and select the best match in terms of limits and coverage to meet your needs.

Insurance Buyers' Council, Inc.
Since 1948, Insurance Buyers' Council, Inc. (IBC) has had a mission to provide their clients with unbiased information. IBC is not affiliated with companies that sell insurance to assure that the information they provide is completely unbiased; they do not benefit financially from any insurance recommendations. Combined, IBC's staff possesses over 300 years' worth of experience in the insurance and risk management industries.

---

[1] National Association of Insurance Commissioners (NAIC) – Cybersecurity (article dated 11/17/16) - http://www.naic.org/cipr_topics/topic_cyber_risk.htm

[2] International Risk Management Institute (IRMI) - cyber and privacy insurance

[3] Insurance Business – Cyber crime tactics evolve during COVID-19 pandemic By Bethan Moorcraft (article dated 12/14/20)

[4] Marsh – Insights 2020 article - What OFAC's Ransomware Advisory Means for US Companies

[5] AmWINS 3rd Quarter 2020 State of the Market report

[6] Willis Towers Watson Insurance Marketplace Realities 2021 – Cyber risk survey report dated 11/18/20.

[7] Cowbell - Cowbell Cyber Finds Small-to-Medium-Sized Enterprises (SMEs) More Likely to Adopt Cyber Insurance by Cowbell Cyber dated Jun 18, 2020.