Coverage Insights

Brought to you by: Tooher-Ferraris Insurance Group

Tooher-Ferraris Insurance Group

Common Components of a Cyber Insurance Policy

In recent years, organizations of all sizes and sectors have become increasingly reliant on workplace technology and digital systems to conduct their operations. Nevertheless, utilizing such technology carries additional exposures and liabilities. That's why it's crucial to secure adequate cyber coverage.

Having a cyber insurance policy in place can provide protection against financial losses that may result from a range of cyber incidents, including data breaches, ransomware attacks and phishing scams. Especially as these kinds of incidents continue to surge in both cost and frequency, organizations simply can't afford to ignore the importance of cyber coverage.

Specific cyber insurance offerings differ between carriers. Furthermore, organizations' coverage needs may vary based on their particular exposures. In any case, cyber insurance agreements typically fall into two categories—first-party coverage and third-party coverage. It's best for policyholders to have a clear understanding of both categories of coverage in order to comprehend the key protections offered by their cyber insurance. This article outlines the primary components of a cyber insurance policy.

First-party Coverage

First-party cyber insurance can offer protection for losses that an organization directly sustains from a cyber incident. Types of first-party coverage include:

- **Incident response costs**—This coverage can help pay the costs associated with responding to a cyber incident. These costs may include utilizing IT forensics, hiring external services and restoring damaged systems.
- **Data recovery costs**—Such coverage can help recover expenses related to reconstituting data that may have been deleted or corrupted during a cyber incident.
- **Business interruption loss**—This coverage can help reimburse lost profits or additional costs incurred due to the unavailability of IT systems or critical data amid a cyber incident.
- **Contingent business interruption loss**—Such coverage can assist with expenses stemming from business interruptions caused by a third-party cyber incident (e.g., a supplier, vendor or utility).
- **Cyber extortion**—This coverage can help pay costs associated with hiring extortion response specialists to evaluate recovery options and negotiate ransom payment demands (if applicable) during a cyber incident.
- **Reputational damage**—Such coverage can help recover lost revenue related to higher customer churn rates and reduced sales resulting from poor publicity following a cyber incident.
- **Financial theft and fraud**—This coverage can help reimburse direct financial losses stemming from the use of workplace technology to commit fraud or theft of securities, money or other property.
- **Physical asset damage**—Such coverage can assist with expenses resulting from the destruction of hardware or other physical property due to a cyber incident.

Third-party Coverage

Third-party cyber insurance can provide protection for claims made, fines incurred or legal action taken against an organization due to a cyber incident. Types of third-party coverage include:

- **Data privacy liability**—This coverage can help recover the costs of dealing with third-party individuals who had their information compromised during a cyber incident. These costs include notifying impacted individuals, offering credit-watch services and providing additional compensation.
- **Regulatory defense**—Such coverage can help pay fines, penalties and other defense costs related to regulatory action or privacy law violations stemming from a cyber incident.

- **Multimedia liability**—This coverage can help reimburse defense costs and civil damages resulting from defamation, libel, slander and negligence allegations associated with the publication of content in electronic or print media. Multimedia liability coverage can also offer protection amid copyright, trademark or intellectual property infringement incidents.
- **Network liability**—Such coverage can help recover expenses related to third-party liability concerns that may arise from a cyber incident affecting IT networks. Network liability coverage can also provide protection in the event that cybercriminals pass through IT networks to attack other parties (e.g., customers, investors or suppliers).
- **Technology errors and omissions liability**—This coverage can reimburse costs associated with third-party claims alleging technical service or product failures, including claims filed in response to a cyber incident.

For More Information

Overall, it's evident that cyber insurance has become increasingly vital for organizations across industry lines. By securing proper coverage and understanding the key elements of their policies, organizations can stay properly protected against various cyber threats.

For additional insurance guidance and solutions, contact us today.

This Coverage Insights is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel or an insurance professional for appropriate advice.