The Value of Cyber Insurance

As cyberattacks become more frequent and costly, it's crucial for organizations to maximize their financial protection against related losses by purchasing sufficient insurance. Cyber coverage, also known as cyber liability insurance, can help organizations pay for a range of expenses that may result from cyber incidents—including (but not limited to) data breaches, ransomware attacks and phishing scams.

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 highlights the value of cyber insurance by outlining common first- and third-party coverage offerings.

First-party Coverage

First-party cyber insurance can offer financial protection for losses that an organization directly sustains from a cyber incident. Covered losses generally include the following:

- **Incident response costs**—This coverage can help pay the costs associated with responding to a cyber incident. These costs may include utilizing IT forensics to investigate the breach, restoring damaged systems, notifying affected customers and setting up call center services.
- **Legal costs**—Such coverage can help pay for legal counsel to assist with any notification or regulatory obligations resulting from a cyber incident.
- **Data recovery costs**—This coverage can help recover expenses related to reconstituting data that may have been deleted or corrupted during a cyber incident.
- **Business interruption losses**—Such coverage can help reimburse lost profits or additional costs incurred due to the unavailability of IT systems or critical data amid a cyber incident.
- **Cyber extortion losses**—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 pay for crisis management and public relations services related to a cyber incident.

Third-party Coverage

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

- **Data privacy liability**—This coverage can help recover the costs of dealing with third parties who had their information compromised during a cyber incident. These costs may include handling third-party lawsuits or legal disputes, 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.
- **Media 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.

Conclusion

As a whole, it's evident that cyber insurance can make all the difference in helping organizations avoid large-scale financial losses amid cyber incidents. It's best for organizations to consult trusted insurance professionals to discuss their particular coverage needs. Contact us today for more risk management guidance and coverage solutions.