CYBERRISKS&LIABILITIES

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.

Cyber Security for Small Business

High-profile cyber-attacks on companies such as Target and Sears have raised awareness of the growing threat of cybercrime. Recent surveys conducted by the Small Business Authority, Symantec, Kaspersky Lab, and the National Cybersecurity Alliance suggest that many small business owners are still operating under a false sense of cyber security.

The statistics of these studies are grim; the vast majority of U.S. small businesses lack a formal internet security policy for employees, and only about half have even rudimentary cyber security measures in place. Furthermore, only about a quarter of small business owners have had an outside party test their computer systems to ensure they are hacker-proof, and nearly 40% do not have their data backed up in more than one location.

Don't Equate Small with Safe

Despite significant cyber security exposures, 85% of small business owners believe their company is safe from hackers, viruses, malware, or data breaches. This disconnect is largely due to the widespread, albeit mistaken, belief that small businesses are unlikely targets for cyber-attacks.

Data thieves are simply looking for the path of least resistance. Symantec's study found that 43% of attacks are against organizations with fewer than 250 employees.

Outside sources like hackers aren't the only way your company can be attacked—often, smaller companies have a family-like atmosphere and put too much trust in their employees. This can lead to complacency, which is exactly what a disgruntled or recently fired employee needs to execute an attack on the business.

Attacks Could Destroy Your Business

As large companies continue to get serious about data security, small businesses are becoming increasingly attractive targets—and the results are often devastating for small business owners.

According to a recent study by the Ponemon Institute, the average annual cost of cyber-attacks for small and medium-sized businesses is over $2 million. Most small businesses don't have that kind of money lying around, and as a result, nearly 60% of small businesses victimized by a cyber-attack close permanently within six months of the attack. Many of these businesses put off making necessary improvements to their cyber security protocols until it was too late because they feared the costs would be prohibitive.

10 Ways to Prevent Cyber Attacks

Even if you don't currently have the resources to bring in an outside expert to test your computer systems and make security recommendations, there are simple, economical steps you can take to reduce your risk of falling victim to a costly cyber-attack:

1. Train employees in cyber security principles.
2. Install, use and regularly update antivirus and antispyware software on every computer used in your business.
3. Use a firewall for your internet connection.
4. Download and install software updates for your operating systems and applications as they become available.
5. Make backup copies of important business data and information.

6. Control physical access to your computers and network components.
7. Secure your Wi-Fi networks. If you have a Wi-Fi network for your workplace, make sure it is secure and hidden.
8. Require individual user accounts for each employee.
9. Limit employee access to data and information, and limit authority to install software.
10. Regularly change passwords.

In addition to the listed tips, the Federal Communications Commission (FCC) provides a tool for small businesses that can create and save a custom cyber security plan for your company, choosing from a menu of expert advice to address your specific business needs and concerns. It can be found at www.fcc.gov/cyberplanner.

Conclusion

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.