ARTICLE

Dropsuite

Cyber Insurance: A Key Element in a Proactive Security Strategy

Introduction

Cyber-attacks are more common and costlier than ever before, largely due to the growing dependence on information technology and the accelerated pace of digital transformation. Large-scale ransomware attacks like that on the Colonial Pipeline[i] and malware attacks such as the SolarWinds attack[ii] highlight the growing threat to businesses of all sizes. In fact, businesses are experiencing on average 130 security breaches per year per organization[iii].

Ransomware attacks are among the most prominent: the number of organizations hit with ransomware in 2021 was 66%, up from 37% the prior year[iv]. While the average ransom paid is more than $800,000, the cost to remediate a ransomware attack is a massive $1.4 million[v].

Cyber security has rapidly become a board-level issue as a majority of companies indicate the board wants to understand the company's ransomware protection levels and is making security a budgetary priority[vi].

As the threats grow, so too do the number of businesses turning to cyber insurance for protection from financial losses. Here we explain what cyber insurance is, how it works, what it costs, and what to look out for.

Cyber Insurance Defined

Cyber insurance, also called cybersecurity insurance or cyber liability insurance, is a contract that a business can purchase to help manage cyber risk and recover from losses associated with cyber-attacks.

Similar to auto or homeowners insurance, cyber insurance protects businesses from losses caused by an event covered under the user's policy. What's covered, the costs of that coverage, and the terms of a policy can vary, but cyber insurance can help businesses manage cyber risks and recover from losses associated with attacks, including disruptions in business and legal expenses. Cyber insurance can be a valuable asset and a reliable safeguard, as long as you go in with your eyes wide open.

Two types of Cyber Insurance and What They Cover

Most cyber insurance policies include two types of coverage: first-party and third-party.

First-party coverage (sometimes called data breach insurance) applies to the costs that directly affect your company. It is especially important for retailers, as well as any organization that collects credit card data.

First-party coverage typically covers business costs related to:

- Legal counsel – to determine your obligations regarding notification and regulatory compliance
- Customer notification (and sometimes call center services)
- Crisis management and public relations
- Forensic services to investigate a breach
- Recovery and replacement of lost or stolen data
- Lost revenue
- Fees, fine, and penalties associated with the breach

Third-party coverage provides coverage for claims that are made against your business by injured third parties. Companies that worry about a customer blaming them for failing to prevent a data breach that impacts their data may choose third-party cyber insurance in addition to first-party insurance.

Third-party coverage generally includes:

- Payments to consumers affected by the breach

- Claims and settlement expenses arising out of lawsuits
- Losses related to copyright or trademark infringement or defamation
- Costs for litigation and responding to regulatory inquiries
- Settlements, damages, and judgments
- Accounting costs

Who Needs Cyber Insurance?

It turns out that just about every business and organization needs cyber insurance. If you handle credit card numbers or any personally identifiable information (PII), if you need to comply with state regulations requiring you to notify customers of a data breach involving PII, if you work in the cloud, you should seriously consider cyber insurance. In short, any business that creates, stores, and manages customer or employee data online could benefit from cyber insurance.

Cyber insurance is especially important for small businesses, since they are often attractive targets due to the perception that they have weak security. For many, a cyber-attack can spell financial disaster: 60% of small businesses go under within six months of a cyberattack[vii]. Cyber insurance can dramatically reduce the financial impact of a breach.

60% of small businesses go under within six months of a cyberattack. Cyber insurance can dramatically reduce the financial impact of a breach.

Not Every Business Qualifies

All this sounds good, but purchasing cyber insurance is not a slam dunk. Businesses need to meet some stringent requirements in order to qualify. In the early days of cyber insurance, underwriters would rely on questionnaires to determine the risk posture of a potential policyholder. Today they know that approach is insufficient to determine how effective an organization's security controls really are. Instead, many insurers require their clients to meet the CIS Critical Security Controls®, which embody cybersecurity best practices and are recommended for adoption by many cyber laws and regulations[viii].

CIS Controls May Be a Requirement for Cyber Insurance

CIS Controls include 18 cybersecurity requirements, many of which are just good business. Basic requirement: inventory and control all enterprise and software assets, classify and manage data, and maintain secure configuration of enterprise assets and software. Strong identity and access management controls include assigning and managing authorization and access to accounts and services, especially administrator and service accounts.

CIS Controls are strict when it comes to continuous vulnerability management and review/control of audit logs, as well as ensuring email and web browser protections and anti-malware solutions are in place, used, and up to date. Security awareness and training are key requirements for cyber insurance, since so many enterprise cyber risks stem from phishing and social engineering attacks. Network management and monitoring are important, as well as ensuring the security of service providers.

An MSP can act as a trusted advisor, explains Daniel Johnson, CEO of MachineLOGIC. ""The CIS Controls are not overly technical in how they are presented, making them much more approachable by a business owner and their MSP partner. As the MSP, we can help our client assess each CIS control and work together on how it can be met through a combination of technology solutions, policy, reporting, or a change to the business workflow."

"CIS Controls are approachable by a business owner. An MSP can act as a trusted advisor, helping the client assess each control and how it can be met."

– Daniel Johnson, CEO, MachineLOGIC

Secure Backup and Recovery

Some of the most important requirements relate to the insurer's ability to accurately quantify cyber risk and then use that assessment to price the cyber insurance premiums: they do this by assessing the security of backup and the adequacy of data recovery. Many organizations believe that if they have cloud backup, that is sufficient. However, misconfigured identities, machines publicly exposed to the internet, third-party identities with the ability to elevate privileges, and similar issues can render a normal backup insufficient to recover from a cyber-attack, especially in the case of a ransomware attack.

To minimize risk, insurers want to feel confident about the security and resiliency of the backup architecture. They

also stress the need for comprehensive search and audit capabilities, encryption, role-based access, and multi-factor authentication. All these are important because they not only protect data, but they can also alert you to any modification to stored data and ensure the recovery processes will function as expected if there is a breach. Equally important is the ability to restore data quickly, which becomes vital not just in regulated industries but also in any company that needs to investigate an HR complaint or an IP issue.

Secure backup should include encryption, role-based access, multi-factor authentication and comprehensive search and audit capabilities.

The 18 CIS Critical Security Controls

1. **Inventory and control of enterprise assets:** Inventory, track, and correct all assets (end-user and network devices, IoT and servers) on the network and in the cloud, because you can't defend what you can't see.
2. **Inventory and control of software assets:** Actively manage all software to ensure only authorized software is installed and can execute, and can be patched when needed.
3. **Data protection:** Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data during its lifecycle, including encryption at rest and in transit.
4. **Secure configuration of enterprise assets and software:** Change default configurations to strong initial and continually managed configurations to avoid degrading security.
5. **Account management:** Assign and manage authorization to credentials for user, administrator, and service accounts through a comprehensive identity and access management program.
6. **Access control management:** Create, assign, manage, and revoke access credentials and privileges for enterprise assets and software based on minimal authorization needed for a role.
7. **Continuous vulnerability management:** Continuously assess and track vulnerabilities on all enterprise assets, via vulnerability scanning tools and a verified patching process.
8. **Audit log management:** Collect, alert, review, and retain audit logs of events to help detect, understand, and/or recover from an attack.
9. **Email and web browser protections:** Improve protection and threat detection through required use of fully supported browsers and email clients and relevant filtering services.
10. **Malware defenses:** Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.
11. **Data recovery:** Establish and maintain strong data recovery practices including backup and retention procedures, encryption, role-based access, multi-factor authentication and comprehensive search and audit capabilities.
12. **Network infrastructure management:** Establish, implement, and actively manage network devices to prevent attackers from exploiting vulnerable network services and access points.
13. **Network monitoring and defense:** Establish and maintain centralized security event monitoring, host-based and network intrusion prevention and detection solutions.
14. **Security awareness and skills training:** Regularly conduct up-to-date security awareness training including authentication and data handling best practices to reduce cybersecurity risks.
15. **Service provider management:** Develop a process to evaluate service providers who hold sensitive data or are responsible for the enterprise's critical IT platforms or processes to ensure appropriate protection.
16. **Application software security:** Manage the security lifecycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses.
17. **Incident response management:** Develop and maintain an incident response capability (policies, plans, procedures, roles, training, communications) to prepare, detect, and quickly respond to an attack.
18. **Penetration testing:** Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls and simulating the objectives and actions of an attacker.

What it costs

Cyber liability insurance can be an affordable option for a small business. Many – 27% – of small businesses pay less than $1000 per year, while another 36% pay between $1000-

$2000ix. In general, if a business handles a few thousand records, it may choose a policy with a $1 million occurrence limit, and a $1 million aggregate limit. This can help avoid financial devastation following a serious cyber-attack. Business that handle many more records containing PII or that are in regulated industries such as healthcare may need higher limits.

Factors affecting policy costs include the amount and types of sensitive data, the industry, related claims history, revenue, coverage limits, and the number of employees. Of course, the choice of first-party and/or third-party coverage impacts price as well. Pricing of policies and the amount of coverage offered are changing rapidly as the demand for cyber insurance grows, threats evolve, and insurance companies struggle to keep up with trends.

Many small businesses pay less than $1000 per year for cyber insurance.

Buyer Beware

It is easy to see the attraction of cyber insurance for many businesses. The idea of sharing or offloading risk is enticing, but be careful not to make assumptions about what the insurance will and will not do. When looking into cyber insurance, take the time to understand exactly what the policy you are considering actually covers, and how.

Check to see if the policy will cover human error(88% of all data breaches) or insider attacks. Many do not. They may also fail to cover pre-existing vulnerabilities, so not patching a known vulnerability in a timely manner could render the expected coverage nonexistent. Some will not cover the long-term consequences of a breach (imagine the years-long effects of an Advanced Persistent Threat.) Others may not respond in the case of intellectual property theft. Take the time to look carefully at the policy and feel free to ask questions to ensure you understand its full scope. A trusted MSP can help you understand both your current security posture and the coverage you need.

If it is important that you purchase a policy that will provide defense of your business in a lawsuit or regulatory investigation, make sure to look for "duty to defend" wording.

Sub-limits on the policy can be extremely important. Carefully read the binder letter (the document you receive before the policy goes into effect) to make sure you understand the specific coverage for individual risks. While you may think you are purchasing a $1 million policy, the details included in the binder letter may indicate that, for example, your business email compromise (BEC) protection is covered as social engineering fraud, with a much lower limit of coverage. Don't wait until a breach occurs to find out the details.

Another key item to investigate is whether the policy pays "on behalf of" or "by reimbursement". The former means that the policy pays costs up front, while the latter means that you, the business, will pay costs and then request reimbursement from the insurance company later. Each has its pros and cons: "on behalf of" saves your company money in the short term, but you don't control the timing of the payments and cannot easily see when your limits are being reached. "By reimbursing" gives you more control, but you may have to come up with significant amounts of money in the event of a breach –something that may not be possible for all businesses.

Final Words of Advice

Cyber insurance may be one of the best solutions your business could invest in for your future. It covers a wide range of expenses resulting from a data breach and/or cyber-attack. However, it may be difficult to determine which insurer to go with, what type of policy to choose, and how to read the fine print to understand exactly what is covered, and to what extent.

The best advice for many businesses is to turn to your MSP for advice on cyber insurance consultants or trusted brokers who can help you decide both the policy specifics and the coverage limits. Armed with the MSP's assistance with security best practices and areas of potential exposure and liability, the consultant can better understand your capacity for risk and its effect on the type of coverage you seek. Matt Lee, Senior Director of Security and Compliance at Pax8, advises, "A cyber insurance consultant can help clients understand the nuances of insurance. They can benefit from having someone who can look at the market as it changes, and help guide clients to the right policy and the right coverage."

A positive byproduct of the cyber insurance exercise is that your business will probably increase its cybersecurity maturity level. By working with the MSP to ensure all 18 CIS Controls are in place, you can close gaps and shore up defenses across the board. Insurers are demanding this level of security maturity, to help them make cyber protection work for both their companies and the insured. Today, rather than relying on questionnaires or subjective assessments, organizations can take steps to improve their security posture and the way they communicate it to insurance companies, customers, and the leadership

team. All told, cyber insurance can be a valuable asset and a reliable safeguard for any business, regardless of its size.

References

i. Colonial Pipeline Cyber Incident
ii. What You Need to Know About the SolarWinds Supply-Chain Attack
iii. Cyber Security Statistics The Ultimate List Of Stats Data, & Trends For 2022
iv. The State of Ransomware 2022
v. Ibid
vi. 2022 Cyber Insurance Market Trends Report
vii. 60 Percent of Small Businesses Fold Within 6 Months of a Cyber Attack.
viii. Cyber Insurance Conundrum: Using CIS Critical Security Controls for Underwriting Cyber Risk
ix. Cyber Liability Insurance

CONTACT US

For more information, please contact us:
www.dropsuite.com | sales@dropsuite.com