Readying Your Business for Effective Cyber Liability Insurance Coverage

WHITEPAPER

TOPICS COVERED

Businesses today rely heavily on the digital world to fuel their operations, and as such, they happily enjoy the associated benefits of convenience, profitability, flexibility and more.

That convenience, however, is counter-balanced by the ever-evolving security threat landscape. As businesses scramble to keep up and fortify their technology environments with critical security defenses, cybercriminals remain at the ready to take advantage of any potential vulnerability.

The aggressive evolution of cyber threats — both in sophistication and speed — has resulted in a pressing need for organizations to prepare for the "when" rather than the "if". As an added layer of necessary protection, businesses are also turning to cyber liability insurance to fortify their protection.

omega systems
technology managed

Why Organizations Turn to Cyber Liability Insurers

Cyber liability insurance is designed to protect businesses from the financial losses associated with data breaches, theft and disruptions resulting from cybersecurity incidents. Policies often cover legal fees, regulatory and compliance penalties, recovery expenses, criminal investigations and other associated financial impacts.

The need for cyber insurance coverage has grown exponentially in recent years, as more and more businesses of varying sizes have experienced cyber-related incidents.

71%

of respondents to the World Economic Forum's Global Cybersecurity Outlook 2022 report have cyber insurance either to:

1. Limit financial liability for specific cyber incidents or
2. Benefit from incident response and cyber professional services made available through an insurance carrier.

10 Things You Need to Know About Cyber Liability Insurance

01. You probably need it. Every business in every industry is vulnerable to a cybersecurity incident. While of course there are varying levels of exposure, you should assume if your business handles any sort of sensitive information (customer PII, credit card/banking information, medical information, etc.), that you need cyber liability coverage. Your standard corporate policy likely does not cover cybersecurity-related incidents, and thus, you'll need to explore standalone coverage.

02. It won't be a cakewalk to get it. Truth be told – securing cyber liability coverage is not a fast or easy process. Many businesses are finding it difficult to qualify, as carriers rapidly increase their expectations and standards. Insurance applications can be extremely detailed, and many providers also require companies to benchmark their cyber risk programs against comprehensive compliance frameworks such as NIST.

03. It won't be cheap either. Easy? No. Inexpensive? Also no. Cyber insurance premiums over the last two years have skyrocketed and are expected to continue increasing an average of 20-30% per year. Of course, specific policy premiums will be reflective of many different variables.

04. There are a variety of factors that may influence your coverage. Size, geography, regulatory requirements, and industry are just a few of the factors that will influence your business' cyber insurance quote. Industries like healthcare & financial services, in particular, are frequently targeted by hackers; as a result, their coverage is often more expensive.

05. Coverage is ultimately determined by your organization's level of risk. In addition to the aforementioned variables, your company's insurance coverage will most significantly be dictated by your level of security risk – and the programs you've implemented to mitigate said risk. Most businesses, unfortunately, have very little insight into their specific risks and vulnerabilities, as well as how those risks correlate to the value of their sensitive data. Emerging technologies like data discovery can give companies a leg up in identifying critical vulnerabilities and providing transparency into the potential financial impact of security incidents.

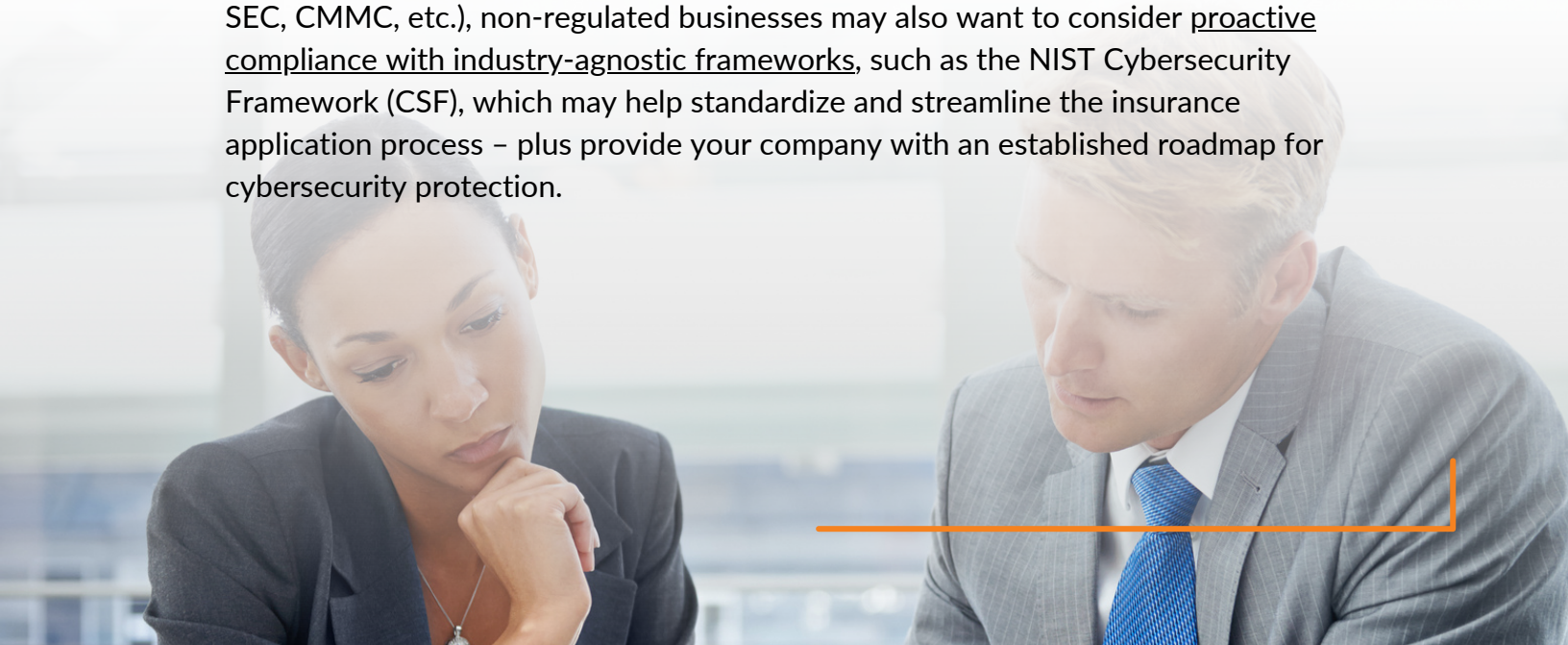
06. Not everything will be covered. Every policy is different, but most cyber liability policies do not cover future financial losses, system and technology upgrades, and impacts to company valuation/market share.

07. Coverage will likely include some potentially expensive ramifications. Liability coverage for cybersecurity does typically include a number of relatively costly items that could result in the event of a cybersecurity breach or incident, including forensic costs, cyber extortion/ransomware costs, legal fees and lawsuits, and certain regulatory fines.

08. Technology is a big focus (obviously). Because of the nature of most cybersecurity breaches and incidents, your cyber insurance application will primarily focus on technology and systems you have in place to protect your network and sensitive data. From firewall protections to monitoring tools to multi-factor authentication software, carriers will ask detailed questions about your hardware and software infrastructure.

09. But policies are critical too. While information gathering, cyber insurance carriers will also focus on the policies and procedures you've implemented to both prevent cybersecurity risk AND respond to incidents that inevitably occur. This level of detail will help providers verify that you've taken the necessary time to think through potential vulnerabilities across your organization and the necessary steps to take to thwart and react to serious cyber incidents.

10. Regulatory compliance will work in your favor. As part of the cyber insurance application process, carriers will want to know if your business is subject to or voluntarily follows any regulatory frameworks or best practices. While certain industries may require compliance with regulatory guidelines (e.g. HIPAA, PCI DSS, SEC, CMMC, etc.), non-regulated businesses may also want to consider proactive compliance with industry-agnostic frameworks, such as the NIST Cybersecurity Framework (CSF), which may help standardize and streamline the insurance application process – plus provide your company with an established roadmap for cybersecurity protection.



Shocking Cyber Liability Considerations

- Businesses can be turned away for renewals when cybersecurity protections have not been implemented within a certain period of time (e.g. within the past year).
- Premiums can soar well over 300% compared to prior years if protections are lacking as compared to the threat landscape.
- It's nearly impossible to find true cyber liability coverage without multi-factor authentication (MFA).
- Every cyber liability policy is different, therefore understanding the language and asking questions to a policy provider is key.
- Many small businesses have cybersecurity insurance coverage as part of their standard property/liability policy, however this often results in a lack of coverage, should they experience a loss.
- Some insurance companies no longer offer stand-alone cyber liability insurance policies.

12 Focus Areas for Cybersecurity Compliance

(from the Independent Insurance Agents & Brokers of America)

01	**Risk Assessment** Intended to identify and prioritize risks and vulnerabilities present in your organization's infrastructure and controls
02	**Written Security Policy** Should outline your organization's processes and procedures for mitigating cybersecurity risk, including access control, data privacy, monitoring, oversight and governance, and business continuity
03	**Incident Response Plan** In addition to your written information security policy (WISP), you should also document an incident response plan that outlines how your organization will respond in the aftermath of a cybersecurity breach or attack
04	**Employee Training** How you educate and train employees on evolving cybersecurity risks and how to mitigate them; examples include annual cybersecurity awareness training and phishing exercises
05	**Penetration Testing & Vulnerability Scanning** Intended to identify vulnerabilities in your organization's network and systems that could be threatened inadvertently or maliciously
06	**Access Control** Details how your organization manages and restricts access to sensitive information across networks, systems, applications and other on-site and online access points
07	**Third Party Risk Policy** Outlines your organization's approach to third party risk management, including how you manage vendors' access and control over your organization's data and resources
08	**Data Encryption** A technology method that ensures sensitive or confidential information is transmitted and stored securely to prevent unauthorized access
09	**Corporate Governance** Refers to how an organization maintains management and oversight of the company's policies, procedures and practices related to cybersecurity risk management
10	**Audit Trail** Tracks and maintains a record of activity across your organization's network to document how data is accessed, altered and shared
11	**Multi-Factor Authentication** A security functionality that requires users to provide independent verification to access systems, applications and devices across the organization
12	**Disposal of Non-Public Information** Refers to policies and practices that ensure sensitive information is securely removed, deleted or destroyed

Factors That Impact Premiums

Are your employees trained to spot the latest cyber threats?

Cybersecurity Awareness Training helps address the #1 threat to organizational security – human error! Hackers depend on taking advantage of users' ambivalence and oversight and will use phone calls, emails, texts, links and other methods of communication to trick users into sharing sensitive information or financials. Regular security training should educate employees on the types of threats to be aware of and provide them with actionable steps they can take to assess the validity of incoming threats via phishing and other advanced methods.

Have you performed data discovery and classification?

If you don't know what data is valuable to your business or the impact theft or loss of that data could have, how can you effectively protect it from would-be hackers? Organizations are often guessing what hackers are stealing and why. They focus on protection and skip the fundamental measure of identifying what data needs to be protected and how theft or loss of that data is impactful on their business. It's imperative to understand what kind of data your business stores and shares, where this data is located, and who has access to it in order to effectively implement safeguards to secure it.

Insurers want to identify an organization's loss history.

They have a vested interest in finding out how the vulnerability has been addressed to ward off future attacks.

Are your applications and systems updated?

Outdated hardware and software can lead to gaping vulnerabilities and provide hackers with easy access to your organization's data. Patch management is critical and will add an important layer of defense to thwart entry through potentially vulnerable access points.

Do you have sufficient backup?

Whether your data resides on local servers, end user computers or in the cloud, it is crucial to implement secure, remote backup to enable fast recovery in the event of a breach or data loss event.

Do you have a loss history?

Gaps in cybersecurity understanding and lack of awareness leave organizations exposed to risk. Unfortunately, cyber liability insurers see repeat offenders — previous breach victims that often believe an attack won't happen again. Unfortunately, the opposite could be true. If a hacker feels their attack was successful, they sometimes retarget the same businesses.

Where are your business and customers located?

Since sensitive data is subject to state-level laws and regulations, insurers look at location as a means to determine cyber liability and litigation costs.

A phenomenon study from Help Net Security indicates:

50% of cybersecurity attacks are from repeat offenders & **61%** of these were never resolved.

Building a Comprehensive Cybersecurity Program

We've only just scratched the surface in terms of outlining cybersecurity protection requirements for sufficient liability coverage. Your business' needs will depend on a multitude of variables, including your size and structure, technographics, regulatory oversight, and of course, your individual carrier's requirements. Fortunately, Omega Systems has deep experience advising customers across various industries in pursuit of new or improved cyber liability coverage. Our security professionals can help guide you as you design and enhance your security posture across your infrastructure, endpoints, applications, controls and written policies and move closer to operating a comprehensive cybersecurity risk management program.

And with our managed IT compliance service, companies can appropriately assess the current state of their IT and cybersecurity environment to aid in securing cyber insurance coverage and guide overall compliance programs.

Contact us to get started today: **www.omegasystemscorp.com/contact-us/**