GOOD INTENTIONS PAVE THE ROAD TOWARDS NIST

The lack of cyber insurance in the supply chain is now a deal-breaker.

Currently, nefarious threat actors are capitalizing on our cyber vulnerabilities during COVID-19.

During the Pandemic and beyond, the DOD is tightening up supply chain cybersecurity measures. Thus, prime contractors will require their subcontractors to obtain cyber insurance.

As cyber threats rise, companies develop and implement cyber risk management strategies concurrently with the search for guidance on best practices.

Cyber insurance carriers may view companies in a more cyber-secure light when underwriting and pricing cyber insurance if they have followed the guidance of the NIST Frameworks.

As cyber threats rise, companies develop and implement cyber risk management strategies concurrently with the search for guidance on best practices.

Fortunately, organizations can rely on valuable guidance:

- The National Institute of Standards and Technology (NIST) -- guiding information security and data privacy, and
- The Committee of Sponsoring Organizations (COSO) of the Treadway Commission – guiding business executives and board members on cyber risk management investments

Organizations looking to adopt and adapt a COSO/NIST Cybersecurity Framework are well-advised to take proactive steps to design, implement, and manage their cybersecurity risk management, including:

- Get Digital Ready – begin at the operational level.
- Adopt and Adapt the COSO and NIST Cybersecurity Frameworks – prioritize investments and assess mission-critical capabilities.

> **"A GOOD INTENTION, WITH A BAD APPROACH, OFTEN LEADS TO A POOR RESULT."**
>
> THOMAS A. EDISON

- Become Part of the Cybersecurity Community – exchange knowledge and ideas with cybersecurity professionals in the same boat.
- Increase awareness of residual cyber risk -- every cyber threat cannot be prevented.
- Consider funding out-of-pocket costs after a cyber incident, such as investigation costs and business downtime.
- Develop a holistic cyber risk management plan – including cyber loss prevention and cyber insurance coverage.

The NIST Cybersecurity Framework

The NIST Cybersecurity Framework (NIST CSF), published in February 2014, and updated in April 2020, provides a uniform standard intended to guide government and businesses in their development and implementation of technical cyber risk management strategies.

The US government, industry sectors (e.g., financial services, healthcare, and energy), and international governments have approved NIST CSF as the governing framework. Thus, it functions as an umbrella over what is referred to as Informative References, including NIST 800-171.

NIST SP800-171 Protecting Controlled Unclassified Information in Non-Federal Systems and Organizations

NIST SP 800-171 is a Special Publication that provides recommended requirements for protecting the confidentiality of controlled unclassified information (CUI).

Defense contractors must implement the recommended requirements contained in NIST SP 800-171 to demonstrate their provision of adequate security to protect the covered defense information included in their defense contracts, as required by DFARS clause 252.204-7012.

NIST Special Publication 800-171, Revision 2, Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations (approved as final and published February 2020).

The protection of Controlled Unclassified Information (CUI) resident in nonfederal systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the federal government to conduct its assigned missions and business operations successfully.

Revision 2 provides recommendations on how to protect the confidentiality of CUI:

1. When the information is resident in nonfederal systems and organizations;
2. When the nonfederal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency; and
3. Where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or government-wide policy for the CUI category listed in the CUI Registry.

The requirements apply to all components of nonfederal systems and organizations that process, store, and transmit CUI, or that protect such components.

The CUI requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations.

Revision 2 provides minor editorial changes in Chapters One and Two, and in the Glossary, Acronyms, and References appendices. There are no changes to the primary security requirements in Chapter Three.

Third-Party Risks From Small and Medium-Sized Manufacturers

The results of the Ponemon Institute's third annual (2018) study Data Risk in the Third-Party Ecosystem indicate that 61% of US companies surveyed had experienced a data breach caused by their vendors or third parties (up 5% from 2017 and 12% from 2016). Dr. Larry Ponemon reported that companies need to take control of their third-party exposure and implement safeguards and processes to reduce their vulnerability.

Another recent Ponemon Institute report indicates that third-party data breaches cost more than in-house breaches, as much as $13 more per compromised record.

Cybercriminals target all sizes of manufacturers because they have valuable data such as employee and customer records, and banking and financial data.

Small and medium-sized enterprises (SMEs) often become accessible gateways into a prime contractor's network, leading to a data breach, ransomware attack, or business email compromise.

Surge in Cyberattacks on the Pentagon During COVID-19

Reports indicate that the DOD has faced unprecedented threats as hackers seek to take advantage of employees with security clearances who are forced to work from home. The threat is particularly insidious for the military and other elements of US national security during the Pandemic.

The Pentagon has seen a surge in cyberattacks, as hackers exploit restrictions from the Pandemic that force an unprecedented number of DOD employees to communicate almost entirely by computer systems. The attack vector of choice is social engineering. Cybercriminals exploit our inherent sense of trust, causing individuals to divulge passwords or wire funds to fraudulent bank accounts due to emails and text messages, ostensibly from a known source. The individual unwittingly gives hackers the keys to the castle, and from that point, they access their private networks.

A Lieutenant General in the Air Force commented that with great opportunities come significant challenges – referring to how the increase in remote work capacity may change the DOD for the better. But in the meantime, hackers are taking advantage of previously untested vulnerabilities.

During the Pandemic and beyond, the DOD is tightening up supply chain cybersecurity measures. Thus, prime contractors will require their subcontractors to obtain cyber insurance.

THE DOD IS TIGHTENING UP SUPPLY CHAIN CYBERSECURITY MEASURES. PRIME CONTRACTORS WILL REQUIRE THEIR SUBCONTRACTORS TO OBTAIN CYBER INSURANCE.

Contractual Obligations Drive Cyber Insurance Demand

Ultimately, contractual obligations are driving the demand for cyber insurance. Prime contractors have or will require cyber insurance in contract terms and conditions with subcontractors. Primes will no longer accept privacy and security risks from their vendors and suppliers.

The lack of cyber insurance in the supply chain is now a deal-breaker.

Stand-Alone Cyber Insurance

With the help of a robust stand-alone cyber insurance policy, you gain the services offered to assess your risk and prepare an incident response plan before you experience a cyber loss.

Location, Location, Location

Most cyber policies provide broad, affirmative coverage for a security event (as defined in the policy). That means that the cyber policy will provide coverage regardless of where the breach or security event occurs, in the workplace, or working remotely at home.

Social Engineering

Notably, in cyber insurance policies, social engineering coverage often refers to funds transfer fraud coverage where tricksters manipulate employees into sending funds to cybercriminals or fake bank accounts.

Recently, we reported on the issue of "Silent Cyber." Relying on other lines of insurance, such as commercial crime policies, or other non-affirmative cyber insurance policies, is a risky business. Resolving social engineering insurance coverage disputes in court is costly, time-consuming, with no guarantee of social engineering coverage.

CYBER INSURANCE IS A COMPLEMENTARY SOLUTION TO YOUR CYBERSECURITY PRACTICES, PROCEDURES & TOOLS UNDER THE NIST CSF

Ransomware

Many cyber liability policies provide cyber extortion coverage to protect your business against ransomware losses. During the COVID-19 crisis, we have seen new ransomware threats to businesses of all sizes, even to facilities tasked with saving lives.

For example:

- Ransom payments – when hackers lock your network or computer system demanding payment of ransom for the key to unlocking your system.
- Loss of business income (after a brief waiting period) -- during the cyber event.
- Extortion-related expenses – expenses incurred due to the extortion threat, such as expenses incurred to make the ransom payment and the cost of hiring a security expert for an incident response.
- Repair costs – losses due to damage, disruption, theft, or misuse of your data, such as the cost to restore, replace or reconstruct programs, software, or data.

Data Breach

Most cyber insurance policies provide data breach coverage, both first-party coverage costs for data breach response, investigations, legal notification obligations, and services, as well as third-party liability coverage for damages paid to third parties for claims or lawsuits.

Cyber insurance is a valuable, complementary solution to your cybersecurity practices, procedures, and tools under the NIST CSF and Informative References (e.g., NIST 800-171).

Takeaways

- During the COVID-19 Pandemic cybercriminals have increased cyberattacks due to increased vulnerabilities at businesses and government agencies.
- A holistic cyber risk management strategy includes both cybersecurity measures and robust stand-alone cyber insurance coverage.
- Residual cyber risks exist -- breaches, ransomware attacks, and fraudulent wire transfers happen. Cyber risks that cannot be mitigated should be covered by cyber insurance.
- The time has come to reach out to a specialized cyber insurance broker to set you on the right course towards holistic cyber risk management.

Reach out to a specialist cyber broker, such as Cyber Armada Insurance, to request and robust cyber solutions appropriate for your needs and cyber risk tolerance. We understand the evolving demands and expectations of cyber insurance clients.

Contact Cyber Armada today to examine how your company faces potential financial losses from business interruption caused by IoT or supply chain failure cause by a cyberattack. Contact us at 888.727.6232.

CYBER ARMADA
INSURANCE

888.727.6232 | info@cyber-armada.com | www.cyber-armada.com