CYBER RISK TRANSFERS FOR USG CONTRACTS

History reveals the proliferation of cyberattacks against the US Government

Cybersecurity regulations, frameworks, and standards highlight the need for improved cybersecurity compliance and capabilities. However, that is only one side of the equation. The other side of the equation is comprehensive (aka Stand-Alone) Cyber Insurance.

Stand-Alone Cyber Insurance is a crucial component of the USG contract process.

Your traditional commercial insurance policies will not likely provide the cyber insurance coverage needed to meet your USG contractual obligations or to protect your balance sheet after a cyberattack.

Since cyber insurance is not standardized, you need specialists to ensure that you obtain the coverage that is right for your business.

It is time for the talk – about cyber risks in the US Government (USG)

A shift is taking place in response to the ongoing history of cyberattacks on federal agencies' systems in the USG.

Significant Cyber Attacks on the Pentagon – During COVID-19 and Before

Reports indicate that the Department of Defense (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.

History reveals multiple incidents of cyberattacks on the DOD, as reported in Lawfare, from 2006 to 2012:

- *F-35 development – February 2012* – It was announced that delays and high costs for the development of fighter plane F-35 stemmed from responding to cyberattacks that stole classified information discussing the technology.

- *Unmanned aerial vehicle – December 2011* – Iran claimed to have gained possession of RQ-170 Sentinel stealth drone with a cyberattack.
- *Army – April 2010* – Lost personal data of reservists.
- *Unmanned aerial vehicle feeds – December 2009* – Downlinks from US military UAV's were hacked by Iraqi insurgents using inexpensive file-sharing software, allowing them to see what the UAV has viewed.
- *US Central Command – November 2008* – Classified networks at DOD and Central Command relating to US involvement in Iraq and Afghanistan were subject to a cyberattack.
- *Naval War College – November 2006* – The Naval War College in Rhode Island had to shut down all computer systems for two weeks following a cyberattack. The Naval War College develops strategies for naval warfare, as well as in cyberspace.
- *Non-Classified IP Router Network – August 2006* – A senior Air Force Officer announced that "China has downloaded 10 to 20 terabytes of data from the NIPRNet."

Steps to win USG Contracts

Regulations and Framworks

The Federal Acquisition Regulations (FARs) govern the procurement and acquisition process with US federal agencies. FARS is used by all executive agencies in their acquisition of supplies and services with appropriated funds.

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 USG, 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 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.

Cyber Solutions for Small and Mid-Sized Business (SMB)

How can a small or mid-sized business (SMB) successfully maneuver through this regulatory compliance process?

SMBs without a CISO, a Risk Manager, or a strong IT team, face the difficult task of extracting the information needed from each regulation, framework, or standard leading to the best outcomes, and even requisite certifications to be awarded government contracts.

Virtual Chief Information Security Officer (vCISO)

According to ISACA's State of Cybersecurity 2020 Report, and Surveys, organizations with unfilled cybersecurity roles anticipate, and suffer, more cyberattacks.

SMBs looking to connect the regulatory dots and develop a holistic cyber risk management plan may hire a Chief Information Security Officer (CISO), to guide them through this development process. A CISO is generally a senior-level executive who is responsible for establishing and maintaining the company's vision, strategy, and program to ensure information assets and technologies are adequately protected.

What if your business needs a CISO on a part-time or task-specific basis (e.g., to obtain Cyber Maturity Model Certification (CMMC), or to build an incident response plan?

A virtual CISO or vCISO is an outsourced security advisor (with the same function as a CISO) made fractionally available to you, on an as-needed basis. If you have a customer asking about how you are handling their data, or a regulator inquiring about compliance, or your board is asking if the company is addressing cyber risk as a business risk, then a vCISO could be a solution.

Focusing 2020 Vision on Third-Party Vendors and Suppliers

Third-Party Risk Management and Comprehensive Cyber Insurance are essential when preparing to bid for USG contracts

As the DOD embarks on a new road towards CMMC, prime defense contractors, and their third-party vendors and suppliers are keenly aware of the importance of third-party risk management (TPRM) within the supply chain. Contractors must ensure that their Subcontractors comply with data privacy and protection laws.

As we have reported, during the COVID-19 Pandemic, hackers have stepped up their cyberattacks to capitalize on reduced cybersecurity protection and increased human error while working from home.

Recently, Cyber Alliance Program released the Mimecast report indicating that ***COVID-19 boosted cyberattacks by 30% in 100 days.***

CONTRACTORS MUST ENSURE THAT THEIR SUBCONTRACTORS COMPLY WITH DATA PRIVACY AND PROTECTION LAWS

The Association for Data and Cyber Governance (ADGC) suggests that organizations assess the new terrain of remote work by third-party vendors to identify changes that may have occurred at a vendor by asking the right questions:

- Has the vendor gone out of business?
- Has the vendor made drastic cuts to its workforce, impacting the risk-management process?
- How has the Pandemic impacted their cybersecurity practice–and their stability?
- Has the vendor moved to any new technologies or networks to keep their workforce remote?
- Has the vendor assessed the elevated risk of an attack?
- Is the vendor in danger of a security lapse because they cannot pay for their security services?
- Has the vendor furloughed members of their IT or Security Team?
- Has the vendor conducted proper remote-work training for their employees?

If the answers to these questions raise any red flags, consider stepping in to help with security concerns, or ending the relationship with the vendor.

Owning Vendor Cybersecurity Challenges

Institutions should remember that they own their vendors' challenges

For example, earlier this year, when the New York Department of Financial Services (NYDFS) asked its members to file a plan on how to assess the financial risk arising from COVID, the plan called for an evaluation of any third party's cybersecurity preparedness.

Any cyber failure on the part of your vendor or supplier falls on your shoulders. That is the reason that prime contractors are shifting their focus on subcontractors in the USG contract process.

Your institution needs to:

1. Update Your Service Level Agreements, and
2. Obtain comprehensive Stand-Alone Cyber Insurance.

Update Your Service Level Agreements (SLAs)

The service level agreements (SLAs) between firms and their vendors contain critical information that might need to be reviewed and reworked considering changes brought on by the Pandemic.

In addition to the questions to ask each vendor (mentioned above), your organization should review the SLAs, confirming answers to some crucial questions about each vendor:

- What level of authentication is required to access the vendor's networks?
- Do vendors continuously monitor their network and all connected devices?
- What is the vendor's remote work policy?
- Does the vendor require their vendors to comply with security standards?

Contractors will need to seek the advice of legal counsel on SLAs.

Obtain Comprehensive, Stand-Alone Cyber Insurance

Your business can survive a cyberattack (directed at you or a third-party vendor) with the help of cyber insurance to protect your bottom line:

- If you suffer a data breach, your business will need to stop the breach, investigate, notify all those impacted, recover, or restore your data, and possibly face claims or lawsuits by injured parties.
- Surviving is difficult to do without an incident response plan/team to:
    - Stop a data breach or fend off a ransomware attack.
    - Investigate a data breach or ransomware attack to stop future cyberattacks.
    - Notify your clients, consumers, and employees (in compliance with various laws) after a cyberattack.
    - Assist you with recovering or restoring lost or stolen data.
    - Assist you with meeting your business continuity plan.
- If you suffer a ransomware attack, you can be compensated for the ransom payment (made with the prior written consent of the insurer) and for lost profits during the time business operations were disrupted or halted.
- If you are fined by regulators or credit card companies after a data breach, those fines are covered by cyber insurance (so long as allowed in the relevant jurisdiction under the particular facts of the matter).

Regularly updating your cybersecurity is step one. Requiring the same from your third-party service providers is step two. Obtaining robust Stand-Alone Cyber Insurance to transfer your residual cyber risk is step three

Notably, a contractor seeking NIST capabilities and compliance will be on a stronger footing after obtaining comprehensive, Stand-Alone Cyber Insurance.

Most importantly, cyber insurance is a crucial step for contractors and their subcontractors to increase their chances of winning USG contracts and protecting their financial status after a cyberattack.

Cyber insurance is a valuable, complementary solution to your cybersecurity practices, procedures, and tools (under the NIST CSF and NIST 800-171) as you pursue USG contracts.

Takeaways

- Ideally, third parties that access your network, touch your company, or touch your sensitive or critical data should have their own robust Stand-Alone Cyber Insurance to respond first to a cyber incident.
- You are advised to confirm this when you conduct your vendor cyber risk assessment, and when you negotiate relevant contract provisions (working with your legal counsel on SLAs).
- Amendments to regulations, frameworks, and standards seek to drive the change towards cybersecurity improvements – but that is not where the story ends.
- Cyber incidents continue regardless of an increase in cybersecurity measures due to human error and unforeseen attack vectors.
- Thus, the additional financial protection of comprehensive, Stand-Alone cyber insurance is essential.

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.

CYBER ARMADA
INSURANCE

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