WINNING GOVERNMENT CONTRACTS WITH CYBER INSURANCE

Cyber insurance may be the differentiator in bidding for government contracts.

The US government is seeking to protect critical data and stop the massive leakage of data that we have suffered at the hands of hackers and cybercriminals over the past fifteen years or more.

Companies doing business with the DOD need to prepare for the impact of CMMC requirements -- on them, their contractors, and subcontractors.

What will differentiate your company from the rest of the pack?

First, superb cybersecurity. The US government wants to stop the flow of critical data into the hands of hackers and cybercriminals.

Second, affirmative cyber insurance. Your company will undergo a cyber risk assessment to obtain a cyber insurance policy, providing your business with a jump start in the race to win government contracts

Cybersecurity Maturity Model Certification (CMMC)

Cyberattacks on supply chains are well-documented, and on the rise, especially during COVID-19. The US government is responding by increasing data protection requirements for companies to which they award government contracts.

Currently, the Department of Defense (DOD) contractors use self-attestation of adherence to requisite cybersecurity practices.

The Cybersecurity Maturity Model Certification (CMMC), taking effect in fall 2020, will require all defense contractors to have their cybersecurity status audited and certified by an independent third party before they can do business with the department.

CMMC ESTABLISHES CYBERSECURITY AS A FOUNDATION FOR FUTURE DOD ACQUISTIONS

Protected Information

CMMC aims to protect two kinds of information:

- **Federal Contract Information (FCI):** FCI is information provided by or generated for the Government under contract not intended for public release. The CMMC model uses the basic safeguarding requirements for FCI as the Federal Acquisition Regulation (FAR) Clause 52.204-21 and the security requirements for CUI as specified in NIST 800-171 / DFARS.
- **Controlled Unclassified Information (CUI):** CUI is information that requires safeguarding or dissemination controls pursuant to and consistent with laws, regulations, and government-wide policies, excluding classified information under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or Atomic Energy Act of 1954, as amended.

Five Levels of CMMC:

In late 2020, the DOD is scheduled to assign levels of cybersecurity maturity for companies to obtain CMMC and win specific government contracts.

Companies must protect their networks and demonstrate compliance via five levels (basic through advanced) of cybersecurity maturity.

The level of certification of cybersecurity maturity for prime contractors and subcontractors depends on the *nature of the contract* – aligning a set of processes and practices with the type and sensitivity of the information to be protected:

- **Level 1:** Safeguard Federal Contract Information (FCI)
- **Level 2:** Serve as a transition step in cybersecurity maturity progression to protect CUI.
- **Level 3:** Protect Controlled Unclassified Information
- **Level 4-5:** Protect CUI and reduce risk of Advanced Persistent Threats

CMMC Implementation

In a recent article in Medium, Leslie Weinstein, President of CMMC Consulting, discussed a recent market survey published by the Army for a future Assault Breacher Vehicle Remote Control System (ABV RCS) proposal. Here, the DOD will likely expect companies to pass the CMMC level 3 before awarding them a contract. That means the prime contractor will probably need to achieve CMMC level 3 before the contract award, and the prime's subcontractors will need to demonstrate their CMMC level (to be determined).

Weinstein emphasized the importance of cybersecurity for all companies doing business with the Government. Early adopters may have an unseen advantage to get ahead of competitors in the race for government deals.

Notably, industries with diverse supply chains should be aware of CMMC's impact, including Aircraft, Engine and Parts Manufacturing, Ship Building, and Space Vehicle and Missile Manufacturing.

Cyber insurance as differentiator

Cyber insurance may be the differentiator in bidding for government contracts.

A holistic cyber risk management plan relies on cybersecurity measures. However, there is another essential aspect of the program – affirmative cyber insurance.

An affirmative (aka stand-alone) cyber insurance policy provides specific, explicit cyber loss coverage as well as important pre-cyberattack and post-cyberattack services. Your company cannot rely on commercial insurance, outside of cyber insurance, for cyber loss coverage.

Your company has an opportunity to leverage your cyber insurance policy, and the underwriting risk assessment, which became the basis for your coverage and premium.

If you have a high-risk score, you will have the opportunity to pivot and improve your cybersecurity levels. That is a jump start right into the CMMC process.

More and more contracts require that all parties, your company, and your third-party vendors and supply chain, obtain cyber insurance.

More and more companies hiring third-party vendors or working with a supply chain are keenly aware of the impact of cyber insurance protection on winning deals.

Whether mandated by law or not, it makes good business sense to seek to stand out by acquiring cyber insurance as part of your efforts to win government contracts.

Takeaways

- CMMC will impact thousands of businesses looking to win government contracts.
- Preparation wins government contracts. Do not delay due to COVID-19.
- A holistic cyber risk management plan includes cybersecurity and cyber insurance.
- A cyber risk assessment offers you a window into your cybersecurity risk level
- A robust stand-alone cyber insurance policy may be the differentiator in winning government contracts.
- Cyber Armada's advocacy helps companies assess and fulfill security protocols and cyber hygiene as part of their cyber risk management.

CYBER ARMADA
INSURANCE

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