COVINGTON

What Every Defense Contractor Should Know About Insurance for Cyberattacks

March 19, 2018

Insurance/Government Contracts

Cyberattacks targeting defense contractors illustrate the need for cybersecurity, for thoughtful planning—and for insurance when security and planning prove insufficient. Understanding your insurance policies before things go wrong can help ensure financial protection when they do.

The Need for Robust Cybersecurity

The Department of Defense recognizes that unfriendly states target the Department's networks. A September 2015, DoD memorandum, "Department of Defense Cybersecurity Culture and Compliance Initiative," provides chilling insight: "30 million known malicious intrusions on DoD networks between September 2014 and June 2015." That translates to an average of 3 million attacks a month or 100,000 attacks a day. Ceaselessly.

Attackers also target contractors. Defense contractors handling Covered Defense Information ("CDI") have worked diligently to meet DoD's information safeguarding requirements. Under Defense Federal Acquisition Regulation Supplement ("DFARS") 252.204-7012, contractors must implement 110 security controls listed by the National Institute of Standards and Technology ("NIST") in Special Publication 800-171 if CDI resides, transits or is stored on their internal networks. The Basic Safeguarding clause at FAR 52.204-21 imposes a subset of these controls with regard to Federal Contract Information. Still, any information system that relies at least in part on human beings remains vulnerable to compromise.

Recent press stories revealed that a cyber-espionage group allegedly associated with Russia's military intelligence targeted defense contractor employees involved in sensitive programs. Deploying "social engineering" (*i.e.*, business email fraud), the hackers targeted the workers' personal email using innocuous-seeming messages to trick them into installing malicious software. Gaining access to employees' personal information would then allow operatives to create more effective "phishing" schemes targeting those employees when the employees were at work and using protected networks. This method certainly could work. In its September 2015 memorandum, DoD attributed 80% of successful attacks on its networks to human error.

The best technical controls and strongest training on cyber risks cannot fully insulate contractors from cyberattacks and their related costs. One study in the civilian sector estimated the average cost for each stolen confidential record as $141 with the average breach exceeding 24,000 records. The study implies average total costs per breach in the millions, not including loss for business interruption. These amounts likely understate the costs to a defense contractor if covered defense information is jeopardized. Defense contractors have mandatory disclosure and preservation requirements if a cyber-incident occurs. They must cooperate with and support

DoD's damage assessment if the Department chooses to investigate. Commercial item defense contractors face both the potential loss of sensitive commercial data and also potential costs of complying with DoD requirements because they are not reimbursed for overhead by the government. Finally, a serious penetration may indicate to DoD an overall lack of controls, potentially subjecting the contractor to breach-of-contract allegations and risk of suspension and debarment, resulting in a loss of future business and additional legal costs.

Insurance

Understanding your company's insurance coverage for cyberattacks—and plugging any coverage gaps—can mitigate potentially significant financial liabilities. Potential losses may be covered under cyber, property, general liability, crime, kidnap and ransom, or errors and omission policies. Important considerations in reviewing these policies include:

- Assess the costs of both your company's most likely and most costly exposures to ensure that your policies have sufficient limits given the risks defense contractors face.
- Critically evaluate application questions about network security practices to reduce the risk of alleged misrepresentation about or negligence in maintaining cyber security. Avoid policy language that conditions coverage, rather than rates, on perfection.
- Where third party vendors provide services, understand whether they create uninsured risks for your business, and if needed seek indemnities.
- Seek realistic "retroactive dates" with adequate time horizons as cyber breaches can remain undiscovered for significant periods.
- Understand whether your Kidnapping and Ransom policy covers cyber threats, such as ransomware.

Policyholders have real leverage at renewal time. *Prepare* for that process by understanding your policies. Covington & Burling routinely advises clients purchasing insurance for cyber risks.

The Benefits of Thoughtful Planning

Defense contractors face a greater than average risk of cyberattacks. But they are more likely to have robust data-security protections, and their personnel are likely better trained. Contractors can point to compliance with requirements of DFARS 252.204-7012 and implementation of the security controls in NIST SP 800-171 as concrete reasons for lower premiums.

Bringing the defense industry's thoughtful planning to insurance for cyber losses makes good sense: well-written insurance can help manage the risks and costs of a breach.

If you have any questions about the material discussed in this client advisory please contact the following members from our insurance and government contracts practice:

Susan Cassidy	+1 202 662 5348	scassidy@cov.com
Rukesh Korde	+1 202 662 5619	rkorde@cov.com
Bert Wells	+1 212 841 1074	bwells@cov.com