CYBERSECURITY

MAKING INSIDE JOBS LESS LIKELY

A new program to prevent insider cyber threats has the right idea—but has government contractors scratching their heads about how to comply.

In May 2016, the Defense Department's Defense Security Service amended the National Industrial Security Operating Manual, creating a new requirement that contractors with DOD facility security clearances have a written plan for implementing an insider threat program aimed at preventing cyber attacks. DSS further mandated that the plan be in place by November 30, 2016.

This requirement for cleared contractors is a natural extension of Executive Order 13587 and the National Insider Threat Policy—both signed by President Obama in 2012—which called for the creation of an insider threat task force to develop a government-wide program for deterring, detecting, and mitigating insider threats. Given that cleared contractors have access to and safeguard significant amounts of classified information in performing work for and on behalf of government agencies, it makes sense to require similar programs for them.

So why formalize a program now? According to Adelicia Cliffe, a partner in Crowell & Moring's Government Contracts and International Trade groups, "The glare of the 2013 document leaks by Edward Snowden and the arrest in 2016 of another National Security Agency contractor for long-term document theft highlight that insider threat risks are not limited to agency employees, and that contractors are also in a position to exploit and compromise classified information. When security breaches of this magnitude happen, the government has to step up its efforts and make prevention a bigger priority."

NOT ENOUGH SPECIFICS, POTENTIAL LAND MINES

The DSS program has five minimum requirements for affected contractors:

- Designation of an insider threat program senior official to establish and execute the program
- Development of a written implementation plan
- Reporting of "relevant and credible information" regarding potential insider threats
- Training programs for managers and all cleared employees, plus annual refreshers
- Information security controls to monitor activity on classified information systems

But DSS's guidance falls short on specifics—in fact, it expressly states that the plans must be tailored to each organization's business—leaving contractors with unanswered questions about the plan's logistics, content, and training, among many areas. For now, they've had to figure things out as they go.

As with the federal agency insider threat program requirements, contractors must implement the insider threat program consistent with legal, civil liberties, and privacy policies. Cliffe emphasizes the significance of this intersection as a particularly thorny area for cleared contractors, in light of the sensitivity of insider threat information and the potential consequences of reporting an individual under the program.

She strongly recommends that contractors include privacy experts in the planning and implementation of their insider threat programs. These experts should be key advisors to be consulted early and often, she says.

"Contractors should proactively engage with DSS to get ahead of the curve to avoid compliance issues and help shape DSS's expectations going forward." —*Adelicia Cliffe*

"As cybersecurity escalates in importance for many businesses, responsibility is shifting from IT professionals to corporate risk managers, lawyers, and CEOs." —*Evan Wolff*

WHAT ELSE SHOULD CONTRACTORS DO?

Contractors should take additional steps to make their insider threat programs practical, feasible, and flexible, Cliffe says. The result should be something that works both for the contractor's business and its existing industrial security program, and that satisfies the DSS requirements.

First, interdisciplinary teams should be set up to foster collaboration across management, legal, and technical groups. An example would be a work group or task force that includes representatives from human resources, the legal department, and operational and technical departments.

Second, contractors' obligations under their programs are numerous and substantial, meaning that they'll need significant resources both to comply and monitor compliance. They should plan ahead to make sure that such resources are in place.

Third, recent experience shows that contractor employees aren't the only potential source of insider threats—subcontractors, vendors, and other business partners with access to sensitive information pose major threats as well. Contractors should therefore consider extending their training programs beyond their own personnel to include third parties with access to classified information.

Finally, contractors should use the program as an opportunity to review and upgrade their current information systems, security policies, and security procedures to ensure compliance with the DSS requirements.

Cliffe takes this idea a step further: "Even better," she says, "contractors should proactively engage with DSS to get ahead of the curve to avoid compliance issues and help shape DSS's expectations going forward."

FIVE TRENDS IN INFORMATION SECURITY AND PRIVACY

What's the latest in information security and privacy law? Evan Wolff, a Crowell & Moring partner, co-chair of the firm's Privacy & Cybersecurity Group, and former advisor to the DHS, notes these emerging trends:

CYBER AS A TEAM SPORT

As cybersecurity escalates in importance for many businesses, responsibility is shifting from IT professionals to corporate risk managers, lawyers, and CEOs.

DEVELOPMENT OF REGULATIONS AND STANDARDS

Increasingly, governments are imposing regulatory requirements and standards on companies that handle sensitive government, business, and personal information. Cybersecurity requirements for federal contractors are contained in the Defense Federal Acquisition Regulations and NISPOM. The European Union, Russia, and China have cybersecurity requirements that can also affect U.S. businesses.

ISSUES THROUGHOUT THE CORPORATE LIFE CYCLE

Privacy and cyber concerns must be dealt with from corporate inception and are becoming more significant factors in mergers and acquisitions, to the point where they can be the primary deal drivers. As a result, cyber-focused due diligence is becoming standard.

FEAR OF LITIGATION COSTS

Cyber breaches not only have a negative impact on corporate reputation, but they also can trigger litigation. A massive 2014 cyber attack against The Home Depot has cost the company upwards of $200 million to defend and settle subsequent litigation. Efforts to anticipate and mitigate cyber-related litigation risk are multiplying accordingly.

MORE SOPHISTICATED RISK MANAGEMENT

Cyber threats to the nation, businesses, and individuals are getting stronger and more complex. Risk management will have to get more sophisticated to keep pace, including by investing in technical controls and human resources, often through the creation of new positions, notably chief information security officers.