The Enemy Within

The soft underbelly of cybersecurity

By John W. Chierichella / Sheppard Mullin Richter & Hampton LLP

"Cybersecurity" is a term that occupies virtually everyone these days. The list of U.S. government agencies that have been hacked seemingly grows with each passing day and includes the White House, the Pentagon, the State Department, the Office of Personnel Management, the National Oceanographic and Atmospheric Administration, and even the U.S. Postal Service. Among the prominent victims in the private sector are JP Morgan Chase, Target, Home Depot, UPS, Yahoo, Google, Boeing, Goodwill Industries, eBay, P.F. Chang's and Dairy Queen. As Director of the FBI James Comey famously declared, "There are only two kinds of big companies in the United States. There are those who've been hacked ... and those who don't know they've been hacked."

Hacking often conjures images of outside forces – state-sponsored intruders engaged in military and industrial espionage on many levels and/or private snoops who penetrate networks for pecuniary gain or simply because they can. More and more, however, the government and private companies have come to realize that the most immediate threat to their networks and to the information housed on them is not necessarily an external attack but rather an internal compromise that either results in the direct exfiltration of data by someone authorized to access their networks or who facilitates the exfiltration of that data by an unauthorized third party. This is what is commonly described in cyber-parlance as the "insider threat."

The Insider Threat

To provide some sense of the dimensions of the insider threat problem, it has been reported in recent years that more than 50 percent of all cyberattacks are the result of insider acts. Compounding the risks in this regard, as many as 65 percent of all authorized users of controlled networks can be described as casual onlookers, i.e., individuals who will access information out of curiosity without any real need for access. As and to the extent that these observers are careless in the storage, use and dissemination of the information, or unappreciative of the damage that could be caused by their negligence in those regards, the likelihood of compromise obviously increases. It has been estimated that 75 percent of all compromises of controlled information by insiders may go undetected.

The term "insider" in the cybersecurity world has a fairly broad scope. It includes employees, of course, but it also can include contractors, consultants and business partners. The common characteristic they share is authorized access not only to a company's information networks, systems and data but also to its physical facilities. Once afforded such access, the possibility exists that they may compromise the confidentiality, integrity or availability of company's information.

The reason that insiders pose such a threat is not merely their access to controlled information. It is because, frankly, there are so many of them and because the factors that might motivate them to compromise a company's systems are many and varied. In some cases, as noted above, there really is no motivation in the dictionary sense of the word. They may just be careless, leaving the information in their possession in a vulnerable position for access by unauthorized users, or they may have provided witting or unwitting access to their system credentials to third parties. But there are insiders who act for reasons other than pure negligence, including revenge on companies that overlooked them for promotions, salary increases or bonuses; ideology; financial need driven by self-destructive behaviors, such as drug addiction, alcoholism or gambling; and a combination of ego satisfaction and thrill seeking. The deliberate insider, driven by motive and purpose, poses the greatest risk for obvious reasons. First, as an insider, he/she is likely best situated to understand the information systems, their weaknesses and vulnerabilities, and how and when they can best be exploited. Second, he/she starts from a position of trust, in which the organization has already accredited him/her sufficient access to key systems, which facilitates even wider access through the exploitation of poor internal access controls. Third, he/she likely knows how to use the organization's own technology to extract, manipulate, exfiltrate, destroy or disclose sensitive information. Fourth, because he/she is personally motivated, the compromise is much more likely to be planned and methodical, or structured to take advantage of ad hoc, episodic unintentional lapses in security by others.

More than 50 percent of cyberattacks are due to insider acts, and 75 percent of insiders who compromise controlled information may go undetected.

System-Wide Defenses

If you operate in the aerospace and defense sector, evolving cybersecurity obligations have been a fact of life for some time. For example, the Department of Defense (DoD) imposes obligations on its contractors pursuant to the clause set forth at DFARS 252.204-7012 regarding "Safeguarding Covered Defense Information and Cyber Incident Reporting." This clause, which has morphed considerably in the last three years, requires the contractor, among other things (a) to provide "adequate security for all covered defense information on all covered contractor information systems that support performance of work under this contract," (b) to "[r]apidly report cyber incidents" to a specified electronic site, (c) to "conduct a review for evidence of compromise" when a cyber incident is discovered, and (d) to include the clause in all subcontracts, including subcontracts for commercial items. Not surprisingly, each of the quoted terms in the foregoing sentence is worthy of separate discussion. For the purposes of this article, however, the most salient fact regarding DFARS 252.204-7012 is what it does not address in any direct fashion, i.e., insider threats.

Insider threats, however, are now the subject of recent changes to the National Industrial Security Program Operating Manual, DoD 5220.22-M (NISPOM), promulgated by the Defense Security Service (DSS), which manages the nation's industrial security program, including the issuance and maintenance of facility security clearances (FCLs) and personnel security clearances (PCLs). The changes, commonly known as "Change 2" to the NISPOM were published on May 18, 2016, and described in an Industrial Security Letter issued by DSS on May 21, 2016. Pursuant to these changes, all contractors holding current FCLs must, by November 30, 2016, have in place a written program to address insider threats.

Because the NISPOM changes relate to contractor personnel who hold or are being processed for PCLs, the risk of "harm to the national security of the United State," is greater and the requirements of the insider threat program mandated by Change 2 are far more stringent than those most companies outside of the classified arena are likely to embrace. For example, the NISPOM's Insider Threat Program requires a contractor to "access, share, compile, [and] identify ... relevant information covered by the 13 personnel security adjudicative guidelines that may be indicative of a potential or actual insider threat." While those 13 guidelines make eminent sense in the case of national security risks, with respect to which the government has extraordinarily wide latitude, employees may well have cause for complaint in the private sector, unrelated to the government's issuance of PCLs, concerning the compilation by companies of dossiers on employees regarding several of these 13 guidelines used by the government, and under Change 2, by its cleared contractors: (1) allegiance to the United States, (2) foreign influence, (3) foreign preference, (4) sexual behavior, (5) personal conduct, (6) financial consequences, (7) alcohol consumption, (8) drug involvement, (9) emotional, mental and personality disorders, (10) criminal conduct, (11) security violations, (12) outside activities, and (13) misuse of information technology systems.

Building an Insider Threat Program

Leaving aside the question of which of these guidelines can properly be used to assess insider threat risks by a private company in an unclassified setting, unrelated to government contracts – a question best left to human resources or labor counsel and civil liberties practitioners – there are nonetheless aspects of the NISPOM Insider Threat Program that should be considered for implementation and/or adaptation and scaling by companies concerned with insider threats:

- A formal program – the adoption of a formal program will generate greater focus and discipline on the detection, prevention and mitigation of insider threats
- Formal appointment of a senior official of the company to oversee and manage the insider threat program – authority to act and accountability for results are essential to any effective program, whatever its subject matter
- Interdisciplinary collaboration – information regarding potential insider threats is likely to reside in various repositories through the enterprise, e.g., human resources, security, legal, information systems/information assurance. It is essential that the information be collected from all precincts. This is not merely personnel information; it is information regarding security systems and protocols, breaches and "escapes" that have occurred in the past, corrective measures, the necessity for privileged access in all instances, informational firewalls, physical security, and the like

Continued on page 41

John W. Chierichella *is a partner in the international law firm of Sheppard, Mullin, Richter & Hampton LLP. He can be reached at jchierichella@sheppardmullin.com.*

Export Control Reform

Continued from page 39

The drivers in enforcement consistently have been the desire to encourage compliance and avoid national security escapes involving the most sensitive technologies. As U.S. foreign policy and national security concerns evolve, we're seeing more of a focus on technology and cybersecurity as related to export controls. Our clients face the challenge of protecting their global networks from foreign actors eager to breach those networks.

An interesting development is new voluntary disclosure guidance issued by the DOJ involving export control cases. They've instructed the public to include them in the submission of voluntary disclosures that involve willful activities on the part of parties. It suggests that they continue to want to be actively engaged in export control investigations, continuing the strong trend in export controls. If you look at the cases over the past few years, including the Weatherford case, which was an extraordinary case in 2014 that involved coordination across many agencies beyond DOJ, we expect that the case trend will continue at or above its current pace.

MCC: What do the next two to three years have in store for export control? What impact do you expect the change in administration to have?

McCarthy: There are critical questions about where we go from here. The agencies have suggested, both publicly and in discussions we've had with them, that there's ongoing momentum. Updates to the rules, the cycle of reviewing them, and the engagement of industry to help with that process will continue over the coming years because there's a lot of support for that in Defense, State and Commerce. The questions revolve around whether the next administration will take what's been accomplished to date and move it forward beyond where it is now toward the goals of a single list, a single IT platform, and a single enforcement and administrative agency. We won't know the answers until we see who is appointed, who remains in the agencies in the new administration, and what the intentions of those officials are.

MCC: On a different note, Akin Gump has a body called the regulatory practice steering committee. Tell us about that and your role in it.

McCarthy: We've always had a very strong regulatory practice that's complemented our reputation as a market leader in the public law and policy space. The steering committee, which launched in 2016, serves a coordination and leadership function within the regulatory practices to generate ideas for collaboration in areas that will help serve our clients and reinforce our strengths. For example, the committee has helped identify interdisciplinary needs for clients in the health industry that may have environmental and trade issues. We're hoping the committee will be another great resource that allows us to generate thinking and build connectivity within the firm and among our clients around the globe to help us continue to deliver innovative and efficient legal services.

The Enemy Within

Continued from page 21

- Insider threat training for those managing the insider threat program – this would include not only training on preventive measures and responses to insider actions but also training regarding applicable state and federal laws. Employer/employee agreements regarding the collection and safeguarding of records, data, and assets, and training regarding applicable legal, civil liberties and privacy policies would also be included
- Insider threat training for all employees with access to company networks, systems, data and assets – such training can only make employees more aware of the risks posed by careless conduct and of the consequences of such conduct; it can also serve to make would-be actors aware of the company's strong oversight infrastructure and the likelihood of exposure, which facilitates deterrence
- An annual report to management by the insider threat program team – report cards are not just to acknowledge achievement but to identify opportunities for improvement

Beyond the cues provided by the recent changes to the NISPOM, all companies should include these elements as part and parcel of their insider threat programs:

- Rigorous pre-employment screening of applicants that is consistent with the level of access to key information that the employee will have
- Periodic monitoring of individual employee security practices
- Sanctions for violation of information security policies
- Segregation of various classes of data and information with access controls peculiar to those with a genuine need for access to the particular data in any given repository
- Establishment of a response plan and creation and training of a response team, which may include third-party experts

On April 22, 1970, cartoonist Walt Kelly first published his famous Pogo poster, reminding us all that "We have met the enemy and he is us." Although written with reference to the first Earth Day, it seems quite apt to the insider threat issue. Recognizing the fact and nature of insider threats allows the target to prevent, minimize, mitigate and/or recover from the risks that are posed.