in-house

Lessons for General Counsel from Recent Cyberattack on the U.S. Office of Personnel Management

Joe D. Whitley, Daily Report

August 4, 2015

While most consumers seem to find the various media reports of public and private sector cyberattacks relatively unremarkable, an April cyberattack on the U.S. Office of Personnel Management (OPM) and other recent high-profile breaches should remind general counsel that "no sector, network or system is immune to infiltration by those seeking to steal commercial or government secrets and property to perpetrate malicious and disruptive activity." (See "The Budget Message of the President")

President Barack Obama's proposed budget for the 2016 fiscal year seeks $14 billion to bolster cybersecurity efforts across the U.S. government. This article will explore whether you, as general counsel (or those advising general counsel), are taking appropriate measures to protect your company or client from cybersecurity breaches, exposure, and liability.

OPM: The Successful Target of a Cyber-Attack

In April, just two months after the president requested $14 billion to make cybersecurity improvements, the OPM discovered a cybersecurity incident potentially affecting 21.5 million current, former and prospective government employees and independent contractors. Investigations confirmed that these individuals' most private information, including Social Security numbers and personal data collected through employment applications and background checks, had been compromised.

While the OPM has involved the Department of Homeland Security and the FBI to address the security breach and any continuing threats, immeasurable and irreversible damage has already been done. The extent and severity of the damage? It is too soon to tell.

What Next?

Unofficial blame has been placed on Chinese hackers, and the speculation is that stolen

information will likely be used for many purposes that will advance both state and private interests in China, to the detriment of U.S. interests. Admittedly, we are traveling into unknown territory with the OPM breach having such a major impact, so we will likely face an unfolding challenge to our national security and proprietary information for many years to come.

Unfortunately, the issue of cybersecurity breaches and resulting international violations and damages is not redressable by U.S. laws and regulations alone. Although five Chinese perpetrators have been indicted in relation to prior similar attacks, it is unknown whether such individual perpetrators will ever actually face punishment in the absence of an extradition treaty with China or other similarly positioned countries. Further, the reality is that the stolen information has already been disseminated. Much damage has already been done.

Some proponents of retribution cite the UN Charter as authority to take responsive action against China; however, there is no universally applicable international law governing responses to cybersecurity attacks. Most of the arguments in favor of retribution require very nuanced analysis of such international law concepts as "use of force," "unlawful intervention" into the domain of another state, breach of state sovereignty, or breach of an obligation owed to another state—concepts that have not traditionally been applied to the cyberindustry and do not generally afford private entities (as opposed to states) any authority to retaliate.

Further, the analysis generally oversimplifies the careful consideration that must be given to economic and foreign policy effects of such action against another nation. There have been talks of international treaties to address these concerns; however, such discussions remain conceptual and are largely irrelevant to today's cyberbreaches.

The Impact on General Counsel

In a rapidly evolving digital age with countless unknowns and limited remedies, general counsel in every sector of the economy should now be concerning themselves with the preemptive and responsive measures they should take when—not if—they fall victim to a cybersecurity event.

In a 2014 publication on data security breaches, the Washington Legal Foundation explained that every entity storing electronic information will be subject to a cybersecurity event at some point. See Jana Valdetero and David Zetoony, "Data Security Breaches: Incident Preparedness and Response 9" (Washington Legal Foundation 2014). What remains relatively unknown (and potentially treatable) is the extent of such a breach and the resultant damages.

One thing is certain: the right breach, in the absence of appropriate preventive and remedial measures, has the potential for grave consequences for a company's reputation, continuity, competitive advantages, liabilities and unbudgeted expenses (e.g., investigation, notification, regulation and prevention).

To combat the unknowns, general counsel should adopt comprehensive and quantifiable preventative measures to pre-empt cybersecurity breaches and enable swift response when breaches are detected. In the digital age, all companies should have in place written security programs, policies and procedures delineating important security protocols, contacts, escalation measures, incident response plans and employee training programs.

These and related legal documents should be kept on hand in both paper and electronic format by general counsel and other affected personnel, so that threats can be swiftly assessed and

addressed. This is especially critical when dealing with the onslaught of legal, regulatory, and media attention that can be expected when a breach occurs.

Additionally, general counsel need to consider involving outside legal counsel at the earliest possible moment, both to ensure that attorney-client privilege protects documents and communications in the aftermath of an incident, and also to ensure that evidence is properly investigated and controlled to avoid chain of title issues. An outside legal team should also address various aspects of the breach, including: isolating the breach, leading a forensic investigation, managing media inquiries and other communications, addressing human resource issues, and advising as to ongoing business operations. Outside counsel will ensure that all responsive and remedial measures taken are appropriate and well-documented, which may provide an additional layer of insulation from civil exposure in the current uncertain regulatory climate.

Finally, general counsel should be diligent in selecting or upgrading cyberinsurance policies. With the evolving and escalating nature of cyberattacks, it is likely cyberinsurance providers will modify policies to exclude or limit the liability coverage for incidents or cap reimbursement for costs expended and remedial measures taken.

In light of the previously discussed costs associated with security breaches, both known and unknown, general counsel should routinely investigate the application and coverage of any cyberinsurance policy and be sure that coverage is appropriate in light of the individual entity's particular risk factors.

Navigating Conflicting State

Disclosure Laws and Preparing for a Federal Regulatory Response

At least 47 states have laws addressing the type and content of security breach notifications required of entities affected by intrusions. The laws vary from permissible electronic notification to mandatory mailed notices. Further complicating the issue is that many entities do business in and have contact with affected parties from many states.

General counsel should understand and apply state law in the states where they operate or seek guidance from outside counsel as to which state laws govern notifications to affected parties and whether their presence in a state relegates them to mandatory compliance. Of course, these notice requirements must be carefully synthesized with privacy laws governing both intra- and international operations of U.S. businesses as well.

General counsel should also be aware that mere compliance with mandatory notice laws may not protect an entity from civil exposure and will likely not, in and of itself, re-establish the entity's course of business and reputation. Victims whose data has been leaked in the wake of cybersecurity breaches have sued for damages under various legal theories, including negligence, breach of contract and breach of fiduciary duty, among others. Unfortunately, most known cases have resulted in confidential settlements, leaving the case law on the subject relatively undeveloped.

In light of these issues and the increased scrutiny regarding recent cyberintrusions, efforts are

being made to establish a federal regulatory scheme to provide more guidance to the private sector and bolster confidence in the public domain.

As a result of this highly dynamic environment, general counsel also need to keep themselves apprised of proposed changes to federal law governing notice requirements and other regulatory standards. For example, to bridge the apparent gaps and conflicts in state cyberbreach law, five proposals were submitted to the Senate in 2014, and in January 2015 the president announced the proposal of the "Personal Data Notification and Protection Act," which aims to set a federal standard for notifying victims of cybersecurity breaches. H.R. 1704, 114th Cong. (2015). General counsel should follow the progression of this proposed legislation and respond accordingly if one of these proposals or a similar bill is passed.

Concluding the Cautionary Tale

General counsel and other private sector personnel interested in the topics discussed above and the latest in cybersecurity issues confronting the public and private sectors are encouraged to attend a cybersecurity forum hosted by Baker Donelson in partnership with the Israeli government. It will feature experts from throughout the Southeast and will be aimed at staying ahead of developments in cybersecurity and its impact on technology, manufacturing, health care, logistics and energy. The forum will be held in Atlanta on Aug. 20. To register or for more information, go to www.cybercon.us.

As a general counsel you are a leader in the uncertain struggle to protect your company from cyberattacks, and this program should give you some much-needed guidance.

Madeleine G. Kvalheim and Brett A. Switzer, associates in Baker Donelson's Atlanta office, also contributed to this article.
