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

Joe D. Whitley
Update to original August 4, 2015 publication

While most consumers seem to find the various media reports of public and private sector cyberattacks relatively unremarkable, a 2014 cyberattack on the U.S. Office of Personnel Management (OPM) and other recent high-profile breaches, including those of companies such as Target and Home Depot, should remind general counsel of President Obama’s words in 2015 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.”

President Barack Obama’s final proposed budget for the 2017 fiscal year increased the amount sought to bolster cyber security efforts to $19 billion, and in 2016, he directed his administration to implement a Cybersecurity National Action Plan. The White House characterized the plan as the “capstone of more than seven years of determined effort by the [President Obama’s] Administration, building upon lessons learned from cybersecurity trends, threats, and intrusions.” While it remains to be seen whether President Trump will continue with President Obama’s efforts, President Trump has identified cybersecurity as a priority for his first 100 days in office. President Trump as tapped former New York Mayor Rudy Giuliani to head up the new cybersecurity task force. 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 2014, 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? While it has been over two years, it is still 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.

According to the 2016 Global Economic Crime Survey conducted by PwC, cybercrime is on the rise, climbing to second place among the most-reported types of economic crime (the first being asset misappropriation). And its borders are expanding beyond the traditional view of computers—PwC notes a “sharp increase in attack activity involving the so-called Internet of Things, including cars and household devices.” PwC further reports that the retail sector has seen significant increases in cybercrime activity, which is well illustrated by the more recent attacks on Target and Home Depot. What remains relatively unknown (and potentially treatable) is the extent of a cyber 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). Indeed, in its survey findings, PwC notes that about fifty organizational respondents reported losses over $5 million related to cybercrime, and some reported losses in excess of $100 million. Yet, reputational damage was reported as the “most damaging impact” of cybercrime.

To combat the unknowns and to prepare for the financial and reputational impacts, 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. And while this may all seem logical, PwC reports that only thirty-seven percent of organizations participating in its survey reported a fully operational incident response plan. Moreover, 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, the District of Columbia, Guam, Puerto Rico and the Virgin Islands 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, reestablish 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. One more recent known example, however, is Target, which settled various lawsuits brought by banks, credit card companies, and customers whose data was obtained during a cyberattack in 2013 for a collective total of more than $100 million. In early 2017, the Eighth Circuit Court of Appeals ordered the district court to determine whether all customers were treated fairly in the settlement of their claims, so this number could rise. Home Depot also announced a settlement of $19.5 million to compensate consumers who were impacted by a 2014 data breach.

In light of these issues and the increased scrutiny regarding recent cyber intrusions, efforts have been 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, and the new administration’s position of less regulation, general counsel also need to keep themselves apprised of proposed changes to federal law governing notice requirements and other regulatory standards.

One of the most recent pieces of legislation is the Cybersecurity Information Sharing Act of 2015 [P.L. 114-113], which the United States Congress passed as part of a last-minute omnibus appropriations bill at the end of the 2015 legislative session, and which President Obama signed into law later the same day. The Act aims to promote a collaborative, crowdsourcing approach to cyber-defense efforts through the sharing of information related to cyber threats between the public and private sectors, while simultaneously protecting the privacy rights of individuals whose information may be implicated. The law incentivizes private sector participation by extending liability protections to private sector entities that share information and defensive measures with the government and other members of the private sector, which many companies consider a pre-requisite to any sort of information-sharing arrangement.

The Act, which will remain in effect until September 30, 2025 unless repealed, does not, however, provide the type of streamlined regulation that is desired by the private sector and identified as a priority in the President Obama’s Cybersecurity Executive Order issued in 2012. While President Trump has taken the position of less regulation, he has also identified protection of the country’s infrastructure from cyber-attack as a key component to his first 100 days in
office. To that end, President Trump has named former New York Mayor Rudolph W. Giuliani to lead a cyber security task force. Thus, general counsel must continue to pay particularly close attention to industry sector-specific developments at both the state and federal level.