The CYBERSECURITY LAW REPORT

www.cslawreport.com Volume 1, Number 10 August 12, 2015

FINANCIAL SERVICES

Cybersecurity 2.0: The Role of Counsel in Addressing Destructive Cyberattacks

By David Fagan and Ashden Fein
Covington & Burling

It is well understood that cyber threats evolve and, in turn, require constant vigilance and evolution of defenses. It is less common among enterprises to have a precise understanding of what it means for cyber threats to evolve. Many enterprises view such "evolution" as focusing on the *means of attack*, such as new malware or "vectors of attack." However, a risk-based approach to cybersecurity – which is generally the practical legal mandate for enterprises – should recognize a more significant evolution of the cyber threat: the evolution of the *type and effect of the cyber-based threat* – from data loss (e.g., lost backup tapes or laptops), to data theft (e.g., nation-state infiltrations for economic espionage or criminal hacks for profit), to more destructive attacks that have arisen with greater frequency over the past few years.

In more personal terms, the difference between data loss or theft (which may be viewed as "Cybersecurity 1.0") and data and property destruction ("Cybersecurity 2.0") is the difference between having your house robbed and having your house burned to the ground. It is, of course, a best practice to protect homes from both risks – to have security alarms and fire detection and suppression systems. Yet on the cyber front, many enterprises (to the extent that they are prepared or focused at all on the risks) are principally training their resources and defenses on protecting their data from exfiltration. There is no question that the risk of data exfiltration is very real and must be addressed, but resources, including legal resources, should also be trained on the possibility of more advanced threats committed to destruction, not just theft.

The Evolution of Cybersecurity

The majority of cyber-related attacks focused on enterprises have been opportunistic in nature – not targeted at any particular individual or company – and conducted by relatively unskilled hackers. These data-focused attacks are both the most common and least dangerous types of attacks, and they also are minimally successful because the majority of people know not to open spam email or click on links in their email. According to Verizon's 2015 Data Breach Investigations Report, only 23% of recipients open phishing emails.

Dating back several years, however, there has been a proliferation of more targeted attacks from nation states and sophisticated criminal organizations that demonstrate persistence (multiple efforts to find vulnerabilities over the course of months or years) and sophistication (exploiting unknown vulnerabilities and covering traces once inside an organization) to steal data. For example:

- ATM-processing companies suffered breaches that resulted in customers' ATM cards numbers and PINs being stolen and used by thieves. In one case, in less than 12 hours in 2008, Eastern European hackers infiltrated RBS WorldPay and stole customers' ATM card data and encrypted PINs, cracked the card users' PINs, and further stole more than $9.5 million from those accounts.[1]
- In May 2011, Lockheed Martin suffered a cyberattack through the unauthorized use of its employee remote connection application. The attack was enabled by the fruits of a previous cyberattack on RSA Security, the electronic token vendor that provided remote access security to Lockheed Martin.[2]

- Since 2005, more than 75 data breaches have been publicly disclosed in which bad actors compromised 1 million or more records, including Heartland Payment Systems (130 million records, 2009), Target (110 million records, 2013), Home Depot (190 million records, 2014), and Anthem (80 million records, 2015).[3]

See also "*In a Candid Conversation, FBI Director James Comey Talks About the 'Evil Layer Cake' of Cybersecurity Threats*," The Cybersecurity Law Report, Vol. 1, No. 5 (Jun. 3, 2015); and "*In a Candid Conversation, FBI Director James Comey Discusses Cooperation among Domestic and International Cybersecurity Law Enforcement Communities (Part Two of Two)*," Vol. 1, No. 6 (Jun. 17, 2015).

In response to these threats, companies continue to develop institutional controls to defend against and mitigate data theft resulting from cyberattacks, and counsel are increasingly involved in such risk mitigation efforts. These controls include, among other things, developing incident response plans focused primarily on data loss, assessing vendors for their ability to protect data and shifting liability risks for data loss through contractual arrangements, establishing insider threat detection programs focused on employee or contractor access to sensitive data, and obtaining insurance coverage for data breaches.

With the exception of a few industries, these controls continue to focus principally on protecting data from being exfiltrated or accessed by unauthorized persons, or mitigating and remediating any data-related losses, and not specifically protecting the integrity of IT systems or preventing physical destruction resulting from hacked networked devices.

The more disturbing trend in cyberattacks, however, is squarely focused on destruction. These malicious attacks are directed at harming a business rather than directly benefiting the attacker. The most infamous of such attacks is the one perpetrated against Sony Pictures Entertainment (SPE) in November 2014, which reportedly rendered unusable nearly half of every computer at SPE.[4] In its FY14 20-F to investors, Sony Corporation reported that, as of March 31, 2015, SPE spent approximately $41 million to investigate and remediate the cyberattack on its network and IT infrastructure, and that cost did not include any losses from the impact on its intellectual property or from any litigation or regulatory actions. Sony, however, is not the only entity to suffer such an attack:

- On a single day in 2012, Saudi Aramco suffered a cyberattack resulting in approximately 30,000 of its internal network computers being destroyed, with its data erased and replaced with an image of a burning American flag.[5] The malware used in the attack had an imbedded timer that was programmed to execute across the entire enterprise at the exact same time and also had code that rewrote the computers' master boot record, effectively disabling the system.[6]
- In February 2014, hackers released malware that destroyed the information technology infrastructure of the Sands Casino. The company executives managed to stop the attack the same day it began, by quickly removing the entire company from the Internet.[7]
- In December 2014, Bloomberg reported the cause of an August 2008 explosion in a crude oil pipeline just outside of Rehafiye, Turkey to be that of Russian state-sponsored hackers.[8] These hackers exploited a vulnerability in networked surveillance cameras meant to protect the pipeline, to gain access to the industrial control systems and cause super-pressurized crude oil to explode. The explosion caused extensive damage to the pipeline, spilled more than 30,000 barrels of oil into an aquifer, required companies to pay $5 million in transit tariffs per day for three weeks while the pipeline was inoperative, and cost the Republic of Azerbaijan $1 billion in export revenue.[9]
- In January 2015, Wired.com reported that the German Federal Office for Information Security released a report detailing a cyberattack on a German steel mill resulting in large-scale damage.[10] The report outlined that hackers used a sophisticated phishing scheme to gain access to

the plant's business network to further gain access to the plant's industrial control systems. According to Wired.com, the hackers were able to manipulate and disrupt the control systems to cause the blast furnace to fail to shutdown properly, "resulting in 'massive' – though unspecified – damage."[11]

- On July 21, 2015, Wired.com reported that researchers were able to wirelessly carjack a Jeep Cherokee by remotely controlling the dashboard, transmission, brakes and steering through accessing the vehicle's Internet-connected technology.[12] Although this cyberattack occurred in a somewhat controlled environment, it is another example of a present-day vulnerability that can have a destructive effect in the physical domain and not just isolated to IT systems.

Implications of Destructive Cyberattacks for the Role of Counsel

The emergence of destructive cyberattacks underscores the importance for legal departments to have an understanding of their enterprise's operations, supply chains, IT dependencies and cyber-threat profile. Counsel should adequately advise on compliance, governance, risk management, litigation and other core legal issues surrounding cyber-threats, especially as the frequency and severity continue to increase. There are several steps that counsel can take to help their organizations manage the risk from such attacks:

Incident Response Preparation

Cyber-related incident response and business continuity plans should train for destructive cyberattacks, not only loss of data, and should ensure that appropriate resources are identified that can manage the attack and make a decision to shut down a network in order to preserve it. Counsel's active involvement in the training under such plans, including tabletop exercises, can establish and preserve privilege and protect the results of such simulations. See also "*Preserving Privilege Before and After a Cybersecurity Incident (Part One of Two),*" The Cybersecurity Law Report, Vol. 1, No. 6 (Jun. 17, 2015); *Part Two*, Vol. 1, No. 7 (Jul. 1, 2015).

Vendor Assessment and Contracts

It is fairly standard for vendors to be assessed for their ability to protect data that may be shared with them, and, in turn, for vendor contracts to impose data security requirements and apportion liability for breaches involving data. Such assessments and contractual terms, however, often do not focus on underlying risks that could contribute to destructive cyberattacks, such as steps a vendor has taken to assure the availability, integrity and reliability of its network. Likewise, for vendors of connected devices or other IT equipment, most supply assessments and contracts do not include terms that address the importance of the equipment to the availability, integrity and reliability of the network in which the equipment is installed – or, for that matter, impose other than the most basic requirements on the vendor for its own supply chain and assurance practices. In a world of destructive cyberattacks, it may behoove counsel to review such assessments and contractual terms to ensure that, in appropriate circumstances, they account for and address the possibility of such attacks.

Governance and Disclosure

Since 2011, the SEC's Division of Corporation Finance has recognized that cyber incidents could result in disruption to operations that could require disclosure to shareholders and the SEC as a risk factor.[13] Counsel should plan on potentially having to disclose destructive attacks, but only after taking into account the occurrence, frequency and severity of prior cybersecurity incidents, as well as the potential costs and other consequences associated with such incidents. Counsel can work with their IT departments and businesses to understand the possible effects of destructive cyberattacks and be prepared to conduct a materiality analysis very quickly following such an incident.

Insurance Policies

In May 2014, the insurance industry introduced broader cyber-related exclusions to the standard commercial general liability policy, in an apparent effort to confine such coverage to the specialty cyber risk policies that many insurers have sold in recent years. These cyber policies are not standardized, however, and many contain limiting conditions and exclusions, including exclusions for physical injury and property damage. Counsel should carefully examine these cyber policies, alongside the other lines of coverage in a company's insurance program, to determine whether potential cyberattacks resulting in destruction of IT systems or physical infrastructure, and not just loss of data, might fall within a coverage gap. See also "*Analyzing the Cyber Insurance Market, Choosing the Right Policy and Avoiding Policy Traps*," The Cybersecurity Law Report, Vol. 1, No. 2 (Apr. 22, 2015).

Conclusion

In addressing cybersecurity threats, legal counsel, just like other aspects of an organization, should recognize the evolving nature of the threat and ensure that their organization is properly focused, from a legal standpoint, on the possibility of destructive cyberattacks and not just data theft.

David Fagan, a partner in Covington's global privacy and data security and international practice groups, counsels clients on preparing for and responding to cyber-based attacks on their networks and information, developing and implementing information security programs, and complying with federal and state regulatory requirements. He has been lead investigative and response counsel to companies in a range of cyber and data security incidents, including matters involving millions of affected consumers.

Ashden Fein is an associate in Covington's global privacy and data security, litigation and white collar defense & investigations practice groups He focuses on representing companies and individuals in government and internal investigations, including clients in the defense, cybersecurity and national security industries; regulatory matters concerning national security law; and global privacy and data security. Before joining Covington, Fein served in the United States Army as a prosecutor where he specialized in cybercrime and national security investigations.

[1] Kim Zetter, *Russian Convicted of $9 Million RBS WorldPay Hack Avoids Jail*, Wired (Feb. 9, 2011).
[2] Christopher Drew & John Markoffmay, *Data Breach at Security Firm Linked to Attack on Lockheed* (May 27, 2011).
[3] Keith Collins, *A Quick Guide to the Worst Corporate Hack Attacks*, Bloomberg (March 18, 2015).
[4] Peter Elkind, *Inside the Hack of the Century*, Fortune (Jul. 1, 2015).
[5] Reuters, *Saudi Arabia Says Cyber Attack Aimed to Disrupt Oil, Gas Flow* (Dec. 9, 2012) [hereinafter "Reuters"]; Jack Clark, *Shamoon Malware Infects Computers, Steals Data, Then Wipes Them*, ZDNet (Aug. 17, 2012); Nicole Perlroth, *Connecting the Dots After Cyberattack on Saudi Aramco*, New York Times (Aug. 27, 2012).
[6] See Reuters.
[7] Ben Elgin & Michael Riley, *Now At The Casino: An Iranian Hacker in Every Server*, Bloomberg (Dec. 11, 2014).
[8] Jordan Robertson & Michael A. Riley, *Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar*, Bloomberg (Dec. 10, 2014).
[9] Id.
[10] Kim Zetter, *A Cyberattack Has Caused Physical Damage for the Second Time Ever*, Wired (Jan. 8, 2015).
[11] Id.
[12] Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway – With Me In It*, Wired (Jul. 21, 2015).
[13] See Division of Corporation Finance, Securities and Exchange Commission, *CF Disclosure Guidance: Topic No. 2: Cybersecurity* (Oct. 13, 2011).