The CYBERSECURITY LAW REPORT

www.cslawreport.com Volume 1, Number 16 November 11, 2015

INFORMATION SHARING

What Companies Can Learn from Cybersecurity Resources in Pittsburgh

By Mark Rush and Joe Valenti
K&L Gates

Cyber crime is a serious threat – it cripples companies, damages economies, funds terrorism, launders drug money and bleeds the assets of individuals, according to the DOJ. Often this cyber war is waged from shadows overseas (and often in the form of corporate cyber espionage). Companies should be using a broad array of tools to prevent and mitigate the effect of international and domestic cyber crime, such as information sharing, sufficient cyber insurance as well as a thorough breach response plan that includes proper notification and preservation of evidence for future actions.

One place where law enforcement and the private sector have come together is Pittsburgh, where a string of major cyber crime cases have recently been prosecuted. Developments there can serve as a model for cybersecurity measures across the country and across industries. In this article, we describe cybersecurity best practices before, during and after a breach, as well as some unique ways government officials as well as companies in Pittsburgh specifically are handling cyber crime.

Nearly Every Company in Every Industry Is an Attractive Target for Cyber Criminals

Organizations around the world and across industries possess sensitive information that cyber criminals covet. One prosecution brought in federal court in Pittsburgh shows that multi-national industrial companies have been attacked by Chinese government officials in concerted efforts to obtain trade secrets and economic information. Government contractors are routine targets for state-sponsored cyber criminals because of the sensitive information and weaponizable technology they typically possess. Financial institutions store personal and banking information for their customers that can be sold in dark markets. Healthcare companies store personal health history and related billing information. Educational institutions store valuable intellectual property generated by the nation's leading researchers.

Pittsburgh, Pennsylvania Houses Key Resources for Cyber Defense

The threats cyber criminals pose know no geographic boundaries. Pittsburgh-based organizations, however, have quite a bit of field experience in defending against the efforts of cyber criminals. Organizations like the National Cyber-Forensics & Training Alliance (NCFTA) and the Computer Emergency Response Team (CERT), based at Pittsburgh's Carnegie Mellon University, have been at the forefront of preventing and detecting cyber attacks long before these attacks were recognized as threats to national security.

NCFTA, a nonprofit entity, aims to identify and defend against evolving cyber-based threats by bringing public, private, and academic sectors together in one space. In this space, subject-matter experts from the FBI are embedded and work together with subject-matter experts from private corporations – sharing information and resources – to defend against cyber threats.

This model proved successful. Dan Larkin, former Unit Chief of the FBI's Cyber Initiative and Resource Fusion Unit (CIRFU) and founder of the NCFTA, stated that, between 2000 and 2005, the NCFTA was involved in initiatives that resulted in hundreds of cyber criminals being charged. This early success resulted in growth. Now, the FBI has embedded the CIRFU at the NCFTA's office. The NCFTA's private membership also is constantly growing.

On the investigation and enforcement side, the U.S. Attorney's Office in the Western District of Pennsylvania has developed an expertise in analyzing cyber attacks and prosecuting cyber criminals. Often through

legal and expert counsel, cybersecurity-oriented organizations work together and with companies around the world to combat cyber crime and enhance preparation and defense for the inevitable cyber attacks to come.

See also "*How the Legal Industry Is Sharing Information to Combat Cyber Threats*," The Cybersecurity Law Report, Vol. 1, No. 12 (Sep. 16, 2015); and "*Energy Industry Demonstrates Public-Private Cybersecurity Coordination*," The Cybersecurity Law Report, Vol. 1, No. 14 (Oct. 14, 2015).

How the NCFTA Works

Companies involved in the NCFTA are better prepared to prevent and respond to cyber attacks, according to Larkin. This is because of the valuable information shared among partners related to best practices and trending threats, as well as the access to law enforcement to arrest and prosecute cyber criminals rather than merely shifting them to another website, server or business unit.

NCFTA members receive up-to-date feedback through monthly peer calls and listservs, giving partners the ability to fine-tune their cybersecurity programs to defend against trending threats before an attack occurs. Participating in the NCFTA also demonstrates to government agencies that a company is proactive in protecting its customers.

The NCFTA expects that its partners actively participate and share intelligence. To meet this expectation, a company must have a subject-matter expert (many times a chief risk officer) who is capable of collaborating and cooperating with the other partners at the NCFTA. Smaller companies may not have this expertise, but Larkin points out that those smaller companies can work with the NCFTA through a trade association. See also "*Shifting to Holistic Information Governance and Managing Information as an Asset*," The Cybersecurity Law Report, Vol. 1, No. 2 (Apr. 22, 2015).

Insuring Cybersecurity Risk

Cybersecurity insurance can play a vital role in an organization's overall strategy to address, mitigate and maximize protection against cyber risk, but choosing the right insurance product presents real and significant challenges. There is a diverse and growing array of cyber products in the marketplace, each with its own insurer-drafted terms and conditions that vary dramatically from insurer to insurer—and even between policies underwritten by the same insurer. In addition, the specific needs of different industry sectors—and different companies within those sectors – are far-reaching and diverse.

Although placing coverage in this dynamic space presents a challenge, it also presents substantial opportunity. The cybersecurity insurance market is competitive, and cybersecurity insurance policies are negotiable. The terms of the insurer's off-the-shelf policy form can often be significantly enhanced and customized to respond to the insured's particular circumstances. Frequently, these enhancements can be achieved for no increase in premium. Coverage exists for third-party as well as first-party (to cover the organization's own digital assets and income loss) liability. For insight from K&L Gates partners Roberta Anderson and Sarah Turpin, see "*Analyzing the Cyber Insurance Market, Choosing the Right Policy and Avoiding Policy Traps*," The Cybersecurity Law Report, Vol. 1, No. 2 (Apr. 22, 2015).

Investigating a Security Breach

After a hack occurs, companies will have to investigate to determine how the breach occurred, what systems were affected and what information was stolen. Attacks can occur from either external or internal sources. A breach may be as simple as a rogue employee walking away with a thumb drive full of trade secrets or it could be as complicated and as politically charged as a state-sponsored cyber attack. Regardless, companies victimized by cyber criminals will need to identify the

responsible parties and their methods and use this new information to re-evaluate and fine-tune their cybersecurity programs.

Often, this investigation will involve looking at data logs and examining alert systems to re-create the timeline leading to a breach. This information may contain signals, which at the time appeared to be random and unrelated to a breach, but – in hindsight – were strong indicators that a cyber attack was underway. See "*DOJ Encourages Cyber Incident Reporting and Advance Planning with Best Practices Guidance*," The Cybersecurity Law Report, Vol. 1, No. 4 (May 20, 2015).

Finally, companies will need to identify how its customers have been affected by identifying what, if any, sensitive information has been stolen. Using appropriate forensic tools, companies should isolate and document the flow of information taken by cyber criminals to identify ongoing problems and potential risks from the post-breach use of the data stolen.

Preserving Evidence of a Crime or for Civil Actions

In most cases, a company that is a victim to a data breach is also a victim of a crime and perhaps a potential defendant in government enforcement actions or class-action litigation brought by its own customers or employees. The affected data, hardware and software may become evidence for criminal prosecution or civil litigation. Federal law enforcement has been active in pursuing cyber criminals and seizing or subpoenaing the evidence needed to bring them to justice.

At the same time, the FTC has been heavily involved in enforcing privacy laws and bringing actions against companies for failing to maintain security of consumers' private information – particularly when companies' privacy policies suggest that such information will be securely maintained or only used for certain purposes. See "*The FTC Asserts Its Jurisdiction and Provides Ten Steps to Enhance Cybersecurity*," The Cybersecurity Law Report, Vol. 1, No. 8 (Jul. 15, 2015).

State attorneys general across the nation have followed this trend, using state consumer-protection laws as a vehicle to bring enforcement actions. Therefore, it is critical to handle evidence properly to avoid obstruction of justice charges, spoliation issues and related problems.

A company, as part of its breach response plan, should train its designated law enforcement coordinator to appropriately interact with law enforcement and consult with counsel in handling the matter. A company that has been hacked should promptly notify in writing all relevant company personnel to ensure the proper preservation of affected property. What may not seem important in the moments after a breach may ultimately lead to the prosecution of an intruder, and perhaps more importantly, the prevention of additional data breaches or future litigation.

Maintaining the relevant evidence may not only stave off civil litigation, but also help persuade law enforcement and civil investigators to view the company as an ally in pursuing a hacker rather than a negligent keeper of information to be taken to task.

Notifying Affected Parties or Complying with Mandatory Reporting Laws

A company's legal obligation to notify federal and state governmental agencies of a data breach must be understood in an ever-evolving regulatory world. Certain companies, such as defense contractors, are typically required to disclose data breaches under the Federal Information Security Management Act of 2002 (as amended), its implementing regulations, data policies derived therefrom, or the terms of their contracts.

The health insurance industry, for example, is heavily regulated in this space. The Health Insurance Portability and Accountability Act of 1996 (as amended) (HIPAA) requires "covered entities" to secure individuals' "electronic protected health information" by reasonable administrative, technical and physical safeguards. 45 C.F.R. §160.103; §164.302-312.

Further, HIPAA requires covered entities to report a breach into protected health information to affected individuals, to the Department of Health and Human Services, and, in certain circumstance, the media. 45 C.F.R. § 164.402-408. See also "*Privacy and Data Security Considerations for Life Sciences and Health Technology Companies (Part One of Two),*" The Cybersecurity Law Report, Vol. 1, No. 14 (Oct. 14, 2015).

Several other federal government agencies have requirements regarding data breach reporting. For example, publicly traded companies should be aware that the SEC has noted that, even though the federal securities laws do not explicitly refer to cyber risks and incidents, "a number of disclosure requirements may impose an obligation on registrants to disclose such risks and incidents." The FCC requires certain breaches into Customer Proprietary Network Information (CPNI) be reported to the United States Secret Service and the FBI.

Pittsburgh's Experienced Cyber Crime Fighters

Law enforcement officials located in Pittsburgh are among the best when it comes to assisting victims who report cyber attacks. U.S. Attorney for the Western District of Pennsylvania David Hickton has said, "We need to take as first principles that cyber intrusions affect real people in real ways. Our entire approach in Pittsburgh is victim-centric." This approach has achieved results. Recently, Hickton – along with the FBI Pittsburgh Division and the NCFTA – took down the infamous Darkode forum, an online marketplace for selling malware and stolen data, and launched prosecutions against the cyber criminals associated with it.

Indeed, even if a company is not required to report a breach, government officials generally encourage such reporting for the benefit of everyone. FBI Supervisory Special Agent Thomas X. Grasso, Jr., who has experience investigating cyber crime, said that the "FBI not only wants to investigate data breaches, but we are also eager to help those who have been victimized." Agent Grasso continued, saying, "By collaborating with the FBI, victim companies can gain a better understanding of the threat and how to protect themselves in the future. Bringing cyber criminals to justice is the best way to prevent future attacks."

Implementing the Breach Response Plan

The first 24 to 48 hours after a cyber breach is discovered are critical to mitigating damage to the company and its customers. During that time, the company must effectively implement the breach response plan that it has developed.

As part of the plan, the company should mobilize its first-response team (which may include an outside security/forensics firm), contact its legal counsel, work to preserve the valuable evidence by isolating affected systems, consider obtaining government assistance, and begin to manage the public relations aspects. Documentation of the steps taken by the first-response team is crucial to demonstrate that the company met its obligations to its customers and shareholders. The company's designated officer should document when the breach was discovered and how it was discovered. Further documentation should include dates and times of when the company initiated its breach response plan and when the various parts of the plan were started and completed.

A properly trained member of the breach response team should remove and secure affected systems and hardware to prevent more damage from occurring and to preserve evidence.

Conclusion

Pittsburgh's unique resources and experts offer best-in-class assistance to help a company develop risk-based security measures and navigate the legal implications imposed in the aftermath of a cyber breach. The first 48 hours after a breach will be hectic and overwhelming, but a comprehensive breach response plan developed well in advance

will help a company ensure it manages the chaos without committing a critical error. That plan, specifically tailored and implemented based on the facts surrounding any particular breach, must ensure that the company makes all proper notifications to avoid running afoul of regulatory obligations, unnecessarily creating civil liability or worse – being accused of obstructing justice by intentionally destroying evidence of crime.

Mark Rush is a former Assistant United States Attorney who is now a partner at K&L Gates LLP. He oversaw the formation of the National Cyber-Forensics and Training Alliance. He focuses his practice on regulatory compliance, internal investigations, and criminal and civil defense – including cases involving computer hacking, fraud, corruption, money laundering and Bank Secrecy Act violations. He often represents publicly traded companies in the financial services, healthcare and technology sectors.

Joe Valenti previously worked as an analyst for the U.S. Government on counterterrorism, economic espionage, and other sensitive national-security issues and spent seven years as a computer technician and programmer in the private sector. He is now a senior associate at K&L Gates LLP and focuses his practice on regulatory compliance, internal investigations and criminal and civil defense.