The Metropolitan
Corporate Counsel®

www.metrocorpcounsel.com

October 2013 Volume 21, No. 10

Cybersecurity Issues: An Overview

The Editor interviews ***Richard ("Jay") Johnson,*** *Of Counsel, Jones Day.*

Editor: What experience do you have in dealing with cybersecurity issues?

Johnson: Prior to joining Jones Day, I was a federal prosecutor in the Eastern District of Texas. I handled a variety of cases and investigations there, including white-collar fraud and identity theft. I also was the District's coordinator for computer hacking, intellectual property, and electronic evidence issues, better known by the acronym "CHIP."

The Justice Department has recognized the seriousness of the threat imposed by criminal cyber actors to privacy, financial security, and critical infrastructure, among other things. In addition to the Computer Crime and Intellectual Property Section in Washington, DC, the Department has CHIP prosecutors in place in every district across the nation to handle the threat. As the Eastern District's CHIP coordinator, I helped guide the District's preparation for and response to intellectual property crime and cyber crime, I conducted industry outreach and law enforcement training regarding such crime, and I counseled prosecutors on collecting electronic evidence.

Editor: What types of businesses are the targets of cyber criminals?

Johnson: All types of businesses are seemingly targeted, from news outlets and critical infrastructure to the financial and healthcare industries to intellectual property owners. And Fortune 500 companies are not the only targets. Many cyber criminals view small and mid-sized businesses as vulnerable because their

Richard Johnson

security measures are frequently less than adequate and their resources are limited.

Editor: Where cyber theft of personal information about customers, employees, patients, clients, or others is possible, what steps should companies take to assure themselves that systems are in place to foil such attempts, to identify the stolen information, and to promptly notify those whose information has been compromised?

Johnson: No set of steps can completely eliminate cyber risk or provide complete assurance that failsafe systems are in place. Generally speaking, however, the right mindset starts at the top. Executives must focus on cybersecurity like they do profits and losses. They should funnel significant resources towards it and assume that a failure to do so will impact their bottom lines. Specifically, they should elevate within their companies the priority of cybersecurity issues and the people that are charged with handling them. The Justice Department's announcement in July that five men from Russia and the Ukraine were charged with stealing 160 million credit card numbers, enough for roughly half the population of the United States, serves as a reminder to corporate executives to remain diligent.

A cyber attack is a hectic event. A response plan on dealing with one, prepared in advance, is critical. The plan should identify those people within and outside of the organization – computer forensic specialists, attorneys, media consultants, etc. – who are responsible for assessing a breach, for mitigating the ill effects of it, and for responding to or notifying federal and state law enforcement, customers and investors. And a static plan relegated to a dusty file cabinet in the legal and IT departments is not helpful. An executive needs to own it and needs to be the point person in the C-level suite for implementing it in the event of an attack. Executive buy-in is absolutely critical.

Editor: Is software available to assist a company in detecting or foiling cyber intrusions?

Johnson: Just as no set of steps can completely eliminate cyber risk, no software aimed at detecting and preventing a cyber intrusion is completely effective. Nothing will make a computer network impervious to an attack. That is the unfortunate bottom line. In fact, the worst case scenario is that such tools and measures provide a false sense of compliance within an organization so that it grows complacent. However, companies should have baseline protections in place, including a sophisticated hardware-based firewall that provides real-time intrusion monitoring, updated software and operating sys-

Please email the interviewee at rjohnson@jonesday.com with questions about this interview.

tems across every computer in the organization, routine monitoring of all network traffic, a security policy that requires frequent updates to passwords and regular monitoring of administrative access policies, and employee training on the latest social engineering tactics, such as phishing attempts that mimic communications from trusted businesses or colleagues. These are a few examples.

A multilayered approach to security, combined with thoughtful and advanced planning and executive-level buy-in, will do much to at least reduce risk.

Editor: What about internal theft. What should companies do to assure their data collection is protected?

Johnson: The internal risk is significant. Employees may know where data and intellectual property are located and have the necessary credentials to access both. Companies should identify assets that are most likely to be targeted, such as personal data on customers or significant intellectual property. They should isolate these assets and strictly limit internal access to them where possible to only those employees that need access to perform work functions. They should maintain clear policies that notify employees as to what they may do while on the corporate network and, more importantly, what they may not do. They should employ data loss prevention tools where feasible to monitor and limit various methods of copying data. Again, complete assurance or elimination of risk is a lofty but largely unattainable goal. But the risk of theft can be reduced.

Editor: Describe any federal or state legislation or regulations or case law penalizing cyber crime.

Johnson: A variety of laws have been passed at both the state and federal levels to address cyber crime, and they deal with everything from cyberstalking to spamming to using malware to intentionally damage a computer. There is no shortage of laws on the books. At the federal level, the Computer Fraud and Abuse Act is the government's principal tool in the fight against cyber crime and the statute most used by federal prosecutors. Among other things, it prohibits intentionally accessing a computer without authorization or in excess of authorization. And those found guilty face monetary fines and federal prison, in some cases up to 20 years. Some people argue that the Act is a classic overreach and that it outlaws seemingly innocent conduct. For example, an employee may "exceed authorized access" by using a work computer to check football scores online when not authorized by the employer to do so, or to check the news, or to surf the Web. Others argue that the ill effects of economic espionage, computer intrusions, the spread of malware and other things compel stronger legal protections.

Many of these laws were written before the average person had access to multiple home computers, to Internet-ready cell phones, to cloud computing. A comprehensive update to the legal regime is almost certainly in order, but recently proposed cybersecurity legislation that tackles information sharing and other topics appears stalled in Congress. Setting aside whether additional legislation is desirable, one thing is clear. The practical limitations of enforcing the cyber crime laws already on the books now pose an immediate problem.

Our laws don't apply everywhere. Our ability to enforce these laws is not equal everywhere. Criminals may be located in foreign and sometimes unfriendly countries and are thus out of reach. Government resources are limited, and prosecutors necessarily need to be selective in the cases that can be pursued. And unlike bank robbery, for example, where numerous witnesses may come forward to identify the culprit, determining who may be responsible for a cyber attack, a task known as attribution, may prove daunting.

Enforcement of existing laws is challenging.

Editor: Can you briefly describe the latest efforts of the White House to encourage information sharing between the public and private sectors? Do you have concerns?

Johnson: Our nation's critical infrastructure – power plants, pipelines, transportation facilities, financial organizations, etc. – is increasingly connected to networks and consequently susceptible to cyber attack. On February 12, 2013, the White House issued an executive order on cybersecurity that among other things promotes the sharing of information between the public and private sectors. It also calls for the development of a cybersecurity framework and charges the National Institutes of Standards and Technology with leading that effort. Adoption of the framework is voluntary, but industry is concerned that the framework's guidelines will establish a standard of care that, if not met, will open up new avenues of liability. Industry is also concerned with the potential use of the framework as a springboard for increased regulation.

The White House has proposed liability limitations as incentives for adopting the framework, and a White House cybersecurity official said last week in Dallas, Texas, that the administration is asking regulators to give the voluntary program time to succeed, that the framework does not call for new regulatory actions for sectors that are not already regulated. But industry should nonetheless be mindful of such concerns and watch closely as the cybersecurity framework develops. A preliminary draft of the framework will issue by October 10, 2013.

Editor: Are cybersecurity issues raised by storage of data in the cloud?

Johnson: Cybersecurity issues are raised by the storage of data in any location that can be accessed by others, be it in the cloud or otherwise. And the cloud poses certain unique challenges. An organization is literally handing over control of its most sensitive asset – information. The concerns are somewhat analogous to those raised by the use of third-party contractors to perform functions involving personal data. Does the cloud computing service offer acceptable security measures? Does an organization's agreement with the cloud computing service include provisions assigning liability in the event of a loss of data? What must an organization tell regulatory bodies about the risks involved in a cloud storage proposal? How are state reporting requirements addressed? How are data retention policies affected? Is the data stored in a jurisdiction with a more stringent data privacy protection regime? How are discovery obligations satisfied?

We'll see more certainty in this area as the law catches up with technology.