The Metropolitan Corporate Counsel®

www.metrocorpcounsel.com

Volume 19, No. 9 September 2011

Reducing Cybersecurity Risks – Government And Business Working Together

The Metropolitan Corporate Counsel (MCC) had the privilege recently of interviewing the ***Honorable Robert Menendez****, United States Senator from New Jersey, and* ***Fernando M. Pinguelo,*** *a Partner with Norris McLaughlin & Marcus, P.A. in its Bridgewater, New Jersey and New York City offices. Senator Menendez is a leading figure in the Senate in addressing cyber risks to the United States government and economy. Mr. Pinguelo is a lawyer who counsels businesses on cybersecurity and data protection concerns.*

Hon. Robert Menendez

Fernando M. Pinguelo

Editor: Thank you, gentlemen, for sitting down with us and sharing your insights on the pressing issues of cybersecurity and data protection. Senator Menendez, let's start with you. With competing priorities like the economy and the ongoing wars to contend with, where do you see cybersecurity falling in terms of congressional focus and attention, and why?

Menendez: I introduced the Cybersecurity Enhancement Act because I see cybersecurity as a top priority. Senator Reid has made cybersecurity a priority for this Congress. This is a bipartisan issue that has received overwhelming support in the past; the House voted to pass the Cybersecurity Enhancement Act during the last Congress by a margin of 422 to 5. I've been working with Representative McCaul, a House Republican who is leading the effort in the House, and I'm confident that Congress will address this pressing concern.

Editor: Mr. Pinguelo, what common cybersecurity issues are businesses seeking advice on, and what cyber issue do you expect to see more of in the future?

Pinguelo: Without question, one of the most common cybersecurity breaches businesses face involves disgruntled employees who turn their technological prowess against the company. Typically, when these "malicious insiders" leave a company, voluntarily or not, they work for a competitor, and there is always the possibility that they will attempt to steal intellectual property from their former employer. Malicious insiders sometimes use their familiarity and access to their employer's information systems to damage, extort or embarrass their employer, perhaps as an act of revenge. And, the most dangerous scenario is when the malicious insider joins forces with outside criminals to wreak havoc on an enterprise level.

While corporate espionage – clandestine techniques used to steal valuable information from businesses – has been around for quite some time, its methods in cyberspace continue to advance beyond the bounds of present-day sophistication, particularly in the area of social media. For example, the rise of social media, sparked by the advent of Facebook, MySpace, and others, has ignited a societal change in how people and businesses across the world communicate. One of the more recent techniques being used to extract valuable business information is "scraping," a method that employs software that allows cyber-spies to harvest personal details from thousands of users on social networking sites. When scraping is targeted at the profiles of a certain company's employees and the information collected is reconstituted, it has the potential to alert a competitor to such things as a new product launch or internal discord at the target company. Other uses of social media information include harvesting personal information to decipher answers to common security questions used by financial and retail companies to secure their data – such as date of birth, place of birth, and mother's maiden name. This information, in turn, could be used in combination with seemingly less intrusive information like email addresses to gain access to one's personal, financial or confidential company data.

The scope of potential nefarious uses of this information is endless.

Editor: Senator Menendez, how important is having a U.S. workforce trained in technology-related skills and aptitude to the future of the U.S.?

Menendez: It is imperative as virtually our entire critical infrastructure is tied to cyber networks. The Senate's Sergeant at Arms reported that computer systems of Congress are probed or attacked 1.8 billion times per month, which costs about $8 billion annually. And, as Mr. Pinguelo highlights, cyber attacks are also targeting private institutions – there have been 288 publicly disclosed breaches at financial services companies that exposed at least 83 million customer records over the last six years, most recently NASDAQ OMX Group and Citibank Inc. We must train our workforce to combat such attacks, for if investors do not trust that these institutions are secure, our financial markets simply cannot work.

My legislation would specifically promote the development of a cybersecurity-skilled federal workforce, promote cybersecurity education and awareness to the public, and strengthen the role of the National Institute of Standards and Technology in developing and implementing a public cybersecurity awareness and educa-

Please email Mr. Pinguelo at fmp@nmmlaw.com with questions about this interview.

tion program to encourage the adoption of best practices.

Editor: Mr. Pinguelo, what types of solutions do clients seek as far as cybersecurity is concerned, and what are some that you recommend?

Pinguelo: The business, the business, the business – that's what drives the solutions clients seek. When faced with a cybersecurity breach crisis at 3:00 a.m., clients do not want you to recite the law. They want direct, definitive answers, they want to understand and weigh the business risks, and they want that *before* you get a call from them.

I find a three-pronged approach – assess, confirm, and act – works best. In assessing the breach, I ask a lot of questions and determine what, if any, response is required – both legally and practically. Believe it or not, a significant percentage of breaches do not compel a legally required response.

Confirming a breach is an important element, and I draw upon a team of technical professionals whose job it is to work with the in-house IT folks and determine precisely what happened. More often than not, because of the clandestine nature of these cybercriminals, what may appear to have happened on the surface happened much differently when you dig deeper into the technology.

Acting requires a measured approach that compels adherence to both legal *and* business obligations. For example, a legal team must be prepared to identify all obligations under federal and state privacy and information management response and notification requirements and international data protection laws, including those involving cross-border data transfers.

And, I find that close collaboration with local authorities, many of which now have cybersecurity units, often is advisable to clients for a variety of reasons, including the fact that their business may be one of *several* targets of a cybercriminal enterprise. In fact, the U.S. Attorneys Office and others have implemented outreach programs to help businesses address these issues, and we work with these prosecutors to assist our clients.

Some preventative measures I recommend include (1) train employees to raise awareness about such threats, (2) watch historical patterns that might alert you to an employee who, for example, accessed sensitive corporate information at an alarming rate, (3) implement industry-recognized security measures, such as limiting the number of users who have access to your computer systems, (4) subject anyone with network access to appropriate background checks, (5) limit access to the network where practical and monitor use within the boundaries of the law and your capabilities, (6) revoke employees' network access *before* they are terminated, (7) review existing confidentiality agreements and compel them in broader contexts, including in business contacts obtained through social media, and (8) aggressively prosecute wrongdoers so as to provide a deterrent.

You may notice a common theme in each of these solutions: Education and training. Education and training is exactly what leaders like Senator Menendez are advocating, and even more importantly, putting to use.

In the end, we help each company assess its control system to determine if it is doing enough to protect itself. What these simple tips show is that creating a safe cyberworking environment for any company is about more than just software and hardware. Rather, it's about creating a culture that protects the company, its employees, and its intellectual property.

Editor: Senator Menendez, how important is cybersecurity research and development to the vital interests of the U.S.?

Menendez: Recent attacks have shown that we are currently behind the curve in cybersecurity. We must invest in the necessary research and development to ensure that we develop the highest caliber cybersecurity systems.

My legislation is a streamlined approach focusing on research and development and resources to combat the problem. It would require the federal agencies that fund cybersecurity research to cooperate in developing a research and development plan that is anticipatory instead of reactive. This plan would detail their near-term and long-term goals, and the plan would be updated every three years. My legislation would also encourage coordination and prioritization of federal cybersecurity research and development, improve the transfer of cybersecurity technology to the marketplace, and reauthorize several National Science Foundation Research and Development programs that include grants to safeguard computer and network privacy.

Editor: Senator Menendez, how important is a joint approach among government, private enterprise and academic institutions in combating the growing threats to our nation's cybersecurity? Can or should government do it alone?

Menendez: Cybersecurity doesn't affect the government alone and government doesn't always have the best or only answer. Therefore the government should not respond alone. Both federal computer systems as well as civilian computer systems have been targeted by various groups. The only path to effective cybersecurity is to foster a cooperative spirit among the public, private and nonprofit sectors.

My legislation would create a task force to coordinate efforts between the federal government, universities, and the private sector. My bill would also require the research and development plans developed by the federal agencies to specifically detail how the plans would coincide with research in the private sector. The Cybersecurity Enhancement Act would also foster greater cooperation with academic institutions by reauthorizing the National Science Foundation programs to develop cybersecurity degree programs.

Editor: Mr. Pinguelo, what's of greatest concern to you based on what you're seeing?

Pinguelo: Simply, concentration of information. The greatest concentration of private information is often the target of choice. The confidential information of healthcare facilities, financial services companies and financial institutions, and professional services firms such as accounting and law firms, present an attractive, concentrated repository of private information. Now more than ever, proactive measures are needed to counter this evolving threat, especially in industries where cybersecurity has never been a priority.

Another issue concerns state government networks, which hold some of their citizens' most vital information, including health records, professional licenses and tax information. The weak economy has caused governments to cut their budgets, reducing their ability to devote expenditures to cyberdefense. Thus, these sources also provide an appealing target for cybercriminals.

Editor: Thank you gentlemen for your insights into this pressing issue.

To learn more about Senator Menendez's efforts to address cybersecurity and other areas, visit http://menendez.senate.gov/. To learn more about Mr. Pinguelo, visit www.nmmlaw.com; or to receive copies of articles he's written on this topic, email him at fmp@nmmlaw.com.