The Metropolitan
Corporate Counsel®
National Edition www.metrocorpcounsel.com
Volume 22, No. 9 September 2014

Constant Vigilance Is Key In The New Cyber World

*The Editor interviews **John Fodera**, Partner in the Consulting Services Group of EisnerAmper focusing on delivering consulting and audit service.*

Editor: Please describe your practice area in the field of data protection.

Fodera: I work in the consulting services group of EisnerAmper in the New York City office, where we focus on helping companies develop a data security framework and program with appropriate technical, administrative and physical safeguards across the board.

Editor: Why is it now more important than ever before that companies have an ironclad data protection program in place?

Fodera: It's critical that companies from a business perspective protect their customers' and employees' information. Such a program makes good business sense in demonstrating the value they place on their clients and how they deal with them in a business relationship. It is extremely important that they protect the data that they're collecting, and the data that is very important to their customers, whether it is credit card information, personally identifiable information or even personal health information, depending on what type of company they're dealing with.

Editor: In advising corporate clients to protect themselves against cyber attacks, have you recommended adoption of the framework proposed by NIST (the National Institute of Standards and Technology)?

Fodera: Yes. The National Institute of Standards and Technology has a great framework to work within, offering some very important guidelines to be followed. Many smaller companies sometimes do not have the expertise to complete such a large framework questionnaire with the caveat that depending on the size of the organization, it should take a look at what guidelines are appropriate for its security platform.

John Fodera

Editor: What are the elements of an effective cybersecurity system? How does this differ from a regular data protection system?

Fodera: That's a great question. The overall umbrella is a data protection system, which encompasses the cybersecurity system as a subset. Looking at the cybersecurity aspect of data security, it is focused on the processes for protecting the network, the computers, and the programs from data attack and unauthorized access. With overall data protection, you have to protect against everything, that is, physical security as well as intellectual property security. For example, how do people secure admittance into your building or office? Is there a key swipe? With data protection you are looking to protect the manual and paper files as opposed to cyber protection, which is looking to protect the web, the computer and the forensics pieces.

Editor: How can failures happen allowing for data breaches to occur where a company has a sophisticated cybersecurity system?

Fodera: The interesting thing is many companies have very good programs in place, but at any time they are susceptible at the point of their weakest link. Many times the weakest links are the employees who sometimes are not aware of the latest policies and procedures. In addition, attacks can happen by people calling up pretending to be someone else and gathering information through an employee's device. The sophistication of the hackers is a constant. They're working day and night to try to break into systems, seeking out companies' vulnerabilities, often coming in through a backdoor scenario. By using wireless communications, hackers are known to set up a truck outside of a store and extract information. Companies need to be on their A-game by educating their employees, using the latest monitoring tools, and constantly testing their overall program to make sure that they actually have adequate coverage for mitigating the risk.

Editor: How can companies cultivate a culture of risk awareness among their employees? What kind of training is needed?

Fodera: I think it's more than just training. I think you hit the nail on the head when you talked about the tone at the top. The culture of the organization is critically important. That message needs to come from top management and the company's directors where everyone needs to understand the current policies and procedures the company follows, understand the gravity of the threat and the fact that it's a team effort. The organization has to work cohesively. Sometimes I will go into an organization that limits the exposure of its employees to knowledge of the risks involved in having employee access to files and records. They will say their IT group handles security. I tell them that more than just the IT department is needed to protect against threats of cyber attacks. It is vital to educate your organization as to what your policies and procedures are if you are hacked so your company can respond efficiently and mitigate the risk as much as possible.

Editor: What can your staff do in helping

Please email the interviewee at john.fodera@eisneramper.com with questions about this interview.

your corporate clients implement a program of training and awareness?

Fodera: Our staff, acting as advisors to companies, have seen many organizations where best practices are being utilized, which gives us a baseline for evaluating the practices of other clients. We can give recommendations for updating their programs, providing training techniques and ways to perform better documentation so companies can get credit for many of the programs that they're undertaking. Also, regulations are constantly changing. In the case of cybersecurity, there are a multitude of different state regulations, as well as those issued by the FTC and some from the European Union Privacy Laws. To be aware of those regulations and to do an adequate risk assessment periodically can help mitigate some of those risks or identify some exposure for which a program of remediation can be developed.

Editor: Do you recommend mandatory cyber-risk education for key employees – top management and directors of companies?

Fodera: I absolutely do. I think it's very critical for the tone and direction to come from the top and for them to understand the risks. Not only should an overall program include an education program, but management and the board should receive reports as to when the audits were done, what exposures were found, and what vulnerabilities were examined. There's much testing that needs to be done on the audit side by way of penetration testing, or some type of internal vulnerability assessment, where you get a diagnostic that can identify some of the weaknesses in your system and areas that need improvement. As soon as these weaknesses are identified through the reports, or shortly after they are remediated, they should make their way up to the executive suite and also to the board so they can understand what management is doing in this complex space.

Editor: Once a cyber breach occurs, what remedial measures do you recommend should be taken?

Fodera: Hopefully, a company has already put together an incident response plan and a breach notification plan. When breaches occur, companies should have a roadmap that can be used to identify who they need to contact internally, including legal counsel, because they need to be advised as to what the legal ramifications and their liabilities are. I also recommend that companies have a forensic firm "on call" to help them quickly identify how bad the breach was and how many records were obtained, ultimately allowing them to lock down the system. Taking remedial measures by following an in-place plan is going to help the company get through a difficult time. It is a costly and time-intensive process to identify a breach, put together a breach notification, institute the incidence response plan, notify authorities and alert customers or others who were breached. Given this impact, as well as the opportunity loss and reputational damage, it's critical to remediate some of the gaps that allowed the breach in their systems in the first place.

The sophistication of the hackers is a constant. They're working day and night to try to break into systems, seeking out companies' vulnerabilities, often coming in through a back-door scenario. By using wireless communications, hackers are known to set up a truck outside of a store and extract information. Companies need to be on their A-game.

You don't know where a breach is going to occur until it happens. As I indicated, some might come from use of wireless by hackers, and sometimes breaches come from internal threats from disgruntled employees. We have read where an employee had the entire payroll on an unencrypted laptop, which was stolen. There are a number of different ways breaches occur. It is vital to put remediation measures in place to prevent what can be cataclysmic disasters.

Editor: Who of your clients are most vulnerable to data breaches?

Fodera: Statistics from the Ponemon Institute study focus on a couple of areas that show that certain industries are more vulnerable or have been more susceptible to attacks. At the top of the list are financial service companies, particularly banks. Large investment companies are also high on the list. The second area that seems to be dominant is in the retail space, where hackers are looking to steal credit card information. Listed below retail as an area hackers are targeting is the medical field, where they are looking to get medical information regarding patients.

Editor: Do you have anything more that you would like to add?

Fodera: The only thing I would add is that I think it is critical that companies analyze their programs and do periodic risk assessments, where they bring in management teams to identify what the threats to a company's data are. As they identify those threats, they should rank the gaps in their systems and prioritize which are high, medium or low risks, and then carefully put together a remediation plan that focuses on tightening up their security practices. It's not a static process. It's an area that needs to be constantly reviewed because the threats are changing daily. With new means of technology, new services that companies are developing, and with new cloud computing providers, companies need to be constantly vigilant and conduct due diligence. There are many exposures that companies have, and they need to identify them and see what they need to do to perform remediation on certain areas of their program.