NACD New England Chapter Event Highlights
Breakfast Event – October 18, 2016

How to Reduce the Impact of Cyber Security Threats

Event Overview

Our online infrastructure currently faces approximately 500,000 cyberattack attempts every minute. The Internet of Things provides an unprecedented opportunity for hackers. Hot topics for our cybersecurity panel include: hacks of mobile payment and other non-traditional payment systems; data manipulation and sabotage; open source vulnerabilities; and ever-more-sophisticated phishing pitfalls. Attendees learned what to do about cyber threat mitigation at this timely, and critical, forum.

About the Panel:

Dr. Peter Fonash is the Chief Technology Officer for the Office of Cybersecurity and Communications in the Department of Homeland Security. He has previously held positions as Cybersecurity Advisor to the Staff Director, Federal Reserve Board; Director of the National Cybersecurity Division; Director of the National Communications System; Chief of the Defense Information Systems Agency's (DISA's) Advanced Technology Office, and Chief of DISA's Joint Combat Support Applications Division. Fonash received a Bachelor of Science in Electrical Engineering; a Master of Science from the University of Pennsylvania; a Master of Business Administration from the University of Pennsylvania's Wharton School; and a Ph.D. in Information Technology and Engineering from George Mason University. He is member of the George Mason University School of Engineering Advisory Board, and a Member of the Institute of Electrical and Electronics Engineers (IEEE).

Dr. Sophie V. Vandebroek has been Xerox's Chief Technology Officer since 2006, a function in which she leads Xerox's research labs globally. She also is the sole director of PARC Inc., a Xerox company that provides custom R&D services to enterprises, startups and government agencies. She holds 14 U.S. patents. She was inducted into the Women in Technology International Hall of Fame and elected into the Royal Flemish Academy for Arts & Sciences in Belgium. Dr. Vandebroek serves on the advisory council of the dean of engineering at the Massachusetts Institute of Technology and is a member of the board of directors of IDEXX Laboratories. Previously, she served on the board of directors of Analogic Corporation and of Nypro Corporation. She earned a Master's degree in electro-mechanical engineering from KU Leuven in Belgium and a Ph.D. in electrical engineering from Cornell University.

Daniel McGahn was appointed Chief Executive Officer of American Superconductor Corporation (AMSC) in June 2011. He joined AMSC in 2006 as Vice President, Strategic Planning and Corporate Development, and was later promoted to Senior Vice President of Asian Operations. In these roles, he was responsible for establishing AMSC's operations in China, Korea and India. McGahn was elected to the board of directors in 2011. He is known as the only outspoken American CEO who has publicly and relentlessly discussed his experience with China's intellectual property theft. His appearances include a very candid interview on 60 Minutes with Leslie Stahl. From 2003 to 2006, McGahn served as Executive Vice President and Chief Marketing Officer of Konarka Technologies, where he helped significantly boost the company's profile with key external audiences and secure nearly $40 million in financing. McGahn holds Master’s and Bachelor’s degrees in engineering from the Massachusetts Institute of Technology.

About Our Moderator:

Walter M. Pressey is Vice Chairman and President (Retired), Boston Private Financial Holdings. He is a respected business leader and independent director, with extensive experience leading financial services institutions, negotiating mergers and acquisitions and conducting investor relations. He is an Independent Director of The Forsyth Institute, a medical research organization dedicated to discovering break-throughs in oral health and disease prevention. Pressey currently serves as a member of the Finance Committee of Boston Children's Hospital, and he serves on the Corporate Advisory Board of The Boston Club.

Meeting Introduction

NACD New England Chapter President Beth Boland opened the October 18th session by thanking the attendees, as well as the main sponsors of the October program, Marsh and Protiviti. She then introduced Moderator Walter Pressey, who in turn introduced the panelists before beginning the formal program.

Panel Highlights

Moderator Pressey opened the discussion by introducing the subject of cybersecurity. He divided victims of cyberattacks into two groups: those who know they have been attacked and those who do not. He then introduced the panelists and asked them to provide introductory comments.

Peter Fonash began, explaining the responsibilities of the Office of Cybersecurity and Communications within the federal Department of Homeland Security. Those responsibilities have included the restoration of Wall Street following the Sept. 11, 2001 terrorist attacks, protecting the federal government's computer networks outside of the military, protecting critical infrastructure, including power and financial systems and a large information sharing program within the government and with the public sector. He then segued into a discussion of intelligent, or "smart," systems, also known as the Internet of Things (IoT). Although these systems promise to add new levels of convenience and sources of data for consumers and businesses alike, they have a significant weakness. "There is tremendous potential, in terms of the quality of life and the things that you can do," Fonash said. "The problem is, we aren't doing very well in cybersecurity, protecting controlled systems. No one is in charge of the Internet of Things."

In this fragmented environment, IoT is very susceptible to external cyberattacks. In response, the Office of Cybersecurity is providing cybersecurity training to information technology officers and other corporate employees charged with protecting their companies' networks. Research shows a low percentage of employees with cyber protection responsibility is sufficiently trained to protect their companies' networks. "The whole idea is that we want all the sectors to self-organize and share practical experience," he said.

Given the increasing number and frequency of cyberattacks, Fonash strongly encouraged companies to undertake a thorough risk assessment. One way to do that is employ the framework recommended by the National Institute of Standards and Technology (NIST). In his view, corporations that want to safeguard their information and protect against liability need to follow the NIST framework. Following these guidelines, companies can enhance employees' cybersecurity training. The framework also enables firms to assess whether they are employing the correct technologies to protect against cyberattacks.

Sophie Vandebroek followed Fonash by discussing potential approaches companies can take regarding cyber protection. She said there are currently many exciting ideas about corporate cybersecurity. She first suggested board directors make sure their companies have a good framework for managing cybersecurity risk. A very good framework, such as the NIST framework, consists of standards, guidelines and practices to promote the protection of critical infrastructure. This prioritized, flexible, repeatable and cost-effective approach should help owners and operators of critical infrastructure to manage cybersecurity-related risk. The framework should also detail how to manage the board's interaction with the company's network. In her view, a company without a framework compromises the security of its information. Next, she reminded the audience that an entire ecosystem is involved when protecting corporate information. Directors need to know the liabilities of their company's information system. These may include supplier interactions with the network and individual devices connecting to the network, including phones, tablets and hotspots.

Daniel McGahn concluded the panel's opening remarks with a description of American Superconductor Corporation (AMSC)'s experience with cyberattacks on its network. The threat, he said, is real. "We are at war. It's a cyber war. If you think about the way conflicts end, there is a winner and a loser. Those who lose, they have to rebuild their way of life completely." In AMSC's case, the threat came from China, which successfully obtained trade secrets regarding AMSC's wind turbine technology. McGahn then described how the Chinese obtained AMSC's technology and the magnitude of the threat to corporate security, from China and other countries. "As a public company, particularly at the board level, it's a very difficult problem to deal with, because you could be so far removed from what they're after or how they're going to attack or how you're going to respond," McGahn said. "You have to act and react as if you put all of your operations and all of your assets in the worst neighborhood in the world. In many cases, we don't fully appreciate that we're all targets. From the government, to individuals, to corporations."

Since the incident AMSC has worked with the federal government to change its business and develop new products. The company has taken lessons it learned to develop solutions to secure the electricity grid.

Q&A Session Highlights

Pressey then opened the discussion to a series of questions from the audience. Highlights are below:

Q. Is there something that might change the dynamic of the cyber threat to corporate networks?
A. Vandebroek said there "definitely is." She said theories are being developed now that could dramatically change how companies think about cyberthreats in the future.

Q. What are the most practical ways in the next three to five years to authenticate and de-authenticate users as appropriate?
A. Fonash began, saying authentication is a difficult practice, with multiple vendors selling multiple standards. "Right now, there aren't any standards," he said. "It has evolved, but I think you have to come up with some simple standard." Vandebroek said there are a number of proposals to standardize and improve authentication.

McGahn countered that these options are currently non-starters for corporations such as power companies because of the magnitude of risk to their networks. AMSC, along with Homeland Security, is working to provide solutions to utilities that make their systems intelligent without increasing cyber risk.

Q: Dan, how do you now protect your intellectual property?
McGahn said that after the incident with China, AMSC learned the attackers had used roughly 800 engineers to copy the turbine technology and could not do so. However, eventually the attackers found an internal employee they could use to hack into AMSC's system. "One of the vulnerabilities, we realized, is our people," he said. In response, the company now encrypts information so that no single actor has access to a complete set of data.

Q: We are starting to look at companies as the victims of cyberattacks, not just as adversaries. What can directors do, given they will be breached?
McGahn responded first, saying the single biggest challenge to a director is disclosure. "You're going to get breached. If you get breached, how do you describe it?" he said. "How do you explain if you don't know what you don't know?" He said that problem causes many companies not to disclose more minor incidents.

Vandebroek emphasized the importance of putting together a communication plan. She also encouraged companies to hire an external expert to help assess their systems. Having a director who is also an IT expert would be an additional safeguard. Fonash likewise encouraged companies to follow best practices in assessing risk and protecting their information.

Q: What should be your information security function within a company?
Fonash said he believes there should be one person, such as a CTO or CIO, who is directly responsible for network security. That person would then report to the CEO. At the same time, a CEO would have dotted-line responsibility for information security.

Q: To what extent should we have a dedicated cyber risk framework?
McGahn believes having a cyber risk framework needs to become inherent in a company's structure and systems. "It has to become a regular part of what you do," he said.

Fonash agreed, saying cyber risk needs to be taken very seriously. "It's one of the most unstable and misunderstood risks you're going to manage," he noted.

Q: Please discuss your cyber security approach to third-parties. Is it industry-specific?
Vandebroek said having a secure ecosystem is important in all industries. She cited the Target breach, in which attackers accessed Target's network through an HVAC supplier. In that case, Target used one portal for all of its suppliers. Fonash suggested creating two portals, one for extremely close supplier relationships and one for all other lesser relationships.

McGahn said companies need to assess whether providing network access, even through an external portal, is worth the security risk. "I would say no," he said. "We make it clear, you can't get to the network."

Q: How do you allocate the resources to invest in cyber security?
McGahn noted that within AMSC's IT budget, cyber security is the No. 1 or No. 2 expense. "It's a priority for us," he said. The company has worked to leverage the expertise of the FBI and Department of Justice, in addition to expending corporate resources.

Meeting Wrap-up

President Boland closed the meeting by thanking the panelists, program committee, sponsors and audience. She closed the October 18th meeting by reminding attendees that the next NACD breakfast program, “Executive Compensation Roundtable,” will be at 7:00 a.m. on November 15 at the Embassy Suites in Waltham.