AUDIT COMMITTEE LEADERSHIP NETWORK
IN NORTH AMERICA
ViewPoints

Issue 46: April 24, 2014

TAPESTRY NETWORKS, INC · WWW.TAPESTRYNETWORKS.COM · +1 781 290 2270

An update on cybersecurity

On March 19, 2014, members of the Audit Committee Leadership Network (ACLN) met in New York to discuss cybersecurity, among other topics.[1] In this session, members were joined by Mr. Joseph Demarest, assistant director at the Federal Bureau of Investigation (FBI) and head of the Cyber Division.[2] For a biography of Mr. Demarest, see Appendix 1, on page 11. For a list of participants, see Appendix 2, on page 12.

Executive summary

Mr. Demarest and the ACLN members touched on three main topics in their discussion of the rapidly changing domain of cybersecurity and its impact on business[3]:

- **Update on the cybersecurity threat** *(page 2)*

  In the short time since the ACLN last discussed cybersecurity, the seriousness of the threat has only increased. Adversaries have grown even more sophisticated in the tools they employ and in the planning and execution of their attacks. Attacks can originate in a fully commercialized criminal underground or in well-funded government espionage agencies.

- **Evolving company responses** *(page 3)*

  Companies are scrambling to improve their responses to the evolving threat. Mr. Demarest and the members noted that many large companies are organizing their defenses more carefully, focusing on the critical assets that must be secure even if perimeter defenses fail and extending security policies to vendors, customers, and other partners. When a serious incident occurs, companies are trying to respond more quickly, with the leadership taking responsibility, especially when an incident becomes public knowledge. Some companies are considering retaliatory tactics, but Mr. Demarest advised caution in the face of unpredictable repercussions. The challenge of what to disclose about cybersecurity and cyberattacks is also evolving, as legislators and the Securities and Exchange Commission (SEC) focus more closely on the issue.

- **Working with the government** *(page 5)*

  Governments are working hard to help companies defend themselves against cybersecurity threats, and the Obama administration has several major initiatives under way. ACLN members heard from Mr. Demarest that the FBI is improving its cooperation with other government agencies, both in the United States and abroad. He told members that they should expect sustained engagement from the FBI, including alerts about threats and unfolding attacks. He also urged companies to build a relationship with the government before they suffer a major attack, though he acknowledged the concerns that companies

---

[1] In the other session, members engaged in a dialogue with Andy Merrill, senior managing director at Teneo Strategy. See Audit Committee Leadership Network, "Dealing with activist investors," *ViewPoints*, April 24, 2014.

[2] Mr. Demarest was speaking in a personal capacity and approved his quotes in this document.

[3] *ViewPoints* reflects the network's use of a modified version of the Chatham House Rule whereby names of members and their company affiliations are a matter of public record, but comments are not attributed to individuals or corporations. Italicized quotations reflect comments made in connection with the meeting by network members and other meeting participants.

often have about sharing information. To help in keeping up with developments, he advised boards to reach out to technical experts within their companies.

Update on the cybersecurity threat

In October 2012, ACLN members met with Shawn Henry, president of the security company CrowdStrike and former executive assistant director at the FBI. At that meeting, members learned that the landscape is rife with adversaries, including criminal groups, foreign intelligence services, terrorists, and hacker activists.[4] They learned about the range of techniques these actors employ, from simple methods of tricking people into revealing passwords to highly sophisticated malware for penetrating networks and stealing data. The harm inflicted could include the loss of key assets such as customer information or intellectual property, direct costs stemming from the loss of business or the need to compensate victims, and reputational damage.

In the March 2014 meeting with Mr. Demarest, the ACLN members and Mr. Demarest noted that developments in the last 18 months have only served to confirm this picture. Indeed, the problem has intensified. Mr. Demarest said, *"The actors are much more sophisticated, in terms of both funding and expertise."* He remarked on the skill that goes into crafting attack methods, such as spear phishing, in which fraudulent email is targeted at a specific victim using information about that victim to make the email appear legitimate. In a pre-meeting conversation, a member said, *"The increasing sophistication of the cyberthreat is unbelievable. Things are happening so quickly, much faster than we thought."*

Members and Mr. Demarest brought up several recent cybersecurity headlines and what they say about the evolution of the threat landscape:

- **The attacks on Target and other retailers.** In December 2013, the retailer Target learned that criminals had breached the company's IT systems and stolen a vast amount of customer data, including credit and debit card data for 40 million customers and personal data such as phone numbers and addresses for another 70 million.[5] The hackers were able to break into Target's network by exploiting holes in network management software and coming in through one of Target's contractors.[6] According to experts, the malware used by the attackers had circulated and steadily improved in the Internet's black markets for attack tools, reflecting the evolution of cybercrime from a solitary activity to a much more organized and sophisticated threat.[7] Echoing the comments of other members and many experts, an ACLN member said, *"It is now a sophisticated, money-making, capitalist environment."*
- **NSA surveillance.** Another major cybersecurity development in 2013 was the steady stream of revelations about the surveillance carried out by the National Security Agency (NSA). Former NSA contractor Edward Snowden revealed that the data collection efforts by the NSA and some of its counterparts in other countries have been bigger in scale and more intrusive than many people had

[4] Audit Committee Leadership Network, *Cybersecurity and the Board,* ViewPoints (Waltham, MA: Tapestry Networks, 2012.

[5] Elizabeth A. Harris, Nicole Perlroth, Nathaniel Popper, and Hilary Stout, "A Sneaky Path into Target Customers' Wallets," *New York Times,* January 17, 2014.

[6] Danny Yadron, "Retail Hackers Exploited Holes in Network-Management Software," *Wall Street Journal,* February 10, 2014.

[7] Charles Levinson and Danny Yadron, "Card-Theft Software Grew in Internet's Dark Alleys," *Wall Street Journal,* January 21, 2014.

realized. These revelations sparked a general outcry across the globe, spawning fears among US technology companies that the trust of their customers is in danger, especially overseas.

The revelations could also affect governmental cybersecurity initiatives. Last summer, the *New York Times* reported that the NSA had been championing a plan to scan Internet traffic for signs of attack against American companies, creating a kind of "Star Wars" defense that would intercept cyberattacks before they reached their targets. As the NSA came under suspicion, however, the likelihood of such a plan going forward was sharply reduced.[8]

- **Spying by foreign governments.** The exploits of the NSA and its allies were not the only governmental operations in the news. A report released by the security firm Mandiant in February 2013 alleged that hackers linked to the Chinese military may have stolen data on product development and business strategies from thousands of American and European companies.[9] Meanwhile, hackers backed by the Iranian government allegedly gained access to software used to run the control systems at energy companies in the United States. These systems regulate the flow of oil, gas, and electricity, and experts note that their vulnerability poses a threat that could be far more serious than the theft of intellectual property.[10]

Evolving company responses

In the face of the ever-escalating cyberthreat, companies are scrambling to improve their defenses and their responses to cybersecurity incidents.[11] Several ACLN members noted that their companies' strategies have evolved in the last few years, as the threat has evolved and awareness has increased.

Defensive measures

Mr. Demarest and the members mentioned several high-level strategies that companies should employ to reduce the likelihood of a successful attack:

- **Get organized.** In a pre-meeting conversation, one member said that security was less and less an afterthought in company planning: *"They consider security when building the business."* Another member said planning for risks was becoming more comprehensive and thorough: *"Concern has increased and evolved into wanting to know the black swan risks [and] … coming up with scenarios and more specific action plans if indeed something drastic happens."* Mr. Demarest also brought up the organizational element: *"How are you aligning security functions across the enterprise? Do you have a detailed black-and-white plan? What does the team look like in terms of skills? What is the structure of your company's authorities and accountability?"*

---

[8] David E. Sanger, "N.S.A. Leaks Make Plan for Cyberdefense Unlikely," *New York Times,* August 12, 2013.

[9] Rachel Louise Ensign, "Cybersecurity Experts Warn Many Cos May Have Had IP Stolen," *Corruption Currents* (blog), *Wall Street Journal,* March 19, 2013.

[10] Siobhan Gorman and Danny Yadron, "Iran Hacks Energy Firms, U.S. Says," *Wall Street Journal,* May 23, 2013.

[11] For a picture of how a broad sample of companies fared on cybersecurity in 2013, see EY, *Under Cyber Attack: EY's 2013 Global Information Security Survey* (London: Ernst & Young Global Limited, 2013).

- **Protect the crown jewels.** Mr. Demarest emphasized an issue members have discussed before: *"Where does the important stuff sit? Companies need to identify the key risks for the organization if something is lost."* Because it is inevitable that attackers will penetrate a company's network, it is important to identify the company's critical assets and ensure that they are protected from a breach. Perimeter security is still vital, but so are defenses within the perimeter.
- **Consider vendors, customers, and other partners.** Defenses should also extend beyond the perimeter. Mr. Demarest pointed to a lesson from recent retail attacks: *"You're only as strong as your weakest link."* Vendors, customers, and other partners are all too often the vector of penetration for companies, so companies must carefully consider what kind of security policies to apply in their interactions with them.

Incident response

The conversation also touched on how companies should respond during and after an attack, especially a serious one:

- **Respond to incidents quickly.** Mr. Demarest and the members noted that the speed with which a company responds to a breach may make a huge difference in terms of the damage ultimately done. Effective monitoring and well-developed contingency plans allow a company to spot an intruder quickly and take action immediately, though action should be appropriate to the situation and may not always involve immediate public disclosures.
- **Have company leadership take ownership.** Companies should demonstrate their commitment to dealing with incidents swiftly and effectively by putting the top executives in the spotlight, especially in the event of a major incident.
- **Be circumspect about retaliation.** Mr. Demarest mentioned services that allow companies to turn the tables on attackers by helping them to penetrate the computers from which the attacks are coming. Known as "active defense" or "hack back," this tactic is a tempting option for companies, especially if they are the victim of repeated attacks. Mr. Demarest urged caution: *"It's dangerous – they can retaliate. You should discuss it with us – whether or not to do it."* He noted that the legal context is unclear and that companies attempting retaliation could be subject to investigation and prosecution, a potentially embarrassing and unproductive outcome.

Cybersecurity disclosures

Disclosure is a challenging issue, both in the immediate aftermath of an incident and in the context of regular financial reporting. An ACLN member noted, *"Since we last met, there's been more guidance from the SEC about disclosure of cybersecurity events. You have to worry about whether there's an obligation to disclose. For some companies, there have been multiple events. When do you disclose, and when don't you disclose?"*

Both state and federal laws require companies to disclose compromises of certain personal data, and these requirements have been expanding.[12] Challenges for companies include the differences in requirements among states and the broadening definitions of personally identifiable information and protected health information. At the federal level, new rules around patient information make it more difficult to avoid notification.

In addition to these requirements involving personal information, however, companies may also have obligations to investors regarding other types of data losses or cyberattacks that have material consequences. The Division of Corporation Finance at the SEC issued guidance in October 2011 on disclosure of both cybersecurity risks and actual incidents. The guidance noted that "although no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents, a number of disclosure requirements may impose an obligation on registrants to disclose such risks and incidents."[13] The guidance goes on to discuss potential obligations stemming from requirements around the disclosure of risk factors, management's discussion and analysis, the financial statements, disclosures about legal proceedings, and other elements of reporting.

SEC chair Mary Jo White has highlighted the importance of the topic in recent speeches,[14] and the SEC held a roundtable on cybersecurity on March 26, 2014, at which participants discussed the pros and cons of more disclosure requirements and the SEC's role in promoting cybersecurity more generally.[15] Since issuing its guidance, the Division of Corporation Finance has sent a number of comment letters to companies about their cybersecurity disclosures, asking for more clarification, and reflecting, as one observer put it, "the Staff's sustained interest in the topic, encouraging disclosures that go beyond a rote warning that a cyber problem could have some type of adverse impact on the business."[16]

The timing of disclosures regarding an attack may take a number of factors into consideration. Companies may consider delaying disclosures in order to research the event thoroughly and prepare for an onslaught of questions and publicity. Law enforcement may request companies to permit an attack to continue – in a controlled manner – in order to learn more about the methods of the attacker. At the same time, federal securities laws (and other laws) may require timely communication about the event. The possibility of litigation by angry consumers or shareholders is a factor, as is the broader reputational damage the company could suffer.

Working with the government

Governments are keenly aware of the cybersecurity threat and the challenges companies face in addressing it. They are especially concerned about the threat to critical infrastructures, such as the financial system and the

[12] David Geer, "Data Breach Notification Laws, State and Federal," *CSO,* November 1, 2013.

[13] US Securities and Exchange Commission, "CF Disclosure Guidance: Topic No. 2: Cybersecurity," October 13, 2011.

[14] For example, Mary Jo White, "The Path Forward on Disclosure" (speech at the 2013 NACD Board Leadership Conference, National Harbor, MD, October 15, 2013).

[15] Joe Mont, "SEC Could Consider New Cyber-Security Disclosures," *Compliance Week,* April 1, 2014. From Commissioner Aguilar's speeches made at the Practising Law Institute's SEC Speaks conference in March 2014, it is clear that the SEC sees cybersecurity as a systemic risk to the financial system, not simply a disclosure issue.

[16] Anthony Rodriguez, "SEC Continues to Target Cybersecurity Disclosures," *Law360,* November 1, 2013.

power grid. In an effort to help companies defend themselves, governments are seeking to provide intelligence in advance of attacks and assistance when attacks occur. They are also building programs for information sharing among companies and with the government, and they are developing standards of best practice to guide companies' security improvement efforts. Governments want to facilitate a coordinated, organized response to an increasingly organized threat. As a cybersecurity expert told Tapestry, *"It takes a network to defeat a network."*

To achieve this goal, however, governments must navigate a number of difficulties, including bureaucratic inertia and complexity, concerns about sharing sensitive data, and last but not least, given the revelations about the NSA, suspicions about governmental motives and means. Congress has taken up the cybersecurity issue repeatedly, assigning various cybersecurity responsibilities to organizations such as the Department of Homeland Security (DHS) and the National Institute of Standards and Technologies (NIST). However, it has not passed any major new legislation since 2002, though many bills have been proposed.

Recent cybersecurity initiatives

In the absence of legislation, the White House has started taking action. In February 2013, the president signed an executive order designed to improve the cybersecurity of the country's critical infrastructure by, among other things, improving information sharing between the DHS and the private sector, expanding a Department of Defense (DoD) information-sharing initiative with contractors to include key infrastructure companies, and calling on NIST to oversee development of a cybersecurity framework to reduce risks to critical infrastructure.[17]

On the same day that the president signed the executive order on critical infrastructure cybersecurity, he also issued a presidential policy directive (PPD-21) that elaborates on the national policy for critical infrastructure security more generally. PPD-21 identifies 16 critical infrastructure sectors, including such obvious ones as emergency services, energy, and water systems, but also many others, such as the chemical industry, critical manufacturing, and information technology. According to the DHS fact sheet on the executive order and the directive, PPD-21 directs the executive branch to develop a "situational awareness capability" addressing "both physical and cyber aspects of how infrastructure is functioning, [to] understand the cascading consequences of infrastructure failures, [to] evaluate and mature the public-private partnership, [and to] develop a comprehensive research and development plan."[18]

The deadlines for these deliverables range from 120 days to two years, and a year after their launch, observers see substantial progress.[19] For example, NIST has completed a cybersecurity framework outlining five core

[17] Mark Clayton, "Why Obama's Executive Order on Cybersecurity Doesn't Satisfy Most Experts," *Christian Science Monitor,* February 13, 2013, 1.

[18] Department of Homeland Security, *EO 13636 Improving Critical Infrastructure Cybersecurity and PPD 21 Critical Infrastructure Security and Resilience* (Washington, DC: Department of Homeland Security, 2013).

[19] Jon Burd, Maureen Kelly, Emile Monette, Annejanette Heckman Pickens, and Pamela Walker, "The Cybersecurity Executive Order: Implementation Efforts in the First 250 Days" (paper prepared for American Bar Association, November 2013), 3.

cybersecurity functions – identify, protect, detect, respond, and recover – and the specific tasks associated with each one.[20]

Mr. Demarest explained that the government is trying to forge a more integrated approach to cybersecurity. For example, he noted that the FBI is *"trying to blend the criminal side and the national security side,"* an effort that has been ongoing since the FBI's Cyber Division was created more than 10 years ago. In addition, the FBI cooperates extensively with other agencies: *"Everything we do impacts the U.S. Intelligence Community..."*[21]

Members wanted to get a sense of how well the government was doing in the area of cybersecurity, given the daunting challenges. One member brought up the vast army of adversaries: *"How do you set priorities when they have hundreds for every one of you?"* Mr. Demarest acknowledged that resources could be a challenge, but he was optimistic: *"It's hard to find talent. Millennials often leave, but then they come back."* He highlighted the Cyber Division's increased cooperation with authorities overseas: *"We have cyberexperts based with local law enforcement in other countries."*

Implications for companies

ACLN members were curious about what the government's efforts mean for their companies: *"What should boards take away from the changes in policy?"* In the meeting in New York, Mr. Demarest and the members discussed two major questions of interest to members:

- **What can companies expect from the government?** A member asked, *"How can the government productively help us?"* Government security agencies monitor cybersecurity threats and have access to critical information for companies trying to defend themselves. Many members' companies have received information from government agencies about hackers penetrating or attempting to penetrate their systems. They have also received help in investigating and remediating attacks. One member commented, *"The FBI was hugely helpful. The company was very happy that we got them involved."*

  Mr. Demarest said, *"Expect a sustained engagement from us … If we see something, we'll alert you."* The *Washington Post* reported in March 2014 that, according to White House officials, the government notified over 3,000 US companies in 2013 that their systems had been breached.[22] The alerts were provided by the FBI, DHS, and other agencies, and in most cases, the company was completely unaware of the breach.

- **What does the government expect from companies?** Mr. Demarest noted that *"it's really important that the private sector works with government."* He explained that companies should reach out to the government before they are in trouble: *"When the skies are blue, that's when CISOs [chief information security officers] should start the dialogue with government."*

---

[20] Matt Kelly, "Cyber-Security Takes Centerstage: Risks, Guidance, and Regulator Wrath," *Compliance Week,* February 18, 2014. For the framework itself, see National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (Gaithersburg, MD: National Institute of Standards and Technology, 2014).

[21] The U.S. Intelligence Community is an umbrella organization of 17 government agencies involved in intelligence.

[22] Ellen Nakashima, "U.S. Notified 3,000 Companies in 2013 about Cyberattacks," *Washington Post,* March 24, 2014.

Mr. Demarest said that the Information Sharing and Analysis Centers (ISACs) established in critical infrastructure sectors are still a work in progress, but that some of them, such as the financial services ISAC, are thriving. He encouraged companies to participate: *"It's good to be a part of these – it's a baseline of information. Your teams may meet others in the same boat."*

Mr. Demarest also acknowledged the concerns companies often have about sharing information, either with other companies or the government. One of the biggest obstacles to engagement with the government, he noted, is the company's general counsel, who is focused on the risks involved in letting certain information leave the company's control. In response to a member's comment that companies may see government systems as less secure, however, he pointed out that government security agencies maintain cybersecurity systems that are very difficult to penetrate.

A looming question for companies is the potential for new rules and regulations. Regulations on data security currently exist in certain areas, particularly in the financial and healthcare sectors. In January 2014, the SEC announced that it will include a review of cybersecurity measures in its routine examinations of investment advisers and investment companies.[23] The SEC's national associate director for the examinations program said that the SEC would be looking to see "what policies are in place to prevent, detect, and respond to cyber attacks."[24] Notably, the SEC also plans to examine "policies on IT training, vendor access and vendor due diligence."[25]

In the wake of additional incidents such as the Target breach, lawmakers may attempt to impose broader requirements. Several legislative proposals have recently emerged in Congress that would expand regulations on cybersecurity.[26] For example, Senators Richard Blumenthal (D-CT) and Ed Markey (D-MA) have introduced legislation creating a process for helping companies establish security plans for protecting consumer data and holding them accountable for following those plans.[27] Mr. Demarest reflected that *"there has been progress, but we need tangible legislation. The NIST framework is a good first step."*

The NIST standards are voluntary, but an observer noted that they would likely be influential: "It will be how companies are judged by lots of different parties – by insurers, by plaintiffs' counsel in class-action litigation following a cybersecurity event. It will form the standard of care for what is a reasonable standard of care in this country."[28]

Board oversight

In the October 2012 meeting, Mr. Henry emphasized that corporate boards have a critical leadership role to play in cybersecurity. He encouraged directors to work with senior management to establish a clear

[23] Sarah N. Lynch, "SEC Examiners to Review How Asset Managers Fend Off Cyber Attacks," *Reuters,* January 30, 2014.

[24] Ibid.

[25] Ibid.

[26] Mauricio F. Paez, Richard J. Johnson, Steven G. Gersten, and Mina R. Saifi, "U.S. Congress Ready to Enact Data Security and Breach Notification Rules After Recent Consumer Data Breaches," *Jones Day Publications*, February 20, 2014.

[27] Richard Blumenthal, "Ahead of Senate Judiciary Committee Hearing on Data Breaches, Blumenthal, Markey Introduce Bill to Protect Consumer Information from Hackers," news release, February 4, 2014.

[28] Ben DiPietro, "The Morning Risk Report: NIST Standards To Serve as Baseline for Policies," *Risk and Compliance Journal* (blog), *Wall Street Journal,* February 13, 2014.

structure of responsibilities, capabilities, and accountability.[29] Reflecting on developments since the 2012 meeting, several ACLN members said that the board's focus on cybersecurity is intensifying, but access to expertise continues to be an issue. Should boards rely exclusively on effective communication from management and internal audit, or should they supplement what they hear from management with expertise hired from outside the company?

Keeping up with the rapid pace of change in the cybersecurity landscape is a persistent challenge, as is determining how deep to go in evaluating the threats to the company and the adequacy of its defenses. One member asked, *"Are we too out of it to know what questions to ask, and how to think about these issues?"* Mr. Demarest encouraged board members to seek help from the experts within a company: *"The techies are happy to explain it to you. Ask them about what protections you have. The NIST framework is a good starting point for a discussion with them."*

A member described a time when government involvement stymied communication between management and the board: *"Management was prevented from talking to the board. How can we react without information?"* Mr. Demarest assured the members that the FBI is aware of the problem and is ready to respond: *"We try to give you something unclassified – 'Here's what you can talk about.' But if you need more, request more."*

Reviewing the role of the audit committee and the board in overseeing cybersecurity, ACLN members and Mr. Demarest developed a set of questions that audit committees can ask management. See Appendix 3, on page 13.

Conclusion

Mr. Demarest and the ACLN members explored a range of issues relating to cybersecurity, including the rapid evolution of the security threat, the measures companies can implement at the enterprise level to defend themselves, and the ways in which companies can work with the government and each other to improve cybersecurity. The picture that emerged was of a pitched battle in which increasingly sophisticated and organized adversaries can only be countered by better organized defenders working more closely with one another. When asked about his vision for cybersecurity in the future, Mr. Demarest mentioned not only technological innovations such as machine-to-machine information sharing, but also cooperation between companies and government: *"The trust between the private and public sector continues to grow and evolve."*

[29] Audit Committee Leadership Network, *Cybersecurity and the Board,* 9–10.

About this document

The Audit Committee Leadership Network is a group of audit committee chairs drawn from leading North American companies committed to improving the performance of audit committees and enhancing trust in financial markets. The network is organized and led by Tapestry Networks with the support of EY as part of its continuing commitment to board effectiveness and good governance.

ViewPoints is produced by Tapestry Networks to stimulate timely, substantive board discussions about the choices confronting audit committee members, management, and their advisers as they endeavor to fulfill their respective responsibilities to the investing public. The ultimate value of *ViewPoints* lies in its power to help all constituencies develop their own informed points of view on these important issues. Those who receive *ViewPoints* are encouraged to share it with others in their own networks. The more board members, members of management, and advisers who become systematically engaged in this dialogue, the more value will be created for all.

Appendix 1: Biography of Joseph M. Demarest, Jr.

As a veteran of the FBI, Joseph M. Demarest, Jr., has worked a variety of investigative matters, including counterterrorism, white-collar crime, organized crime/drugs, violent crime, and foreign counterintelligence. He has held a number of supervisory and leadership positions at FBI headquarters and in the field, including his former position as head of the International Operations Division. In this role, Mr. Demarest was responsible for leading the FBI's international and overseas law enforcement operations, liaison, and training efforts and, as such, managed over 600 employees in 75 foreign and domestic locations.

Mr. Demarest began his career with the FBI in 1988 as a special agent. Upon graduation from new agent training at the FBI Academy in Quantico, Virginia, Mr. Demarest was assigned to the Anchorage Division, where he investigated white-collar crime, drugs, violent crime, and foreign counterintelligence matters. In 1990, he transferred to the New York Division, where he was promoted to squad supervisor in 1999 and was selected as the division's SWAT team leader. In 2000, Mr. Demarest was selected to serve as the drug branch's acting assistant special agent in charge. In this capacity, he oversaw seven active drug squads comprising more than 150 agents, task force officers, and support personnel. He also worked closely with New York and New Jersey High-Intensity Drug Trafficking Area executives in the development of New York City's first Regional Intelligence Center (RIC). The RIC consisted of five sections with a total of more than 550 representatives from federal, state, and local law enforcement agencies.

After 9/11, Mr. Demarest served as a shift commander for the FBI's investigation of the attack, leading a task force of more than 400 federal, state, and local investigators from more than 40 disparate agencies. In 2002, Mr. Demarest was selected to lead a team of FBI personnel deployed to the joint task force at the US naval station at Guantanamo Bay, Cuba. This team conducted interviews, threat assessments, and analysis critical to the FBI's counterterrorism and intelligence mission.

Mr. Demarest was promoted to unit chief at FBI Headquarters in 2002, where he served in the International Terrorism Operations Section (ITOS) within the Counterterrorism Division. In 2003, he was promoted to assistant section chief of ITOS. He later served as an acting section chief in ITOS until he was promoted to assistant special agent in charge of the New York Division's international terrorism branch. He was later selected as the special agent in charge of counterterrorism and served in that role until early 2008.

In December 2008, Mr. Demarest was appointed by Director Mueller to the position of assistant director in charge of the New York Division. During his tenure, Mr. Demarest oversaw several major investigations, including the terrorism investigation known as Operation Highrise, the Bernard Madoff case, and the piracy investigation of MV Maersk Alabama.

Mr. Demarest was appointed assistant director of the Cyber Division in June 2012. He has been the recipient of the Attorney General's Award as well as the Director's Award.

Appendix 2: Participants

Audit chairs who participated in all or part of the meeting:

- Les Brun, Audit Committee Chair, Merck
- John Edwardson, Audit Committee Chair, FedEx
- Gene Fife, alumnus, Former Audit Committee Chair, Caterpillar
- Marie Knowles, Audit Committee Chair, McKesson
- Mike Losh, Audit Committee Chair, Aon and TRW Automotive
- Blythe McGarvie, Audit Committee Chair, Viacom
- Oscar Munoz, Audit Committee Chair, United Airlines
- Guylaine Saucier, Audit Committee Chair, Areva*

EY was represented in all or part of the meeting by:

- Tom Hough, Americas Vice Chair of Assurance Services
- Steve Howe, Americas Managing Partner
- Frank Mahoney, Americas Vice Chair of Assurance Services (effective July 2014)

* Member of the European Audit Committee Leadership Network

Appendix 3: Questions audit committees can ask management

- What cybersecurity threats is management seeing? What threats are they dismissing, and why?
- Is the company using the NIST framework?
- Is the company using what-if scenarios to determine the potential worst outcomes of an attack?
- Where are intrusions coming from? If the origins are unknown, why hasn't management asked government agencies for help?
- What is the response plan for an attack, and how does the plan factor in customers and suppliers?
- Who is on the response team, and are the legal and communications functions involved?
- To whom does the CISO report, and does the CISO work hand in hand with physical security?
- Is the company working with industry groups?
- Is the company sharing information with government agencies such as the FBI?
- If the company is considering the use of "hack back" tactics against intruders, is it aware of the possible repercussions?