EUROPEAN
AUDIT COMMITTEE LEADERSHIP NETWORK
ViewPoints

Issue 40: 12 May 2014

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

Update on cybersecurity

On 2 April 2014, members of the European Audit Committee Leadership Network (EACLN) met in London to discuss cybersecurity, among other topics[1]. In this session, members were joined by Andrew Archibald, deputy director of the National Cyber Crime Unit of the United Kingdom's National Crime Agency (NCA) and Paul C Dwyer, director of strategic solutions at the security firm Mandiant (recently acquired by FireEye).[2] For biographies of Mr Archibald and Mr Dwyer, see Appendix 1, on page 12.

Executive summary

EACLN members and their guests discussed a number of issues related to cybersecurity, which fell into three main areas:

- **Update on the cybersecurity threat and company responses** *(Page 2)*

  Since the EACLN members' last discussion of cybersecurity in November 2012, cyberattacks of various kinds have continued to draw headlines, revealing an increasingly sophisticated criminal underground and extensive surveillance by intelligence agencies like the US National Security Agency (NSA). Mr Dwyer and Mr Archibald underscored the gravity of the threat and Mr Dwyer lamented the impact of NSA contractor Edward Snowden's revelations on trust in government. Meanwhile, companies are scrambling to improve their defenses against evolving threats. Members and guests mentioned measures such as extending security policies to business partners and employees' mobile devices and developing plans that enable quick and effective responses to incidents.

- **Government initiatives** *(Page 5)*

  Governments are also struggling to marshal an effective response to the threat. Fresh legislation and new organizations are emerging at both the national and European Union (EU) level. Efforts are aimed at strengthening government capabilities, supporting cooperation and information sharing among companies and with government, and mandating security measures for certain types of data and in certain sectors. Reflecting on how law enforcement works with the private sector, Mr Archibald pointed to a cultural shift in which deeper engagement on prevention and mitigation increasingly complements investigation and prosecution.

- **Board oversight** *(Page 8)*

  Boards are struggling to keep up with the rapid evolution of the problem and how they address it. Mr Dwyer offered a number of actions for boards to take, noting that companies may be liable for failing to achieve an adequate standard of supervision. For boards and especially audit committees, the question of what to disclose about security incidents and company responses is an additional challenge involving not only compliance with breach notification laws but also strategic considerations around the timing of disclosures and the accounting for associated costs.

For a list of discussion questions for audit committees, see Appendix 3, on page 14.

[1] In another session, members discussed the FRC with Stephen Haddrill, chief executive officer of the Financial Reporting Council. See European Audit Committee Leadership Network, "A dialogue with Stephen Haddrill" *ViewPoints,* 12 May 2014.

[2] *ViewPoints* reflects the network's use of a modified version of the Chatham House Rule whereby names of network participants and their corporate or institutional affiliations are a matter of public record, but comments are not attributed to individuals, corporations or institutions. Network participants' comments appear in italics.

Update on the cybersecurity threat and company response

When EACLN members last discussed cybersecurity in November 2012, they heard about a threat landscape rife with adversaries, including criminal groups, foreign intelligence services, terrorists and hacker activists.[3] They learned about the range of techniques these adversaries use, 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 conversations leading up to the April 2014 meeting and in the meeting itself, the guests and EACLN members noted that developments in the last 18 months have only served to deepen companies' impression of the complexity and seriousness of the threat. One member said, *"The increasing sophistication of the cyberthreat is unbelievable. Things are happening so quickly, much faster than we thought."* Other members observed that a major change in recent years is the public's heightened awareness, which is pressuring companies and policymakers to take action.

Sophisticated criminal attacks on companies and Internet users

A number of attacks in recent years illustrate how the threat from cybercriminals is evolving:

- **An attack on the Port of Antwerp.** In October 2013, the head of the European Police Office (Europol), Rob Wainwright, described a scheme in which drug traffickers hired hackers to penetrate the information technology (IT) systems of companies running operations in the Port of Antwerp.[4] To facilitate the smuggling of drugs through the port, the hackers accessed data on shipping containers that allowed the traffickers to intercept the compromised containers before their lawful owners could do so.

  Mr Wainwright noted that the scheme, which ran for two years starting in June 2011, demonstrated that cybercrime is becoming a more organized, commercial activity.[5] An EACLN member said, *"It shifted from independent hackers to a community of hackers to criminal organizations. That has increased risk."*

- **A sophisticated denial-of-service attack.** Early in 2013, an antispam organization called Spamhaus, based in the United Kingdom and Switzerland, suffered a so-called DDoS (distributed denial-of-service) attack that lasted nine days, targeting a number of Internet exchanges and slowing traffic for many Internet users. While a DDoS attack is in itself nothing new, one commentator remarked on the "scope, duration, and sophistication" of this attack and wondered if similar attacks would follow.[6] An EACLN member said, *"The ability for less well-funded groups to wreak havoc has increased. Setting up DDoS attacks is much cheaper."*

- **A massive breach in the systems of retailers in the United States.** In December 2013, the US 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.[7] The hackers were able to break into Target's

---

[3] European Audit Committee Leadership Network, *Cybersecurity and the Board, ViewPoints* (Waltham, MA: Tapestry Networks, 2013), page 5.

[4] Tom Bateman, "Police Warning after Drug Traffickers' Cyber-attack," *BBC News,* 16 October 2013.

[5] Ibid.

[6] Pat Calhoun, "The Nine-Day Cyber Attack That Broke the Internet," *CNBC,* 3 April 2013.

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

network by exploiting holes in network management software and coming in through one of Target's contractors.[8]

According to experts, the malware used by the attackers circulated and steadily improved in the Internet's black markets, illustrating again the evolution of cybercrime from a solitary activity to a much more organized and sophisticated threat.[9] The news about the breach at Target was followed by similar news from another US retailer, Neiman Marcus, which reported in early January that an attack on its computer systems may have led to data thefts from as many as 1.1 million card accounts.[10]

Other sectors have also been hit with cyberattacks recently. The security firm CrowdStrike reported in January 2014 that a Russian hacking group attacked organizations in sectors that included education, manufacturing, healthcare and government, striking targets in North America, Europe, Asia and the Middle East.[11] Also in January, a massive theft of data from three Korean credit card companies prompted three dozen executives to resign as thousands of Koreans cancelled their credit cards. The thief was a contractor working on security systems.[12]

Reflecting on the current threat landscape, Mr Dwyer said, *"We have to learn from the criminals. They have a great business model. They network, collaborate, share and train each other, so we have to do the same. They have their finger on our pulse, so they know what our reactions are going to be. They don't work in silos, so we can't either. Cybercriminals work with other cybercriminals, pedophiles and terrorists. We treat cybercrimes as silos – fraud, theft, etc. Instead, we have to have a holistic view of cyberthreats."*

Revelations about governmental espionage

Another major cybersecurity development in 2013 and 2014 was the steady stream of revelations about national government agencies – especially the NSA – conducting electronic surveillance. Former NSA contractor Edward Snowden revealed that data collection efforts by the NSA and some of its counterparts in other countries were bigger in scale and more intrusive than many people had realized.

The NSA and other agencies allegedly not only requested data from leading technology firms, but also collected data from those firms apparently without the firms' knowledge.[13] The revelations sparked a general outcry across the globe, leading technology companies to fear for the trust of their customers. An EACLN member said, *"I do see some backlash – any American technology is not as welcome as in the past."*

The United States is not the only nation whose espionage operations have been in the news. A report released by 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.[14] Later in the year, FireEye reported that Chinese hackers breached the computer systems of five European

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

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

[10] Suzanne Kapner, "Malware Lurked for Months inside Neiman," *Wall Street Journal,* 23 January 2014.

[11] Nicole Perlroth, "New Security Report Confirms Everyone Is Spying on Everyone," *Bits* (blog), *New York Times,* 22 January 2014.

[12] Simon Mundy, "Executives Quit after Massive South Korea Data Theft," *Financial Times,* 21 January 2014.

[13] Barton Gellman and Ashkan Soltani, "NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say," *Washington Post,* 30 October 2013.

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

governments around the time of the G20 summit in September.[15] An EACLN member remarked, *"There is a realization that it will be hard to keep out nation-state attackers."*

Mr Dwyer described the multitude of motivations behind Chinese state-sponsored espionage: *"They want to understand your business model. They want to learn from you – what you do and how. They are as interested in your QA [quality assurance] process as anything else. The Chinese army is taking the data and working out what to do with it. They will take your technology and replicate it. They want to understand about M&A [mergers and acquisitions] deals. They use it for other purposes as well. For example, they can learn about financial systems."*

Evolving defenses

In the face of the ever-escalating cybersecurity threat, companies are scrambling to improve their defenses. In a previous EACLN meeting on cybersecurity, several high-level strategies emerged, reflecting the uncomfortable truth that network breaches are inevitable. Hence, companies should prioritize securing sensitive information and systems and monitor the network continuously. At the same time, the network perimeter remains the first line of defense in a multipronged security program.[16]

In the April meeting and conversations leading up to the meeting, EACLN members and their guests reiterated the importance of in-depth defenses. A member said, *"It's important to be able to neutralize attackers when they are in our systems. It's important to segment our systems."* They mentioned vulnerability testing: *"Every year, an outsider does ethical hacking. Every year, they look at procedures, software, etc."*

Members and guests also brought up additional measures for improving cybersecurity. This time the focus was on speed of response and the extension of protection outside the company perimeter, an imperative that has emerged with expanded outsourcing and implementation of new technologies:

- **Plan for a quick response.** One member emphasized the importance of being able to respond quickly to an attack: *"The damage is proportional to the reaction time. Cybersecurity is the ability to understand that you are under attack, and the time of reaction is key."*
- **Scrutinize vendors and other business partners.** A member remarked, *"Most of our businesses have outsourced data management – the pipes that connect business all around the world. We don't have enough visibility into vendors' own security – what are the exposures of vendors' data centers, for example?"* Mr Dwyer said that in 2013, a survey by Mandiant showed that breaches coming through companies' partner networks were increasing,[17] and he recommended that companies not rely on the same vendor for data management and security. Mr Archibald agreed by emphasizing it's important to know who subcontractors are and what access they have to systems.
- **Secure mobile devices.** An EACLN member said, *"The other threat is moving from the PC in a network with a firewall to tablets that are mobile. Tablets are used by employees for enterprise and personal use. That is a new threat vector."* Mr Dwyer elaborated: *"There are two parts of BYOD [bring your own device] – technical and cultural. 'Generation Z' lives in a cyberworld and sees BYOD as their right. They don't want two devices. The traditional model was to build fortress walls. Now data travels*

[15] Sally Davies, "Chinese Hackers Accused of Accessing European Ministries," *Financial Times,* 10 December 2013.
[16] European Audit Committee Leadership Network, *Cybersecurity and the Board*, page 5.
[17] Mandiant, *M-Trends® 2013: Attack the Security Gap™* (Washington, DC: Mandiant, 2013).

the world on these devices. We need to look at the technology. How do we put armor on the data when it leaves the castle? Data shouldn't travel without protection." Social media and cloud computing offer other avenues for hackers to exploit,[18] creating an environment that a member described as *"exploding with complexity and danger."*

Technological advances will continually present new innovations in cybersecurity that will need to be evaluated as potentially worthwhile investments. An EACLN member mentioned the promise of artificial intelligence and analytics: *"Can we develop systems to see risks before they are evident? If we can anticipate the construction of an attack, if the system is thinking in the same way, we can understand the threat before it actually materializes."*

Government initiatives

In pre-meeting conversations, several EACLN members said that governments need to play a major role in cybersecurity. Some members believe progress has been too slow: *"The one who is lagging behind is the government. The government is not taking the lead in protecting us. It's normal for the police to patrol the streets and prevent burglary, but not to patrol the Internet."*

Yet governments are keenly aware of the cybersecurity threat and the challenges companies face in addressing it. They are concerned about access to personal information and intellectual property, as well as the threat to critical infrastructures, such as financial systems and the power grid. And they recognize the need for governments to facilitate a coordinated, organized response to an increasingly organized threat.

As far back as 2001, governments in the Council of Europe drew up a treaty on cybercrime known as the Budapest Convention, which established ground rules for law enforcement efforts on cybercrime. The convention provides guidance on what constitutes a cybercrime and what kind of investigative procedures are acceptable, thereby facilitating cooperation by authorities across borders.[19]

European national governments and the EU are increasingly active in the area of cybersecurity. The European Commission proposed a network and information security directive in February 2013 that focuses squarely on how to coordinate and improve cybersecurity across Europe, and this directive was approved by the European Parliament in March 2014.[20] Other EU legislation also touches on the issue. Governments are addressing cybersecurity on at least three fronts that are directly relevant for companies: strengthening governments' own capabilities, supporting cooperation and information sharing, and mandating data protection and other security measures.

Strengthening government capabilities

Government security agencies can monitor cybersecurity threats and investigate incidents when they occur, and they are attempting to strengthen these capabilities. In the United Kingdom, for example, the National Crime Agency's National Cyber Crime Unit (NCCU) combines the capabilities of two precursor organizations, the Police Central e-Crime Unit in the Metropolitan Police Service and the cyber division of

[18] More technologies are on the horizon. See EY, *Under cyber attack: EY's 2013 Global Information Security Survey* (London: Ernst & Young Global Limited, 2013).

[19] The Convention on Cybercrime was signed on 23 November 2001 and entered into force on 1 July 2004.

[20] European Parliament, *European Parliament Legislative Resolution of 13 March 2014 on the Proposal for a Directive ... Concerning Measures to Ensure a High Common Level of Network and Information Security across the Union* (Brussels: European Parliament, 2014).

the Serious Organized Crime Agency. It has already had success in alerting companies and consumers about threats.[21]

Mr Archibald commented on the challenges and recent developments in the United Kingdom, where there has been substantial progress: *"The NCA's Cyber Crime Unit leads, coordinates and supports law enforcement activity against cybercrime. It has the capability to respond in fast time to rapidly changing threats and collaborates with partners to reduce cyber crime and cyber-enabled crime."*

International cooperation is key. Mr Archibald noted that the United Kingdom cooperates very closely with four other countries – the United States, Canada, Australia, and New Zealand – through a program known as Five Eyes Cyber Crime Working Group. Mr Archibald currently chairs the group. At the EU level, the European Cybercrime Centre (EC3) was established in January 2013 as part of Europol. In its proposed directive on cybersecurity, the European Commission states that cybercrime expertise gathered in the EC3 shall be used to support the member states in capacity building and cybercrime investigations.[22] The cybersecurity directive itself includes a number of measures to expand capacity, requiring, for example, that each member state set up a computer emergency response team for monitoring and responding to cybersecurity incidents.[23]

Supporting cooperation and information sharing

Governments are also building programs for information sharing among companies and with the government. Given the extent of the threat and the escalating severity of attacks, many in the government and the private sector see the need for more and better cooperation. As part of its cybersecurity program, for example, the UK government launched the Cyber Security Information Sharing Partnership in 2013, providing a platform for government agencies, law enforcement authorities and companies to share information on threats and responses in real time.[24]

In addition, MI5, the UK domestic security service, and GCHQ, the British signals intelligence agency, are urging the chairs of boards and audit committees of FTSE 350 companies to participate in a "cyber governance health check" that involves filling out a questionnaire on how their companies are protecting intellectual property and customer data.[25] The results will allow the government to assess the overall state of cybersecurity among the FTSE 350, and they will allow companies to see how they compare with their peers. As part of the health check, the company would discuss vulnerabilities with its audit firm.

In a pre-meeting conversation, Mr Dwyer pointed to the information-sharing efforts that have been established in the United States, such as the FBI-sponsored, region-based InfraGard program and the sector-based Information Sharing and Analysis Centers (ISACs). Although these programs have faced a number of challenges, the US government continues to improve on them, and now that they have been in place for a number of years, they are achieving success in some areas. Mr Dwyer said, *"That is the model Europe needs to push."*

---

[21] Francis Maude, "UK Cyber Security Strategy: Statement on Progress 2 Years on" (written statement to Parliament, London, 12 December 2013).

[22] European Commission, *Proposal for a Directive of the European Parliament and of the Council Concerning Measures to Ensure a High Common Level of Network and Information Security across the Union* (Brussels: European Commission, 2013), page 6.

[23] European Parliament, *European Parliament Legislative Resolution of 13 March 2014 on the Proposal for a Directive ... Concerning Measures to Ensure a High Common Level of Network and Information Security across the Union*, Article 7.

[24] Maude, "UK Cyber Security Strategy: Statement on Progress 2 Years on."

[25] Alison Smith and Henry Mance, "MI5 and GCHQ Urge 'Cyber Health Check' for UK Companies," *Financial Times,* 24 July 2013.

Mr Archibald argued for a cultural shift in how government works with industry and battles cybercrime: *"Industry is a key factor in success on cybercrime as it happens on your networks. You don't want to be a victim; you want to mitigate and fight back. We need intelligence without you needing to report it. We have to accept caveats on how the information is handled. It is working in national security and cyberterrorism, but in law enforcement we can do better. The motivation is that with the government investment in cybersecurity, we have intelligence to share, too."*

Several EACLN members mentioned working with the government, but some wanted more and better intelligence: *"We have good conversations with army specialists, but we don't get their full insights. It would be helpful if the government understood that protecting the financial system is as important as protecting us against tanks."*

Members also acknowledged the value of information sharing among companies. One said, *"Cooperation between companies is essential, including exchange of information in real time."* Some raised the issue of whether such information sharing might cause problems with regulators. One member wanted the government to provide clearer support: *"At least set up a system where we could safely exchange information and really work together as an industry, without being attacked by antitrust people. Now, the question is always, how far can we go?"* Another member was less worried: *"We don't see antitrust issues – we're simply exchanging information on hacker techniques to create a common understanding."*

Mr Archibald emphasized the value for companies of cooperating with other companies as well as the government: *"There is a lot in it for you. If you are a victim and you simply hire someone to fix the breach or patch it, you will be a victim again. You need to understand the criminals and stop them. If you are attacked, would you want to share information with a colleague in another company to stop future attacks? I think you would."*

Mandating data protection and other security measures

Governments are increasingly starting to mandate that companies implement security measures. For example, the EU is working on a major upgrade of its data protection framework, which addresses many aspects of how personal information is processed, stored and transferred, including how the information is secured. In March 2014, the European Parliament approved an amended version of a proposal on data protection put forth by the European Commission in early 2012. Article 30 of the proposal lays out a number of general but nevertheless significant security requirements. Organizations must ensure the security of systems and services processing personal data, and they must be able to take action to protect and restore data in the event of an incident.[26]

The regulation sets up a European Data Protection Board, which will, among other duties, issue guidelines regarding security measures for specific sectors and data processing situations, taking into account developments in technology to determine the "state of the art." Two of the many elements of the regulation that have drawn attention are its jurisdictional scope and the fines imposed for non-compliance. Companies could face a maximum fine of €100 million or 5% of annual worldwide revenue, a much higher

[26] European Parliament, *European Parliament Legislative Resolution of 12 March 2014 on the Proposal for a Regulation ... on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (Brussels: European Parliament, 2014), Article 30.

amount than initially proposed by the European Commission. The regulation would apply to EU citizens' data regardless of where the company processing their data is located.[27]

Mr Dwyer brought up the proliferation of data regulations worldwide and noted its impact on cloud computing in particular: *"The cloud is akin to the electricity grid. It's a great opportunity for business, but 'mind the gap' when you go to cloud computing, because there are various problems. There are over 400 data security regulations and 10,000 overlapping controls from 38 jurisdictions."* Regarding how to handle the multiplicity of jurisdictions, he said, *"We need a unified framework to deal with it using traditional risk management techniques. You have to operate legally. You can delegate, but not abdicate responsibility. Encryption is illegal in some countries. Get legal counsel and procurement involved. Ask where the data goes if you change data centers. How is it scrubbed? Most regulations don't take into account cloud-based technology."*

Mandates to implement security are going beyond protecting personal data. The proposed cybersecurity directive, as amended by the European Parliament, stipulates that operators of critical infrastructures in sectors like electricity, oil and gas, transportation, and food must also take "appropriate and proportionate technical and organizational measures" to protect their networks and information systems.[28]

Board oversight

In the November 2012 meeting, EACLN members agreed that the board has a critical leadership role to play in cybersecurity. They identified several approaches the board can take to ensure effective oversight: leveraging the company's risk management machinery, bringing in internal audit, and hiring outside experts.[29] In conversations leading up to and during the April meeting, members mentioned many of these approaches again.

Reflecting on developments since the 2012 meeting, some members said that the board's focus on cybersecurity is intensifying. One member noted, *"We used to have sessions once every two or three years, but now it's more like once a year. In the audit committee, we now have very in-depth sessions on what we are doing."* Yet a few members worried that the board's attention to cybersecurity is still insufficient: *"Board members are talking about it, but as if it's happening elsewhere."* One member was particularly worried about European boards: *"I don't see the same paranoia as I see in the US, which worries me."*

A persistent challenge for boards is keeping up with the rapid pace of change in the cybersecurity landscape and determining how deep to go in evaluating the threats to the company and the adequacy of its defenses. The issue of expertise continues to be problematic: *"We're not in a position to really know. If they tell us we're safe, we have to accept that."*

Mr Dwyer noted that the Budapest Convention on cybercrime has an article directing governments to establish corporate liability for "lack of supervision and control" that makes a cybercrime possible by employees or agents of an organization,[30] a provision that could be interpreted as establishing liability for the

[27] Stephen Gardner, "European Parliament Votes Overwhelmingly in Favor of Data Protection Reform Proposal," *Bloomberg BNA,* 17 March 2014.

[28] European Parliament, *European Parliament Legislative Resolution of 13 March 2014 on the Proposal for a Directive ... Concerning Measures to Ensure a High Common Level of Network and Information Security across the Union,* Article 14.

[29] European Audit Committee Leadership Network, "Cybersecurity and the Board," page 7.

[30] Convention on Cybercrime, Article 12, paragraph 2.

company if directors do not adequately exercise their duty of care to prevent the company from committing a crime.

Reflecting on the role of the board in defending an organization from attack by others, Mr Dwyer suggested several actions based on recommendations in a forthcoming book by him:

- **Stay informed.** Board members should stay informed about threats and understand the potential impact on their organization (including its supply chain).
- **Assign responsibility.** The board should hold a senior executive accountable for management of cybersecurity risks.
- **Ensure resources are in place.** The board should ensure that sufficient resources are allocated for related cybersecurity risk management activities.
- **Ensure company compliance.** The board should ensure the company keeps abreast of legislation and regulation that deal with cybersecurity, and it should ensure compliance with those laws and regulations.
- **Communicate.** The board should communicate the importance of cybersecurity risk management and all related activities to the entire organization.
- **Request reports.** The organization should provide the board with regular reports on top cybersecurity risks.
- **Insist on internal evaluations.** The board should require internal audit to evaluate cybersecurity risk management capabilities as part of quarterly reviews.
- **Assess organizational capability.** The board should ascertain the organization's in-house capability for handling cybersecurity risk management activities and establish relationships with specialist providers as necessary.
- **Establish metrics.** The board should agree on metrics that will rate the organization's defenses.
- **Ensure integration.** The board should ensure that cybersecurity risk management activities are integrated into all related key processes, such as business continuity, acquisitions, mergers, crisis communication and even marketing.

Cybersecurity disclosures

For boards and especially audit committees, the question of disclosure is another element of the cybersecurity dilemma. What should companies disclose to investors and the public about the cybersecurity threats they face and the measures they have taken to defend themselves? What should they disclose about a cybersecurity incident and its impact?

With regard to personal data, there are clear legal requirements regarding breach notification, and these are becoming more stringent. For example, the EU data-protection regulation currently under negotiation by the European Parliament and the EU Council requires a company experiencing a breach to notify "without undue delay" the supervisory authority in its respective country (Article 31) and the people whose data have been compromised (Article 32).[31] For telecommunications operators and Internet service providers, a new EU regulation on breach notification came into force in August 2013, revising the e-Privacy Directive of 2009.[32] The regulation requires at least an initial communication to national authorities within 24 hours of a breach, followed by more detail within three days.

While there are specific legal requirements around breaches of personal data, other types of breaches or security incidents may present dilemmas of their own. In some cases, public disclosure is clearly necessary, even if personal data are not involved. One member said, *"We disclose when the systems are down; we have to give an explanation."* In other cases, the material impact of an incident on a company's operations or results may need to be addressed. EY experts note that these types of disclosures entail considerations such as the precise timing of the disclosures, the accounting for the costs of a breach, and the impairment of stolen intellectual property.

Conclusion

The EACLN members and their guests discussed a cybersecurity landscape of ever increasing complexity and danger, in which adversaries are highly motivated, skilled and organized. Companies' responses are evolving as well, expanding beyond the company perimeter to focus on business partners and employees' mobile devices. However, Mr Archibald and Mr Dwyer said that cooperation with both the government and other companies is critical. Mr Dwyer noted, *"It takes a network to defeat a network."* As governments seek to deepen cooperation, they are making cultural changes in how they work with each other and the private sector, moving beyond an exclusive focus on investigation and prosecution of cybercrimes to deeper engagement based on mutual respect for stakeholders' concerns and capabilities.

[31] European Parliament, *European Parliament Legislative Resolution of 12 March 2014 on the Proposal for a Regulation … on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data,* Articles 31 and 32.

[32] Warwick Ashford, "EU Data Breach Disclosures to Be Enforced Soon," *ComputerWeekly.com,* 19 August 2013.

EUROPEAN
AUDIT COMMITTEE LEADERSHIP NETWORK
ViewPoints

About this document

The European Audit Committee Leadership Network is a group of audit committee chairs drawn from leading European 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.

EYG no. AU2416

Appendix 1: Biographies of Mr Archibald and Mr Dwyer

Andrew Archibald

Andrew Archibald is the Deputy Director of the National Crime Agency's National Cyber Crime Unit (NCCU), which was formed by joining the Serious Organized Crime Agency (SOCA)'s cybercrime department and the Metropolitan Police's Central e-Crime Unit. The NCCU is responsible for leading the United Kingdom's law enforcement response to cybercrime. On a national level, Mr Archibald chairs the multiagency Cyber Threat Reduction Board, and internationally, he is the UK head of delegation for the G8 Law Enforcement Group and chair of the Strategic Alliance Cyber Crime Working Group.

Prior to the NCA's inception, Mr Archibald was a deputy director of SOCA, responsible for strategy and government relationships and, more recently, cyber and forensics.

Early in his career, Mr Archibald joined Lothian and Borders Police (1984), where he held a variety of uniformed and detective roles, particularly in the field of major crimes. He led complex investigations and covert operations, and as operational head of Special Branch (1999–2000), he led national operations.

Paul C Dwyer

Paul C Dwyer is an internationally recognized information security expert with over two decades of experience. He serves as president of the International Cyber Threat Task Force. Mr Dwyer has been certified an industry professional by the International Information Systems Security Certification Consortium and the ISACA and selected for the IT governance expert panel.

He has worked extensively around the world and trained with such organizations as the US Secret Service, Scotland Yard, the FBI and the National Counter Terrorism Security Office (MI5). He has been approved by the National Crime Faculty and is a member of the High Tech Crime Network.

Mr Dwyer has worked with clients in many sectors, including financial, government, telecommunications, pharmaceuticals and oil and gas.

Mr Dwyer is a leading authority on cybersecurity governance, risk and compliance (GRC) and provides advisory services to a number of organizations around the globe, including Fortune 500 companies, law enforcement and the military (NATO). He has presented on cyberthreats to the UK Defense Committee at Westminster. A prolific contributor to the industry and media, Mr Dwyer is an expert public speaker and has authored a number of cybersecurity GRC training courses for executives. Mr. Dwyer is now a leader in Mandiant.

Appendix 2: Participants

Members participating in all or parts of the meeting sit on the boards of 25 large-, mid- and small-capitalization public companies:

- Mr Aldo Cardoso, Audit Committee Chair, GDF SUEZ
- Mr Ángel Durández Audit Committee Chair, Repsol
- Mr Phil Hodkinson, Board Member, BT (alumnus)
- Mr Lou Hughes, Audit Committee Chair, ABB
- Dame DeAnne Julius, Audit Committee Chair, Roche
- Dr Maurizio Lauri, Audit Committee Chair, UniCredit
- Mr Pierre Rodocanachi, Audit Committee Member, Vivendi
- Ms Guylaine Saucier, Audit Committee Chair, AREVA
- Mr Jack Tai, Audit Committee Chair, Royal Philips

EY was represented in all or parts of the meeting by Mr Christian Mouillon, Global Risk Management Leader.

Appendix 3: Discussion questions for audit committees

- What kind of threats has your company faced recently? What aspects of the evolving environment are of most concern to you?
- How has your company's approach to defending itself changed in the last year or so? Is it doing anything differently?
- What has been your experience so far in working with government agencies on cybersecurity?
- What kind of assistance would you like from the government? What kind of help could your company provide to the government?
- How might the recent revelations about government spying affect trust in government efforts?
- Are you concerned about the possibility of more regulations in the area of cybersecurity, such as mandates to implement security measures?
- Has the board's oversight of cybersecurity evolved in any way? How is the board addressing the issue of expertise?
- How do the audit committee and the board oversee disclosures, including the compliance aspects and the strategic elements?