Audit Committee Leadership Summit

May 2018

ACLS VIEWPOINTS

Lessons from cyber-breach responses

Audit committee chairs and cybersecurity experts alike believe that for most companies cybersecurity breaches are inevitable. *"Everyone knows they might get hacked; all are preparing for some type of event. The attitude has shifted from prevention to protection,"* one audit chair said.[1] Cyber breaches typically carry a high financial cost for companies. In 2017, the average cost of a data breach was $3.62 million.[2] The cybersecurity industry is now a multibillion-dollar business—with experts estimating that nearly $655 billion will be spent on cybersecurity initiatives between 2015 and 2020—and cybercrime could cost businesses worldwide more than $6 trillion annually by 2021.[3] Given the high risk of cyberattacks and the potentially severe consequences, boards and audit committees are focused on ensuring that their companies are ready to respond to a cyber event when it happens.

On April 16, 2018, members of the North American and European Audit Committee Leadership Networks met in London to discuss cyber-breach response and disclosure with two guests: Adam Banks, CIO at Maersk, and Seth Berman, partner at Nutter McClennen & Fish.

Executive summary

This *ViewPoints* includes background information and synthesizes the perspectives that members shared before and during the meeting on the following topics:

- **Real-time responses to cyberattacks** (page 2)

  Cyberattacks vary widely, and the effects on an organization are never identical. In 2017, Maersk was the unintended victim of the NotPetya ransomware attack. It was a massive, costly breach that stripped the company of its global systems. Mr. Banks explained to members how the company assessed the damage, executed its recovery, and communicated with internal and external stakeholders. As with Maersk, any company that is involved in a cybersecurity crisis faces the challenge of responding quickly, thoroughly, and transparently.

- **Cyber preparedness and lessons learned** (page 7)

  After an attack, both victims and observers are wise to assess how the affected companies responded and, as necessary, how they should revise their approach to both cyber-breach planning and broader risk management efforts. A change from prevention-focused thinking to a mindset of detection is critical in today's cyber-risk environment. Companies' preparedness should go beyond basic hygiene to include a broader understanding of

potential threats to the business. The board can play an important role in providing oversight of the company's preparedness.

Real-time responses to cyberattacks

A recent report noted that 1,579 breaches occurred in the United States in 2017, a nearly 45% increase over the already record-high number reported in 2016.[4] These data breaches represent the exposure of over 178 million records across business sectors, financial institutions, and government. How a company responds is critical in reducing collateral damage. *"The biggest challenge is knowing how to respond to an attack,"* said Mr. Berman, *"There is often more damage in a botched response than in the breach itself."*

An important aspect of the initial response is understanding three key factors of the attack:

- **Who are the attackers?** The types of attackers vary depending on the organization under attack. A Verizon study of more than 53,000 security incidents, including more than 2,000 confirmed breaches, occurring in 2017 found that 73% of attacks involved external perpetrators, with 50% of breaches carried out by organized criminal groups and 12% by nation-state or state-affiliated actors; notably, 28% of attacks involved insiders.[5] Failure to properly identify the attacker can delay an appropriate response, sometimes for an extended period. Mr. Berman described a case in which a firm believed that an insider was responsible because the attacker knew the company's systems so well. In reality, it was state-sponsored attackers who had been operating within the company's systems for a year without detection.
- **What are they trying to accomplish?** In the case of malware, the goal of the attack is often to claim a ransom fee to be paid by the victim, while in other cases, the attackers want data.[6] The spectrum is broad, Mr. Berman emphasized: *"There is a big difference in types of attackers and their motivations, between a nation-state trying to shut a company down, criminals trying to get customer information, or someone trying to steal a company's IP [internet protocol address] or data."*
- **How are they doing it?** As the types of attackers and their motives vary, so do their methods. A 2017 European Union Agency for Network and Information Security report identified numerous types of threats in today's environment, including malware, web application attacks, insider threat, data breaches, and cyber espionage, among others.[7] When possible, identifying the root cause helps the company to understand the attacker's objective, determine the impact of the event, and reduce the likelihood of reoccurring issues.[8]

The NotPetya attack on Maersk

In June 2017, Mr. Banks received an unexpected call indicating that Maersk's global monitoring systems could not detect its global IT network. He described the moment he learned about the attack: *"Immediately my phone was flooded with calls from throughout the*

company, but then the calls stopped because our phone systems ran over the network and had therefore failed. Within seven minutes, 50,000 machines were infected, and for six hours, we were in the dark about what had happened." With 99% of systems down by 6 p.m. of that day, Maersk plunged into a crisis.

Maersk's leadership soon learned that the company was the unintended victim of a nation-state attack that migrated into their systems by way of a software update to the online portal for the Ukrainian tax authorities. This malware attack affected many global organizations and is estimated to have cost organizations globally $1.2 billion in combined quarterly and yearly revenue. The cost to Maersk was close to $300 million.[9]

Key elements of Maersk's response

Maersk's leadership responded quickly and thoroughly to the attack. Mr. Banks drew on his experience in the financial services industry to deal with this level of crisis. In the meeting, he described several aspects of the company's response that led to a successful recovery:

- **Communicating transparently with internal and external stakeholders.** Both internal and external communications were essential elements of the company's response. With nearly all internal systems down, including communications, the executive team temporarily used WhatsApp's safeguarded platform. *"Management formed a group and then created cascading reporting groups across the organization, enabling teams to communicate,"* said Mr. Banks. Maersk sent daily updates on port operations, and Mr. Banks even created video messages twice daily to update staff on progress. As the crisis progressed, other executives also provided updates.[10,11] *"We decided to be transparent from the get-go. In hindsight, we didn't have a choice. That was transparency with both customers and internal stakeholders. It was a wise choice by the CEO."* In addition, he noted the challenge of communicating with multiple law-enforcement agencies during a breach that spanned operations in dozens of countries: *"It would have been a nightmare to interact with 165 different agencies. Instead, we interacted primarily with Dutch and UK authorities, while also communicating with several others because there was no cross-border communication between law enforcement."*
- **Prioritizing recovery activities.** At the beginning of the crisis, Maersk's executive team met every six hours to discuss their progress. *"The first three days were spent rebuilding technical capabilities, then rebuilding operational capabilities. We then had to prioritize bringing services back online across the large organization. There were no real turf wars, because there was the shared understanding that getting the IT priorities were primary and others had to come secondary,"* said Mr. Banks. In addition, the executive team and the board gave Mr. Banks the needed decision-making power to act with agility, without complex approval processes.
- **Ensuring business continuity.** While technical teams worked around the clock to restore Maersk's systems, the physical business itself reverted to pre-digital processes: *"We had to*

go back to a 1960s-era booking process. We had some booking data available, and people working at ports had to do physical inspections. About 10% of cases were wrong, so we were able to operate manually at 90% accuracy."

- **Relying on the broader business community, even competitors.** In the crisis, Maersk's leadership knew that it would need help from its network of partners and competitors. "We were never alone, so many hands helped in this recovery. From the very first days, we got phone calls all over Maersk from people who wanted to fly in and help, also from technology partners and other companies. Everyone pitched in," said Mr. Banks in an interview.[12] During the meeting, he said, *"Our networks were consumed by our response. We asked IBM, Microsoft, and others to help. Surprisingly, one of our largest competitors, who is also a key customer, offered office space for our employees to work. It was a risk, but they helped us."*
- **Enlisting skilled talent.** This unprecedented crisis starved global organizations of the talent needed to recover quickly. Cryptographic and forensic specialists were in very short supply, as were other engineers: *"In terms of resources, we peaked at about three thousand additional people, because we needed specific skills like cloud engineers. The world ran out of them for two weeks. Consultants, Microsoft—no one had them. So we appealed to other companies and borrowed expertise. That enabled us to bring the systems back as quickly as we did."*

The board's role during the attack

During the crisis, the board met twice with Mr. Banks and received regular updates from the CEO. *"The board did not interfere with management's work by asking for specific information. If management had to respond to individual board members or committees, it would have taken us away from addressing the crisis at hand,"* Mr. Banks said.

The board did advise management on communications and key decisions; however, it allowed the CEO and CIO to own external communication, so as not to create confusion or deviations from the message from the top.

Lessons from other breaches

Most cyberattacks do not play out like NotPetya did at Maersk. Members and guests discussed some additional considerations for boards:

- **Timing of response can vary.** Mr. Berman highlighted that other types of cyber breaches can have timelines that can vary dramatically from the malware attack on Maersk. *"Most breach responses happen gradually, where there's a period of time between when the breach is initially detected by lower level employees and when it's recognized as a crisis,"* said Mr. Berman.

- **An attacked company might not be viewed as a victim.** Even when under attack, the public might not see the company as a victim. Mr. Berman noted that for many companies, their response can be described psychologically: *"When you've been attacked, you rightly think of your company as the victim. But others will see your company as the bad guy."* Because of this public perception, transparent communication can prove difficult for some companies. He said, *"Often, companies don't know how bad the situation really is and don't know if it affects all or some customers. This makes it harder to be radically open about what's going on, because you simply don't know."*
- **Ransom demands should not be taken lightly.** Members discussed how companies respond if hackers demand ransom payments. These decisions can be complicated because making a payment to a hacker does not always resolve the situation. In the case of Maersk, the company did not pay the demanded ransom. However, Mr. Berman noted, *"Most people do pay—but most attacks are less comprehensive and the amount requested is far less. It would be better if no one paid these attackers, but for some, it is a cheaper fix. NotPetya was quite different and not an easy situation to be in."*

Breach notification regulation in Europe and the United States

Global businesses are experiencing increased pressure from regulators to disclose information about cyber breaches faster and more frequently. Mr. Berman highlighted the benefit of new regulatory measures: *"Ultimately, this transparency will help everyone understand better how these attacks are happening and how to improve security."*

The General Data Protection Regulation (GDPR) becomes law in all EU member states on May 25, 2018; it protects the personal data of European citizens, regardless of where or by whom the data is held.[13] As a result, it applies to nearly all multinational corporations, whether headquartered in the EU or not.

The GDPR requires businesses to fundamentally change their approach to breach notification. It imposes a 72-hour mandatory breach-notification requirement in cases where a breach is likely to "result in a risk for the rights and freedoms of individuals."[14] Companies must inform both customers and relevant authorities in the event of a breach. Violations come with heavy maximum penalties: as much as 4% of the firm's annual global revenue or €20 million, whichever is higher.

In the United States, breach notification requirements have not been legislated at the federal level; however, laws protecting consumer data privacy exist at the state level in every state. Many states have adopted their own laws based on a 2003 California statute that required mandatory notification of a security breach if personal data was compromised. While many of these state laws are similar, they often have different thresholds for when a company must make a disclosure and what must be disclosed.

A major cybersecurity event—especially one that is mishandled—can also harm shareholder value. As a result, market regulators, like the Securities and Exchange Commission (SEC) and the European Securities and Markets Authority, provide guidance for how companies should disclose cyber events to ensure that they maintain investor confidence. In February 2018, the SEC issued further guidance on cybersecurity disclosures, building on the positions its staff issued in 2011.[15, 16] While this interpretative guidance does not represent a significant change to prior staff disclosure guidance, it does present an opportunity for companies to review their current disclosure practices.

Cyber preparedness and lessons learned

According to the National Institute of Standards and Technology, organizations can minimize the impact of a breach "by taking resiliency into consideration throughout the enterprise security life cycle, everything from planning technology acquisitions … and developing procedures to executing recovery and restoration efforts."[17] During the meeting, guests and members considered how lessons from past events translated into actionable ways to prepare for future attacks.

Post-crisis reviews provide critical insight

In pre-meeting discussions, members emphasized the importance of learning from a major breach, either at their own company or a competitor's: *"When breaches happen periodically, you want to ask what we learned from the last event."* Members said that conducting a post-breach evaluation of management's response and giving feedback are important tasks for the board. While exercises provide strong learning opportunities, one member said, *"There is no better instruction than having a breach happen in real life."*

Once Maersk reached a significant point in its recovery, the board executed a detailed review of the company's response. Together, management and the board determined that certain aspects were insufficient, and they initiated a range of changes.

The attack caused Maersk to reimagine its biggest risks. Before the attack, the company's disaster scenarios involved the sinking of one of its largest vessels, explained Mr. Banks. The company did not think to ask, What if all our vessels "disappear"? Mr. Banks said, *"I learned that the attitude to data in asset-based companies is so different. In the financial services sector, data is at the core of the business; however, in asset-based business, data oils the assets, making it efficient and well running. It's very difficult to reverse that thinking."*

Mr. Banks emphasized Maersk's shift to focus on resiliency and recovery: *"We have changed the way we protect ourselves. Now, the ruling assumption is that bad actors are already in our systems."* Members acknowledged the need to consider a broader threat landscape in light of the potential actors who can do harm to their companies. In the aftermath of the attack, Maersk has significantly increased its focus on monitoring the behavior of people and devices, detecting abnormalities, and isolating suspicious actors. *"Nation-state attacks will usually succeed. We expect that we will be attacked, and we need to respond rapidly. We start from the position that, to nation-state attacks, we are insecure, so no device can be trusted and must be monitored,"* Mr. Banks said.

Basic data hygiene is crucial, but is not enough

Members discussed the importance of having effective information technology policies regarding administration rights and system structures. While mundane topics, management's fluency in these areas can give the board a better sense of the company's preparedness.

"The board should ask about hygiene management, such as progress on patching software with the latest updates. Small, medium, large companies all have this issue, and while there are reasons for not getting around to making these updates, it's a huge factor to consider," said a member. Mr. Banks agreed but emphasized the imperative of going beyond routine maintenance: *"Hygiene is important, but it's not enough. Companies should do more. Simply patching is like brushing your teeth but never going to the dentist."*

Exercises and testing provide essential feedback

Experts note that practicing a breach-recovery plan increases the chances for success in the event of an actual breach.[18] Several member companies test cyber-breach readiness through tabletop exercises or *"war games,"* as one member noted. These often involve key senior leaders from across the organization coming together for hours-long, closed-door meetings, where they are challenged by realistic attack scenarios.

One member described an example of this practice. Executive leadership, including the chief financial officer, chief information officer, general counsel, chief digital officer, regional presidents, and the leaders of human resources, internal audit, risk, and communications, convene an incident-management team that runs scenarios every three months. *"Led by risk and internal audit, our security team simulates an incident. The group is confronted constantly with new information, and the teams make decisions and respond in real time. We record the simulations and even exercise having the media arrive on the scene. You forget that it's a simulation because it's so lifelike,"* the member said.

Some members described using external advisers to develop and exercise their plan. Paul Van Kessel, EY's global advisory cybersecurity leader, said, *"Organizations often do not know what to do. Through simulations, our team helps to clarify this process by running exercises with the executive team and board. We then review the simulation to see how people worked through the crisis from a communication, forensic, and legal perspective."*

Penetration testing also provides insight into a system's vulnerabilities. While rebuilding their systems, Maersk utilized red and blue teams to test the new infrastructure; however, the 1,500 attacks attempted each week provide ample testing, lessening the need to run penetration tests, remarked Mr. Banks.

Crisis-communication planning helps companies to respond swiftly

An EY survey found that over 43% of business leaders did not have a communications plan in place in the event of a significant cyber attack.[19] Experts offer the following recommendations for devising a cybersecurity crisis-response framework:[20]

- **Create a cross-functional communication team**, involving key players from across the organization.
- **Establish a clear leadership structure** with a well-defined communication tree.

- **Develop blueprints** for responding to a variety of cyber-attack scenarios.
- **Respond quickly**, with communication platforms—like a dedicated website and two-way channels for stakeholders to ask questions—ready to go.
- **Review the plan continually,** viewing it as a perpetual work in progress and updating it regularly to reflect emerging new threats.

The board provides helpful response-preparedness oversight

Members and guests shared several tactics for boards and audit committees for helping management to prepare for future attacks:

- **Ask detailed questions and dig deep.** Mr. Berman recommended that boards begin with high-level questions and then dig deeper into the details of the organization's cyber-response planning: *"Ask, What testing are we doing? What happens when we do tabletop exercises? How are executive leaders approaching the problem? What scenarios were used? What has been learned? How do they plan on improving?"* One member emphasized the importance of asking both *what* the company is doing to prepare and *how* the plan would be executed.
- **Recognize technical knowledge gaps on the board.** Some members were concerned that boards still lack the skill and knowledge to adequately test management's capability to respond to a cyber attack. One said, *"There is a lack of skill in this area on boards. We have specialists for sector and finance, but we do not have the right people who are able to ask the right questions. We often do not have the right level, the right executive skills to ask the right questions."* Another member said, *"To better understand the issues, I am getting educated on the technical aspects of the company, including system structures and administrative rights; these are practical, concrete issues. There are a number of ways to practically prepare as a board member, not just ticking the enterprise risk management boxes."*
- **Create a specialized technology committee.** Several members noted that their boards have created a separate technology-focused committee to handle both the risks and opportunities in this environment.

Conclusion

Cyberattacks, in some form, are inevitable for most companies. While the case of Maersk's response to NotPetya was unique, it demonstrates the importance of a coordinated response and provides many lessons for boards to consider. As audit chairs, ACLN and EACLN members noted the importance of comprehensive cybersecurity oversight that includes an increased focus on cyber breach response.

About this document

The European Audit Committee Leadership Network (EACLN) and Audit Committee Leadership Network (ACLN) are groups of audit committee chairs drawn from leading North American and 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.

Appendix 1: Participants

EACLN and ACLN members participating in all or part of the meeting sit on the boards of over 40 public companies:

Ron Allen, Coca-Cola Company

Mike Ashley, Barclays

Werner Brandt, Siemens

Julie Brown, Roche

Aldo Cardoso, ENGIE

Mary Anne Citrino, HP Inc.

Carlos Colomer, Abertis

Pam Daley, BlackRock

Dave Dillon, 3M and Union Pacific

Carolyn Dittmeier, Generali

Ángel Durández, Repsol

Eric Elzvik, Ericsson

Edgar Ernst, TUI

Renato Fassbind, Nestlé and Swiss Re

Byron Grote, Tesco, Akzo Nobel, and Anglo American

Siân Herbert-Jones, Air Liquide

Liz Hewitt, Novo Nordisk

Jean-Marc Huet, Heineken

Lou Hughes, ABB

Arne Karlsson, Mærsk

Dagmar Kollmann, Deutsche Telekom

Mike Losh, Aon

Richard Meddings, Deutsche Bank

Nasser Munjee, Tata Motors

Chuck Noski, Microsoft

Appendix 1: Participants, continued

John Rishton, Unilever

Guylaine Saucier, Wendel

Erhard Schipporeit, SAP and RWE

Jim Turley, Citigroup

Steve West, Cisco Systems

Maggie Wilderotter, Hewlett Packard Enterprise

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

- Andy Baldwin, EMEIA Area Managing Partner
- Jean-Yves Jégourel, EMEIA Assurance Leader
- Frank Mahoney, Americas Vice Chair of Assurance Services

Appendix 2: Discussion questions for audit committees

? What common diagnostic procedures do your companies use to investigate cyber breaches?

? Are there particular response frameworks your companies use?

? What external advisers are aiding your companies through the post-breach process?

? As the May 2018 deadline for GDPR implementation approaches, how are your companies preparing?

? How will your companies respond to the SEC's new interpretive guidance on cybersecurity disclosures and controls? What steps is your audit committee taking?

? What good practices have your companies established for communicating cyber breaches to stakeholders, including authorities, customers, business partners and the public?

Endnotes

[1] *ViewPoints* reflects the network's use of a modified version of the Chatham House Rule whereby comments are not attributed to individuals or corporations. Quotations in italics are drawn directly from conversations with network members, guests, and other experts in connection with the meeting.

[2] Ponemon Institute, *2017 Cost of Data Breach Study: Global Overview* (Traverse City, MI: Ponemon Institute, 2017), 1.

[3] Steve Morgan, "Cybersecurity Market Report," Cybersecurity Ventures, May 31, 2017.

[4] Identity Theft Resource Center, *2017 Annual Data Breach Year-End Review* (Identity Theft Resource Center, 2018), 3.

[5] Verizon, *2018 Data Breach Investigations Report*, Executive Summary (Verizon, 2018), 2.

[6] Michael Bartock et al., *Guide for Cybersecurity Event Recovery* (Gaithersburg, MD: National Institute of Standards and Technology, December 2016).

[7] European Union Agency for Network and Information Security, *ENISA Threat Landscape Report 2017: 15 Top Cyber-Threats and Trends* (Athens, Greece: ENISA, 2018).

[8] Bartock et al., *Guide for Cybersecurity Event Recovery,* 10-11.

[9] Fred O'Connor, NotPetya Still Roils Company's Finances, Costing Organizations $1.2 Billion in Revenue, Cyberreason blog, November 9, 2017.

[10] Richard Milne, "Maersk CEO Soren Skou on Surviving a Cyber Attack," *Financial Times*, August 13, 2017.

[11] John Churchill, "When the Screens Went Black," Maersk, September 14, 2017.

[12] John Churchill, "When the Screens Went Black," Maersk, September 14, 2017.

[13] See "EU General Data Protection Regulation: Are You Ready?" *EY Law* (blog), April 20, 2016; Kevin Townsend, "New EU General Data Protection Regulation Affects Multinational Companies," *SecurityWeek*, April 15, 2016.

[14] "GDPR Key Changes," EU GDPR Portal, accessed March 21, 2018.

[15] Securities and Exchange Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. 8166 (February 2018).

[16] EY, *SEC Reporting Update: SEC Issues Guidance on Cybersecurity* (EY, February 22, 2018).

[17] Bartock et al., *Guide for Cybersecurity Event Recovery*, 4.

[18] Ben DiPietro, "An Effective Cyber Breach Response Requires Practice," *Wall Street Journal*, November 3, 2017.

[19] EY, *Cybersecurity Regained: Preparing to Face Cyber Attacks,* 20.

[20] MIT Technology Review Insights, "Crisis Communication After an Attack," *MIT Technology Review,* April 20, 2016.