European Audit Committee Leadership Network

July 2021

EACLN

VIEWPOINTS

Ransomware and cyber-incident response

Recent months have seen a surge of ransomware attacks, in which attackers extort money from organizations by making critical data inaccessible and/or threatening to expose it. The attacks against Colonial Pipeline, the Irish healthcare system, and AXA, among others, demonstrated the gravity of the threat, prompting a renewed focus on cybersecurity by both government authorities and private-sector organizations. Since experts believe that ransomware breaches are inevitable, even for companies with sophisticated strategies to prevent them, minimizing the impact of these attacks must address a range of issues: Should the ransom be paid or not? How can that decision be made and implemented responsibly and effectively? What should be communicated to investors, regulators, and other stakeholders? How should the board be involved?

On June 3, members of the European Audit Committee Leadership Network (EACLN) met virtually to discuss the challenges of responding to ransomware attacks with two guest experts: Mike Maddison, EY EMEIA consulting cybersecurity leader, and Phyllis Sumner, partner and chief privacy officer at the law firm of King & Spalding. *For biographies of the guests, see Appendix 1, on page 9, and for a list of network members and other participants, see Appendix 2, on page 11.*

Executive summary

The discussion focused on the evolving ransomware threat and key preparations that companies and boards can undertake to improve their response to attacks:

- **The surge in ransomware attacks** *(page 2)*

  A recent wave of ransomware attacks has underscored the scale of the threat, prompting increased attention from both government and private-sector groups. Yet the guest experts noted that an "ecosystem" of cybercrime has been growing for years, enabled by advances in tools and techniques, the emergence of hard-to-trace digital currencies, and the continued digitalization of every large business. They warned about double-pronged attacks in which perpetrators not only prevent access to critical data but also threaten to divulge it publicly.

- **Elements of an effective ransomware response plan** *(page 3)*

  Guests and members highlighted the unique challenges of ransomware attacks, in which companies must consider whether and how to engage with their attackers. While some companies adopt a policy of not paying ransoms, many include provisions for payments in their response plans. These should include thorough due diligence regarding the legality of payments, as well as arrangements for outside advisers to assist with the process.

Disclosures to stakeholders must also be carefully weighed, but guests and members saw a shift to greater speed and transparency in divulging information about attacks.

- **Testing the response plans** *(page 5)*

  Both guests emphasized the importance of testing response plans; testing can bring to light a variety of problems, such as insufficient communication or coordination among different functions within the organization. Live-fire drills, in which an outside party is hired to launch an attack against the company, reveal how quickly the company can detect an attack and begin responding and engaging with all the relevant stakeholders.

- **The board's role** *(page 6)*

  The role that boards play in responding to ransomware attacks is evolving, with some boards playing a greater role than others. The significance of some attacks, members noted, would clearly require board involvement. Yet members also acknowledged that discussions of ransomware—and cybersecurity more generally—are often challenging for boards. To improve their understanding of the issues involved, boards are seeking outside advice as well as recruiting more boardroom cyber experts.

For a list of discussion questions for audit committees, see Appendix 3, on page 12.

The surge in ransomware attacks

The EACLN meeting took place as a wave of ransomware attacks were wreaking havoc in industries from energy to healthcare to food. In the weeks before the meeting, ransomware criminals shut down a pipeline supplying almost half the fuel for the US East Coast,[1] shortly after which another attack compromised Ireland's healthcare system.[2] Acknowledging that the pandemic created new vulnerabilities for attackers to exploit, guests noted that the growth in such attacks had been predicted long before. Advances in tools and techniques, the emergence of digital currencies that are hard to trace, and the unending digitalization of businesses have created favorable conditions for a global cybercrime industry in which different kinds of players often work together on attacks. Mr. Maddison said, *"Attackers do not need to be geniuses; they can download tools to launch these attacks. There is also a marketplace for this: ransomware as a service. There is a whole ecosystem."*

The notion of an "ecosystem" of cybercrime has been put forth by other security experts as well. In its 2021 Global Threat Report, the cybersecurity firm CrowdStrike describes an evolving "eCrime ecosystem"—an "active and diffuse economy of financially motivated entities that engage in myriad criminal activities in order to generate revenue."[3] These groups, some specializing in specific attack modes, can work together; for example, "access brokers" gain access to specific targets, which they sell to operators who carry out the attacks, and other players offer malware as a service.

Ms. Sumner described the situation as dire: *"The level of sophistication is going up, and the damage is too. Threat actors are capable of accessing everything, including backups."* She pointed to the double-pronged nature of the threat, in which attackers not only render data inaccessible but also threaten to divulge it, should a first threat fail to yield results. *"There's the*

double threat of dwelling in the environment, stealing data, and then deploying malware to encrypt it. That double threat puts more pressure on organizations to pay the ransom."

Divulging data is facilitated by the establishment of "dedicated leak sites," where data is made public. Data may be released in batches to ratchet up pressure on organizations. In June 2020, several ransomware operators formed a cartel to share data on their leak sites so that they could reach a wider audience.[4] According to security researcher DarkTracer, 2,103 companies have seen their data exposed on data-leak sites since 2019.[5]

For law-enforcement authorities, battling this ecosystem of crime is an ongoing struggle. As criminals exploit new technologies and develop new techniques of attack, government agencies try to match them. The US Federal Bureau of Investigation scored a major success against the attackers that crippled Colonial Pipeline, successfully tracing the Bitcoin ransom payment and retrieving a large share of it; however, experts pointed out that tracing digital currencies remains difficult, and outcomes will vary depending on circumstances.[6] The business model of ransomware remains intact, and criminal groups are developing payment schemes that are even harder to trace than Bitcoin. *"As long as companies pay ransoms and threat actors earn millions, the attacks will keep coming,"* Ms. Sumner noted. Mr. Maddison highlighted the sheer scale of the recent surge and the escalating payments demanded by attackers. The cybersecurity firm Emsisoft estimates that in 2020 ransomware gangs earned $18 billion in ransoms.[7]

Elements of an effective ransomware response plan

An effective response to ransomware that has breached company defenses will depend on preparations made ahead of time, especially an enterprise-wide incident response plan. What elements should be included in such a plan? Ransomware presents challenges that are different from other types of cyberattacks, most notably because the company may wish to engage with the perpetrators. Guests and members focused their discussion on a few key aspects of response plans, including policies on ransom payments, outside advisers, and disclosure.

The decision on ransom payment

One critical question during a ransomware attack is whether the ransom should be paid. Some companies establish policies against paying a ransom as part of their incident response plan, a stance that Ms. Sumner believes governments will increasingly encourage. Payments incentivize future attacks and may not yield the promised results. *"Organizations are making no-pay policies public,"* Ms. Sumner noted, *"because they want payment to be seen as not an option."* She recounted the story of a company that did pay: *"It still took them six weeks to get operational. But between the pandemic and the operational difficulties, they didn't make it. It just underscores that payment is not always an answer."*

Yet there are situations, such as when lives are at stake, when companies may believe they have little choice but to pay and hope for the best. *"It's incredibly difficult to have a policy,"* a member said, *"because each situation can be very different."* A response plan may need to be

nuanced about whether or not to pay, spelling out potential contingencies that include specific provisions for a range of scenarios.

Ms. Sumner acknowledged that provisions for handling ransom demands should be part of the response plan. *"There is a trend to add more detail around how to handle ransom demands in incident response plans and legal playbooks,"* she said, adding that *"a significant amount of due diligence needs to take place before any ransom payment is made."* There could be sanctions on paying certain groups, and insurance companies may only cover the ransom if the proper diligence has been completed: *"You are going to have to prove that you have taken significant steps to mitigate the possibility that you are paying terrorists."* Pressure will come from the intermediaries who facilitate payment as well as governments and insurance companies. *"If the threat actor who is paid is on the sanctions list, the authorities will not only go after the company but also pursue intermediaries who facilitated the payment,"* Ms. Sumner noted.

She also said that provisions for ransom payment needed to be *"very tightly held"* rather than shared, even within the company. Companies should be very careful with that information, she explained: *"The mere fact that an organization has such a playbook, including how they would pay, demonstrates that they might pay under certain circumstances. You would not want that to be public."*

Provisions for outside advisers

When paying ransom is on the table, companies face the unusual challenge of having to interact with criminals. Both Ms. Sumner and Mr. Maddison recommended using outside advisers and intermediaries who are experts in communicating and negotiating with attackers. *"The complexity of dealing with these attacks means that having these people on call is fundamentally important,"* Mr. Maddison said. Both guests underscored the importance of approving these advisers in advance and potentially arranging for retainers. *"I can tell you that they are in hot demand,"* Ms. Sumner warned.

Managing outside advisers is itself a challenge. A member noted that their companies *"prefer to have a law firm deal with third parties and specialists,"* and Ms. Sumner endorsed that approach: *"It's really important that it be directed by lawyers. There should be very specific statements of work to engage vendors just for that project. Otherwise, it's very difficult to maintain privilege and confidentiality."*

A member asked about the role of law-enforcement agencies in assisting with the response. Ms. Sumner said, *"You can get very helpful information from them. That said, you should structure the communications with law enforcement to maintain privilege and minimize disruptions when you are in the middle of a crisis."* She recommended that lawyers manage those discussions. She also noted that working with authorities might be part of the message a company sends about how it is responding, so a company may want to report the incident to law enforcement very quickly.

Disclosure decisions

Ms. Sumner also brought up broader issues around disclosures. Companies have often kept ransomware attacks—and whether the ransom was paid—secret from the public, for fear of encouraging further attacks or suffering reputational damage. The need to ascertain the facts around an incident more clearly might also motivate more limited communications. However, Ms. Sumner said, a shift in approach might be underway, entailing *"a speedier response to external stakeholders."* She pointed to a recent directive from the US Department of Homeland Security that requires pipeline operators to notify the department when they are targeted by cyberattacks,[8] and she mentioned changes in third-party contracting that include requirements to quickly tell business partners about incidents.

Members brought up their own experiences with disclosures. *"We obviously communicated with the regulator, but we had a lot of discussion on whether we should issue a press release. Two days after the breach, we did issue a press release. We didn't have orders to do it, but people were calling us, and we just decided to do it,"* one said. Another member's company had also made an attack public, concluding in a postmortem that it was the right thing to do: *"The company had a chance to tell the story to customers first."* The member had also noticed a broader shift in disclosure practices: *"We see, more and more, a trend to make incidents public immediately."*

Testing the response plan

During the meeting, guests and members highlighted the importance of testing the incident response plan. Mr. Maddison said, *"One thing we don't see enough of is testing, not just in your own environment but in your ecosystem, your supply chain."*

Mr. Maddison outlined the benefits of different types of testing, including live-fire drills in which an outside party is hired to launch an attack against the company. Such testing reveals how quickly the company can detect an attack and begin responding: *"By having those live-fire events, you can understand your mitigation plans better, your ability to detect [an attack] quickly. Live-fire tests pick up incidents that trigger decision processes. How do you engage with all stakeholders in the organization? That is really important."* He mentioned a simulation that he had helped a client conduct, which revealed that certain functions critical to an effective response had been taken out during a cost-cutting effort.

Ms. Sumner also endorsed testing: *"Exercises are critical—some companies have been hotly criticized for not gaming their worst-case scenarios."* She noted that such exercises can bring to light a variety of problems with the response plan, such as insufficient communication and too much (or too little) detail in its provisions. Coordination is key in a ransomware response and should be tested ahead of time, Ms. Sumner explained in a premeeting conversation: *"Ransomware often crosses into more than one response plan, such as plans addressing crises, business continuity, cybersecurity incidence response, and communications. That can create confusion, and it underscores the importance of tying all these plans together. One recent tabletop exercise for a client revealed that it was unclear which plan applied and that some of the plans were inconsistent with each other. Unfortunately, such siloed and uncoordinated plans are common."*

Some members had seen the pitfalls of untested response plans. One member said, *"Management told us later that although they had been confident it was a good plan, it was not detailed enough to help them go quickly through the whole process."* Speed is of the essence. A breach must be detected and acted upon as quickly as possible, a member explained: *"What saved us was that we had someone watching the system 24/7, and this person could shut down all the systems right away. If this person had not had that authority, we might not have been able to restore our data. You have to shut down within 10–15 minutes. The attacker was starting to get into the backups."*

The board's role

The role of boards in responding to cybersecurity incidents is evolving, with some boards playing a greater role than others. Serious incidents clearly require board involvement, EACLN members said. An operational shutdown may be catastrophic, not only for the company but for customers, suppliers, and other stakeholders. *"Something that significant would come to the board, not only because of the financial impact but also because of other stakeholder impacts,"* a member noted in a premeeting conversation.

However, members also acknowledged that cybersecurity issues can be a challenge for many board members. Describing his experience as an executive, a member said, *"What I noticed was that within 15 minutes it became a discussion between subject matter experts. For generalists like me, it was all I could do to keep up. It's a challenge to understand digital considerations, and the board is one step removed."* Other members echoed the point. *"After the first few minutes, it became far too technical for me,"* one said, and another added, *"It's usually too fast moving for the board."*

In the wake of incidents that caught their companies flat-footed, members lamented their failure to anticipate and prepare. *"What kind of questions should we have asked? What was missing? We spent an hour on this issue, asking lots of questions and feeling comfortable. I missed something, but I don't know what,"* a member said, adding, *"How do you challenge controls around cyber? I always feel inadequate."*

One response to the problem is to bring in advisers. At the meeting, a member described an intensifying focus on cybersecurity at his board, which included more frequent interactions with management and bringing in a cybersecurity firm to advise both the audit committee and management. Another response is to recruit cyber experts to the board. *"You should have someone on the board who is able to ask the right questions on cyber,"* a member noted. Some members had already seen this, including one who said, *"An emerging trend is that some boards are appointing IT experts to boards."* But this member also spotted problems: *"Boards want an expert, but the problem is that the rest of the board takes a back seat on the issue. It takes the pressure off. Also, every board has a limited number of seats, so if that's all that an expert brings, they are dragging down the overall competency of the board."*

Other practices that boards might consider include the following:[9]

- **Clarifying what kinds of incidents should come to the board.** While serious incidents require board involvement, there are many incidents that boards do not need to know

about. In general, directors prefer to be informed, but they also prefer not to be overburdened, and they want to avoid distracting management by insisting on briefings that may not be necessary. In a premeeting conversation, an EACLN member said, *"Our philosophy is, in the heat of the moment, let the executives deal with the issue."* Clarifying the threshold for board involvement in ransomware attacks may be especially thorny, however, because of the complex ramifications of paying versus not paying.

- **Participating in the creation of the response plan.** While some directors have noted that the main concern of their boards is to ensure that response plans exist, others believe that directors could be more involved in developing them. Since companies need to be clear about the role of the board in an incident, Ms. Sumner said, board involvement in planning is important: *"Aligning expectations between management and the board is critical. If you don't work through the engagement model between them ahead of time, there will be a disconnect."*
- **Participating in response plan testing.** Though only a few EACLN members have reported board participation in tabletop exercises, some have pointed to the value of participating or at least learning about the results. In addition to clarifying the role of the board, involvement in testing gives directors the opportunity to provide fresh perspectives and learn what kinds of questions to ask when an incident occurs.

Conclusion

Ransomware crime presents some of the most challenging issues boards face today. Guests and members agreed that the surge in attacks and the constant evolution of tools and techniques create an environment that is fraught with danger and uncertainty. While boards may find the challenge especially difficult, top managers often struggle to explain matters clearly to the board. A member noted, *"No audit committee can be comfortable in this environment. I'm not saying management is not transparent, but still, we just don't know."* For management, the ransomware crime wave demands careful preparation, including development and testing of comprehensive incident response plans. For boards, it requires increased attention, including greater understanding of the threats and the company's efforts to prepare for them. *"We don't want to manage the company,"* a member said, *"but we need to know that these issues are being addressed."*

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, management, and advisers who become systematically engaged in this dialogue, the more value will be created for all.

Appendix 1: Biographies of guests

Mike Maddison is a partner and the leader of cybersecurity services for EY across Europe, Middle East, India, and Africa. He has almost 30 years of experience in the field of technology risk, cyber, and physical security. He has delivered significant transformation programs within end-user environments as well as developing cyber-risk mitigation strategies and appropriate organizational designs.

Before joining EY, Mr. Maddison was based in the Middle East, leading risk assurance services across the region for another big-four firm. These services included enterprise risk management, internal audit, cyber and information security, technology risk, and corporate governance as well as operational and finance controls assurance and consulting.

Prior to working in the Middle East, Mr. Maddison was based in London, with responsibility for all assurance and consulting services relating to cybersecurity, business resilience, testing and privacy in the UK and EMEA. He has regularly contributed to broadsheets as well as radio and television and industry publications. In addition, Mr. Maddison has spoken at conferences globally on the topic of cybersecurity and provided briefings at the highest level of government on security and intelligence issues. Before moving into management consultancy, Mr. Maddison held a number of senior risk roles in end-user environments.

Phyllis Sumner is a partner at the law firm of King & Spalding and the firm's chief privacy officer. She leads the data, privacy and security practice. Ms. Sumner regularly counsels corporate boards, senior executives, and other clients regarding data breach prevention, emergency response, remediation, compliance, regulatory enforcement, internal corporate investigations, and other critical privacy and data security concerns.

As a crisis manager, Ms. Sumner works closely with clients' legal, compliance, and business teams to strategize, manage, and defend when significant privacy and data security issues arise. She assists her clients with developing mature incident response plans and leads them through security incidents, including investigations, containment, remediation, communications, and contractual and legal obligations. She represents clients defending against class actions resulting from alleged consumer protection and privacy violations and data security incidents. In 2018 and 2016, Cybersecurity Docket named Ms. Sumner to its Incident Response 30, which lists "the 30 best and brightest Incident Response attorneys" in the United States, and Law360 named her Cybersecurity MVP in 2017 and Privacy MVP in 2016.

Ms. Sumner also represents clients in complex litigation involving the False Claims Act, RICO, the Fair Credit Reporting Act, and fraud. She is known for her negotiation and advocacy skills in and out of the courtroom. Law360 named her "Healthcare MVP" in 2014, and she has been a Georgia "Super Lawyer" since 2013. Atlanta Magazine named her a "Woman Making a Mark" in 2016, and the Daily Report named her a "Distinguished Leader" in 2017.

Previously, Ms. Sumner served as an assistant U.S. attorney in the Northern District of Illinois and the Northern District of Georgia. She successfully prosecuted high-profile cases such as Eric Rudolph and the Centennial Olympic Park bomber, as well as cases involving public corruption, domestic terrorism, credit card fraud, money laundering, healthcare fraud, and other complex criminal matters.

Appendix 2: Participants

The following members of the EACLN participated in part or all of the meeting:

- Werner Brandt, Siemens
- Julie Brown, Roche
- Alison Carnwath, BASF and Zurich Insurance
- Laurence Debroux, Novo Nordisk
- Carolyn Dittmeier, Assicurazioni Generali
- Eric Elzvik, Ericsson
- Margarete Haase, ING
- Liz Hewitt, National Grid
- René Hooft Graafland, Ahold Delhaize
- Dagmar Kollmann, Deutsche Telekom
- Pilar Lopez, Inditex
- Kalidas Madhavpeddi, Glencore
- John Maltby, Nordea
- David Meline, ABB
- Karyn Ovelmen, ArcelorMittal
- Stephen Pearce, BAE Systems
- Ana de Pro Gonzalo, STMicroelectronics
- Bernard Ramanantsoa, Orange
- Jon Erik Reinhardsen, Telenor Group
- Mariella Röhm-Kottmann, Zalando
- Guylaine Saucier, Wendel
- Erhard Schipporeit, RWE
- Gunnar Wiedenfels, SAP
- Martin Wittig, Kuehne + Nagel

The following members of the North American Audit Committee Leadership Network (ACLN) participated in part or all of the meeting:

- Pam Daley, BlackRock
- Dave Dillon, 3M and Union Pacific
- Bob Herz, Morgan Stanley
- Nick LePan, CIBC
- Leeny Oberg, Adobe
- Gerald Smith, Eaton

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

- Marie-Laure Delarue, EY Global Vice Chair, Assurance
- Jean-Yves Jégourel, EY Global Assurance Vice Chair, Professional Practice
- Julie Teigland, EY EMEIA Area Managing Partner

Appendix 3: Questions for audit committees

- ? Has your company been the target of a major cyberattack?
- ? What kinds of threats is your company most concerned about?
- ? How does your company monitor the evolving landscape of threats?
- ? Has your company ever been the target of a ransomware attack? How did it unfold?
- ? What kind of policies has your company established on ransomware? How has it approached the issue of payment?
- ? How have you prepared for the practical aspects of responding to a ransomware attack?
- ? What practices has your company implemented around incident response?
- ? How was your company's incident response plan developed and tested? What is included in the plan? How rigorous was the testing?
- ? What are important considerations and helpful practices as the response plan is activated during an actual attack?
- ? How does your board assist management in preparing for and responding to cybersecurity attacks? What kind of oversight does it exercise?
- ? What has your board—or its individual members—done to improve its ability to oversee incident response?
- ? How does the board approach the special challenges of ransomware?

Endnotes

[1] Myles McCormick et al., "Cyber Attack Sparks US Effort to Keep Fuel Lines Open," *Financial Times,* May 10, 2021.

[2] Laura Noonan, "Ireland's Healthcare System Taken Down After Ransomware Attack," *Financial Times,* May 14, 2021.

[3] CrowdStrike, *2021 Global Threat Report* (CrowdStrike, 2021), 6.

[4] CrowdStrike, *2021 Global Threat Report*, 23.

[5] Lawrence Abrams, "Ransomware Gangs Have Leaked the Stolen Data of 2,100 Companies So Far," *Bleeping Computer,* May 8, 2021.

[6] Evan Perez, Zachary Cohen and Alex Marquardt, "First on CNN: US Recovers Millions in Cryptocurrency Paid to Colonial Pipeline Ransomware Hackers," *CNN,* June 8, 2021.

[7] Hannah Murphy, "'It's a Battle, It's Warfare': Experts Seek to Defeat Ransomware Attackers," *Financial Times,* May 14, 2021.

[8] Rebecca Smith, "After Colonial Pipeline Hack, U.S. to Require Operators to Report Cyberattacks," *Wall Street Journal,* May 25, 2021.

[9] For more on this subject, see Cyber Risk Director Network, *Cyber Incident Response: The Board's Essential Role;* Audit Committee Leadership Summit, *Lessons from Cyber-Breach Responses;* Larry Jones, "The Board's Growing Cyber Imperative," *Corporate Board Member;* Bob Zukis, "Cybersecurity Board Reform Blows into Place for SolarWinds," *Forbes,* March 27, 2021.