Audit Committee Leadership Network

ACLN

VIEWPOINTS

Ransomware, incident response, and the board

Recent months have seen a surge of ransomware attacks, in which attackers extort substantial sums from organizations by making critical data inaccessible or threatening to expose it. The attacks against Colonial Pipeline, JBS, and Apple, among others, demonstrated the gravity of the threat and prompted 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 involves 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 28, members of the Audit Committee Leadership Network (ACLN) met virtually to discuss the challenges of ransomware and incident response with three guest experts: Orion Hindawi, CEO of Tanium, a cybersecurity software and services company; Chuck Seets, Americas assurance cybersecurity leader at EY; and Phyllis Sumner, partner and chief privacy officer at the law firm of King & Spalding. *For biographies of the guests, see Appendix 1 (page 8), and for a list of network members and other participants, see Appendix 2 (page 10).*

Executive summary

Several major themes emerged from the discussion:[1]

- **Cyber extortion now operates as a well-developed business** *(page 2)*

  The guests described a growing industry driven by high profitability and low risk for perpetrators, who can launch attacks against a wide array of targets from jurisdictions unlikely to prosecute. Cryptocurrencies have enhanced attackers' ability to stay anonymous, and ongoing technology deployment can distract companies from shoring up their cybersecurity defenses. At many companies, a lack of basic cybersecurity hygiene—measures such as patching systems and two-factor authentication—makes life easier for attackers.

- **Policies on ransom payments need to be flexible** *(page 3)*

  ACLN members agreed that flexibility on paying is preferable to strict policies against it. They pointed to the dire consequences of not paying, at least in certain cases. Ms. Sumner had seen companies refuse to pay and still recover successfully, but she said that savvy

attackers often ask for ransom sums low enough to make payment the easier option. Mr. Hindawi noted that paying is increasingly seen as a cost of doing business.

- **Preparations for responding are crucial** *(page 4)*

  Companies should take steps to facilitate their response to a ransomware attack, the experts urged. They should develop playbooks with trigger points for escalating the response and communicating with stakeholders. They should also line up third-party support in advance, including experts who can handle the negotiations with attackers, and third-party negotiators should be hired under privilege and put on retainer. Incident response plans should be integrated across an organization, including executives and the board, Ms. Sumner noted; Mr. Hindawi highlighted the importance of a clear chain of command. Guests and members also mentioned the importance of testing response plans, including red-team attacks conducted by ethical hackers.

- **Boards have an important role in preparations** *(page 6)*

  Boards cannot micromanage incident responses, but they can ensure that there is a framework in place to bridge the silos that exist in every organization. Ms. Sumner noted that the incident response plan, which may include a board engagement model, should lay out how and when the board will be involved. Given the complexity of the issues, both the members and guests stressed the importance of expert advice to the board. However, Mr. Hindawi noted that increasing board involvement during an actual incident may not be helpful. Where boards can really make a difference, he argued, is in promoting the cybersecurity hygiene that mitigates the impact of breaches or even prevents them in the first place.

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

Cyber extortion now operates as a well-developed business

The guests noted that cyber-enabled extortion has grown into a *"multibillion-dollar industry,"* an observation confirmed by multiple studies. The cybersecurity firm Emsisoft, for example, estimates that in 2020 ransomware gangs extracted at least $18 billion in ransoms globally.[2] Ms. Sumner remarked on how well organized ransomware threat actors have become, often resembling legitimate businesses in some respects: *"It reminds me of my prosecution of gangs in Chicago. They had a board of directors and a CEO. The business was drugs, but it was highly structured."*

The drivers of growth in the ransomware industry include high profitability and low risk for perpetrators, who can launch attacks against an ever-expanding array of targets from jurisdictions that are unlikely to prosecute cybercrime. *"The biggest factor is that the countries in which they are operating don't believe that it's in the country's interest to prosecute the people that are perpetrating these attacks. These attacks are not coming from countries friendly to the West,"* Mr. Hindawi explained.

Cryptocurrencies have enhanced attackers' ability to stay anonymous, and ongoing technology deployments can distract companies from shoring up their cybersecurity defenses. Mr. Seets explained, *"Every company on this call is deploying digital technology on a routine and ordinary basis. That expands the attack surface. It also distracts organizations from defending the fort. One of our clients was in the middle of an ERP [enterprise resource planning] system update and in the middle of that deployment, they got distracted; threat actors took advantage of that distraction and attacked."*

The technologies used in ransomware attacks are not particularly novel, as Mr. Hindawi explained: *"The thing that I think is most interesting about ransomware is how similar it actually is to many of the attacks that have been happening for the last 10 years. There's this mythology that ransomware is a completely distinct type of attack that we've never seen before."* Rather, ransomware attacks use well-known techniques such as phishing and exploiting software flaws to penetrate organizations' systems.

As a result, there are proven measures for defending against ransomware attacks and mitigating their impact. Unfortunately, they are still not being implemented as widely as they could be. At many companies, Mr. Hindawi pointed out, a lack of basic cybersecurity hygiene—measures such as patching systems and two-factor authentication—makes life easier for attackers. At the same time, he acknowledged that eliminating all vulnerabilities is difficult: *"There's a fallacy that if we just use encryption, we can keep all the data safe. Encryption only really works for data at rest. If you need access to that data on an ongoing basis, that data is actually available unencrypted at the time it is being used."*

Policies on ransom payments need to be flexible

Guests and ACLN members explored a critical question in every ransomware attack: Should the company pay the ransom? The initial inclination of most organizations might be to refuse, a stance often encouraged by law-enforcement authorities. Even contacting attackers is something many companies want to avoid: *"Do we engage with the threat actor at all? There are some risk factors in getting the attention of these groups and beginning discussions and negotiating,"* Ms. Sumner said. Concerns about reputation and incentivizing further attacks are among the reasons that companies refuse payments on principle.

Yet the reality is more complicated. Members described *"eye-opening experiences"* from which they concluded that *"you have to look at the situation"* rather than adhere to a strict policy against paying. A member pointed to the Colonial Pipeline attack: *"Philosophically, you can say, 'Heck no,' but when you know the East Coast is going to run out of gasoline in three to four days, the pragmatic side takes over."*

Several other members agreed. *"It used to be the case that the company would just say no. But now, because of the proliferation of attacks, there is a process that involves assembling a group of people and evaluating the situation—the pros and cons—before making a*

recommendation," one member said. Another added, *"We think we have a good cybersecurity system and everything in place, but if something like this happened to us, we would probably be paying."*

Mr. Hindawi acknowledged that paying might make sense, even if company data has been backed up: *"Rebuilding from backup could take weeks. The question is, Can you wait weeks? The answer is probably no. Backup and restore is a nice last resort."* Ms. Sumner said she has seen cases of companies not paying and still recovering successfully, but that savvy attackers often ask for ransom sums that are low enough to make payment the easier option. Mr. Hindawi noted that *"the stigma of paying is diminishing—it's becoming a cost of doing business."*

It may be beneficial to pay quickly, a member noted: *"If you ask the chief digital officers of these companies, they'll say, 'Pay immediately—you're not going to get a better offer.'"* Ms. Sumner agreed: *"I see companies that pay rapidly because it's impacting their operations and their first instinct is to pay immediately, and the threat actors know that if they come with a number that is not material, it makes the decision to pay easy."*

At the same time, Ms. Sumner noted, paying may not be an easy fix: *"We've also seen cases in which the threat actors don't follow through even after being paid, or they extort again. They provide enough to get the company going again, and then they ask for more money."* The recent attack on Colonial Pipeline was a case in point: the company paid the $4.4 million ransom, but the decryption tool it got in return was not effective, forcing the company to use system backups.[3]

Paying a ransom may also be illegal. Ms. Sumner explained, *"Whenever you are considering making a payment, there are considerable due-diligence steps that need to take place. OFAC [Office of Foreign Assets Control] has made it clear that there will be scrutiny not only of the company paying but the intermediaries who are involved. If an organization pays an entity or a bit coin wallet that is on the sanctions list, there could be legal consequences in addition to reputational harm."*

Preparations for responding are crucial

Even if a decision on payment cannot be made in advance, companies can take steps that will make that decision and others easier when the time comes. Ms. Sumner said that companies need to *"prepare to act strategically, with great speed."* Several measures are especially important:

- **Develop an incident response playbook.** Ms. Sumner urged every company to develop *"a playbook with critical decision points,"* including triggers for escalating the response and communicating with stakeholders, law enforcement, and the public. Incident response plans should be integrated across the organization, she added. Mr. Hindawi highlighted the importance of a clear chain of command.

- **Arrange for outside support.** Third-party advisers should be lined up advance, including experts who can handle the negotiations with attackers. *"We don't recommend that agents of the company do the negotiations themselves,"* Ms. Sumner said, and she warned that outside negotiation experts may be difficult to secure on short notice: *"They are in such hot demand that you cannot get them in an emergency because they're just too booked. Some may need to be put on retainer."* A member said, *"All of my companies have retained a third party or will have identified a third party in the event that payment is recommended."* Ms. Sumner added that these advisers should be hired under privilege. However, she warned, *"Communications with the threat actor are, of course, not privileged, so it is important to keep in mind that they may become public. The company needs to be aware of how they handle that situation so that they do not become embarrassed or look like they crossed a line in dealing with the threat actor."*
- **Test response plans.** Guests and members also mentioned the importance of testing response plans frequently and rigorously. In a premeeting conversation, Ms. Sumner said, *"I believe that regular tabletop exercises are an important component in maturing the plan and preparing for incidents. Include worst-case scenarios. Organizations thinking through tough scenarios now are much better prepared than those who have not. Some clients do multiple tabletop exercises per year."* Mr. Seets suggested that realistic live-fire drills involving red-team attacks, conducted by outside teams of ethical hackers, can be especially helpful. *"You play like you practice, and companies should also incorporate an element of surprise into their simulation exercises,"* he said.

Guests and members mentioned other advance measures that companies might want to consider. A member had seen *"at least one company hold cryptocurrency"* so that they would be able to pay a ransom quickly. Ms. Sumner mentioned the importance of planning for alternative forms of communication as a fallback if other communications systems fail. And while cybersecurity hygiene such as patching systems is not about preparing to respond per se, it can reduce the frequency of successful breaches and make the response more manageable by limiting the ability of attackers to operate within company systems.

Preparations for engaging with attackers is a distinctive aspect of ransomware attacks, but many of the other measures are helpful for mitigating and responding not only to ransomware attacks but also to other types of attacks. Thorough preparation for a range of threats can garner immediate benefits in terms of insurance policies, as Ms. Sumner noted in a premeeting conversation: *"Insurers are turning organizations down because the risk is too high—the companies are not doing enough to prepare. That's where preparedness makes a big difference: in obtaining coverage and getting a good premium."* In the meeting, she noted the importance of understanding the coverage in a company's policies; for example, *"do they cover the third-party vendors that you need?"*

Boards have an important role in preparations

Reflecting on the challenges of responding to cybersecurity incidents, ACLN members described a dilemma for boards: the ramifications of such incidents may be so serious that they require board involvement, yet the technical complexities may be difficult for most board members to absorb and analyze. During a fast-moving crisis when company management needs to act quickly, boards might find it even more difficult than usual to provide meaningful support.

An operational shutdown may be catastrophic, not only for the company but for customers, suppliers, and other stakeholders. In a premeeting conversation, a member argued that boards need to understand the company's plans for both prevention and response: *"From a board perspective, what I want to know is, if faced with this, how are we thinking about it? Yes, we get hit every day, but how are we protecting our systems? And when it does happen, how will we react, who is on point? Because you cannot anticipate the next crisis, but you will know it when you see it. All you can do is set up the critical infrastructure or framework for how you will deal with it."*

Members said that boards may need to weigh in on key decisions, especially those with strategic implications. *"The last thing you want is to have a meeting where the problem is already solved, tied in a bow. If you were not brought in immediately on a situation like this, you have a dysfunctional board,"* a member said. Another mentioned regulatory requirements that may apply in certain industries: *"The board has regulatory oversight over what they do and how they do it as well. If there is even a hint of a breach, I am informed and so is the board. I will get on the phone with legal and others to discuss what they know so far."*

Yet providing input on cybersecurity issues can be a challenge for board members. Many do not have extensive experience with these issues. *"I've got a lot to learn here,"* one ACLN member noted. Members and guests stressed the importance of expert advice to the board. A member advised that *"the best time to meet your experts is before something happens."* Boards are also recruiting members with cybersecurity expertise. Mr. Hindawi said, *"I'm seeing a lot of customers put people with tech experience in the room on the board side. Sometimes you have a board that is not understanding what the CISO [chief information security officer] is saying. You need a level of abstraction at the board level for communication."*

A member noted that boards cannot micromanage incident responses, but they can ensure that there is a framework in place to bridge the silos that exist in every organization. The detailed playbook should include a board engagement model laying out how the board will be involved. *"Align expectations on engaging with the board; for example, is it the lead director or the chair of the audit committee who should receive the first report?"* Ms. Sumner said. A member agreed: *"The board and the management team need to have a playbook. You want to develop that when you're not in a crisis."*

However, Mr. Hindawi also noted that increasing board involvement during an actual incident *"doesn't necessarily correlate with success: seconds count, and you don't want management to spend time on anything but remediation."* Some members expressed similar views in premeeting conversations. *"In these emergencies, there is no time to call a board meeting,"* one member noted, and another agreed: *"We know speed is really important. We don't want the board to be slowing things down."* Where boards can really make a difference, Mr. Hindawi argued, is in promoting the cybersecurity hygiene that mitigates the impact of breaches or even prevents them in the first place: *"There are things you can do right now."*

Conclusion

Ransomware attacks have become a major threat for companies and other organizations, as an entire industry has emerged around cyber extortion. ACLN members acknowledged that this level of sophistication requires a corresponding response from companies and their boards. Careful planning and practice are critical, the guest experts explained, involving both internal and external resources. For boards, the new challenge will require consideration of the tricky balance between delving into detail to ensure sufficient oversight and giving management the maneuvering room to respond effectively.

About this document

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

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

Appendix 1: Guest biographies

Orion Hindawi co-founded Tanium in 2007 and serves as its Chief Executive Officer. Mr. Hindawi leads the product strategy and development of the Tanium platform, in addition to all customer-facing technical operations and management functions.

A technology visionary and accomplished inventor, Mr. Hindawi has led the development of enterprise-scale endpoint security and management platforms for the past 18 years at BigFix, Inc. (acquired by IBM in 2010) and Tanium, in addition to holding multiple software patents in the areas of network communications and systems management.

Mr. Hindawi works closely with Tanium customers on a daily basis in the pursuit of inventing new approaches for solving the significant challenges IT departments face securing and managing large, global enterprise environments. Mr. Hindawi also serves on the Tanium Board of Directors.

Chuck Seets is a member of the EY Americas Assurance Leadership Team, focused on cybersecurity matters affecting EY audit clients.

Mr. Seets joined EY in 1997 in Charlotte, NC, before relocating to Atlanta, GA, in 2001. He assumed several Southeast Region leadership roles, making partner in 2002 and becoming the coordinating partner for a Fortune 300 global manufacturing company (non-audit client).

In 2005, Mr. Seets led the creation of the EY Southeast Audit Committee Network, a forerunner to numerous similar networks, both domestically and abroad. He developed and continues to moderate similar professional networks of Fortune 100 CFOs, general counsels, controllers, treasurers, and corporate secretaries. Further, Mr. Seets has moderated and/or served as a panelist for national organizations such as the Council for Institutional Investors, the Institute of Internal Auditors and others. He also developed the EY CFO Development Program to support those transitioning or aspiring to become CFOs.

Mr. Seets is active in the community, having served on the boards of Central Atlanta Progress and the Georgia Chamber of Commerce. Chuck is also involved in the Juvenile Diabetes Association, having been featured in a publication entitled “Profiles of Courage—Living with Type I Diabetes.” He’s also a past Elder of St. Luke’s Presbyterian Church and serves as a professional mentor to scholar athletes from the University of Georgia.

He has co-authored cybersecurity research published in the Harvard Law School Forum on Corporate Governance and Financial Regulation, and he has been quoted on cybersecurity matters in Bloomberg Law, Institutional Allocator, and other publications.

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 ACLN participated in part or all of the meeting:

- Barbara Byrne, ViacomCBS
- Pam Daley, BlackRock
- Dan Dickinson, Caterpillar
- Dave Dillon, 3M and Union Pacific
- Sam Di Piazza, AT&T
- Bill Easter, Delta Air Lines
- Tim Flynn, JPMorgan Chase and Walmart
- Alan Graf, Nike
- Gretchen Haggerty, Johnson Controls
- Fritz Henderson, Marriott
- Bob Herz, Morgan Stanley
- David Herzog, MetLife and DXC Technology
- Charles Holley, Amgen and Carrier Global
- Michele Hooper, United Airlines
- Hugh Johnston, Microsoft
- Nick LePan, CIBC
- Mike Losh, Aon
- John Lowe, Phillips 66
- Edward Ludwig, CVS
- Louise Parent, FIS
- Ann-Marie Petach, Jones Lang LaSalle
- Peter Porrino, AIG
- Paula Price, Accenture
- Tom Schoewe, General Motors
- Leslie Seidman, GE
- Gerald Smith, Eaton
- John Stephens, Freeport-McMoran
- Tracey Travis, Facebook
- Jim Turley, Citigroup and Emerson Electric
- John Veihmeyer, Ford
- Robin Washington, Salesforce.com
- Maggie Wilderotter, Hewlett Packard Enterprise

The following members of the European Audit Committee Leadership Network (EACLN) participated in part or all of the meeting:

- Jeremy Anderson, UBS
- Carolyn Dittmeier, Assicurazioni Generali
- Margarete Haase, ING
- Liz Hewitt, National Grid
- Dagmar Kollmann, Deutsche Telekom
- Pilar Lopez, Inditex
- Kalidas Madhavpeddi, Glencore
- Stephen Pearce, BAE Systems
- Bernard Ramanantsoa, Orange
- Guylaine Saucier, Wendel

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

- John King, EY Americas Vice Chair of Assurance Services
- Steve Klemash, EY Americas Leader, Center for Board Matters
- Pat Niemann, EY Greater Los Angeles Managing Partner, Center for Board Matters

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

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

[3] Dustin Volz et al., "Colonial Pipeline Said to Pay Ransom to Hackers Who Caused Shutdown," *Wall Street Journal,* May 13, 2021.