European Audit Committee Leadership Network

July 2020

EACLN

VIEWPOINTS

Cybersecurity implications of the pandemic

The COVID-19 pandemic has tested information technology (IT) infrastructures and cybersecurity systems in unprecedented ways. Lockdowns forced employees, including executives, to work from home indefinitely, and companies rushed to provide devices to maintain business continuity and technical support on secure networks. New working conditions, and the new ways of doing business they required, rendered many preexisting controls obsolete.

In some cases, criminals and other bad actors seized on the moment to infiltrate company systems in new and creative ways. The rise of layoffs and furloughs—at a time when the pandemic made it difficult to collect company hardware or deactivate network credentials—created additional risk. IT and cybersecurity departments adapted quickly; at times, though, they were more adaptive than proactive. Audit chairs want to understand which strategies and tactical responses were most effective and which lessons can be useful in future crises.

On 26 June 2020, members of the European Audit Committee Leadership Network (EACLN) met virtually to discuss these issues.[1] They were joined by Robin Dargue, global chief information officer at WPP, and Antero Päivänsalo, chief information security officer at Nokia. *For guest biographies, see Appendix 1, on page 9; for a list of all meeting participants, see Appendix 2, on page 10.*

Executive summary

EACLN members and their guests explored the following three topics:

- **The pandemic disrupted IT systems and invited attacks** *(page 2)*
  The shift to remote work disrupted IT systems, employee behaviors, and cybersecurity defenses. Innovative responses maintained business continuity but increased risk by eroding controls. Bad actors adjusted their tactics to take advantage of technological disruptions and health-related anxieties.

- **Company responses focused on communication and risk management** *(page 3)*
  Companies that responded quickly to the COVID-19 outbreak in Asia learned helpful lessons for the eventual pandemic. Principles-based central messaging that reached everyone in the organization immediately nurtured efficiency and agility. Adjusting controls ensured that business continuity did not create undue risk. Training refreshed and reinforced risk awareness. Risks associated with cloud storage and other third-party solutions were given renewed attention.

- **Board oversight requires engaging on the details** *(page 6)*
  Audit chairs can help their companies by engaging with and supporting their executives on cybersecurity and IT issues. Companies engaging cloud providers and other third parties

should plan carefully and be aware of the downsides. Board oversight of these issues may in the future require additional board technical prowess.

For a list of discussion questions for audit committees, see Appendix 3, on page 11.

The pandemic disrupted IT systems and invited attacks

The COVID-19 pandemic caused people to shift to remote work in remarkable numbers almost overnight. While audit chairs note the surprisingly positive results of this shift, they also acknowledge that it increased some risks. Changes to business practices rendered many preexisting controls impracticable. Moreover, distracted employees were more likely to engage in sloppy network activity. Bad actors rushed to capitalize on these vulnerabilities.

Remote work eroded controls and enabled risky behaviors

Members and guests agreed that companies switched to remote-work models extremely well. Mr. Dargue said that of the many individuals and groups that drove the transition, IT departments deserve special recognition: *"Overnight, everyone went to remote. At WPP, we went from 200 large offices to, in effect, 107,000 one-person offices. It was incredible."* For many companies, the transition was uncomfortable, however. Employees faced the double burden of adjusting to working from home while worrying about the impact of the pandemic on health and well-being. Mr. Päivänsalo stressed that not everybody feels comfortable working remotely: *"Of course there was also a lot of confusion and stress. New ways of working emerged. Many homes are not ideal places to work from. We saw a short-term increase in basic security mistakes by people who know better."*

Mr. Dargue said that as companies came up with new ways to operate their businesses through the pandemic, many did not match those innovations with adequate controls. *"Early on, there was perhaps too much 'do whatever it takes' talk,"* he said. Mr. Päivänsalo agreed: *"Necessity increased our risk appetite and triggered innovation. It is not always a good thing."* Procedural safeguards that could only be completed on-site or in person became impossible to execute. Mr. Dargue said that, for example, crisis conditions made electronic signatures necessary where, before, institutional resistance would have impeded their adoption; however, the risk remained: *"We saw a risk and an increase in potential fraud. The rapid evolution of how things were executed is where we identified potential issues."*

Members and guests highlighted the unique challenge of dealing with third-party providers, many of whom were themselves making rapid changes. They emphasized the importance of assessing and balancing risk as companies contemplate adopting new technology. In some cases, the pace of change during the pandemic made this analysis more difficult.

IT changes and health anxieties invited cyberattacks

The pandemic and the resulting technological changes created new opportunities for bad actors. Mr. Päivänsalo said, *"We've seen a shift in cybercriminals' approaches. They're trying to exploit the event [the pandemic]; they take advantage of it."* The degree and frequency of new attacks varied widely by company and industry. Some members' companies saw a significant increase in the number and sophistication of attacks, while others said the pandemic brought no noticeable uptick in activity. One member said that bad actors are *"a step ahead,"* and another observed *"clear evidence of more cyberattacks."*

Mr. Päivänsalo stressed that each company should identify the cyber risks that affect it the most. At Nokia, for example, *"We're primarily a business-to-business company and not that attractive target for most cybercriminals."* A company's business model, sector, locations of operations, cloud computing practices (discussed below), and other factors may determine its risk profile.

Guests and members identified a number of cyber-risk trends that have emerged during the pandemic. Phishing attacks, which have increased during the pandemic,[2] are a concern at many companies. These attacks often entice end users to click on illicit links or share confidential information by featuring pandemic-related content. Mr. Dargue said, *"With phishing, you play to human nature and stress. People worry about their families. Cybercriminals use social engineering about issues close to people's hearts to obtain their credentials."*

Mr. Päivänsalo said advanced persistent threats are among Nokia's most pressing threats as supplier for critical national infrastructure. These threats, which in many cases are backed by state actors, attempt to access networks over long periods of time in order to steal data, while remaining undetected.[3] Mr. Dargue cautioned members not to underestimate the sophistication of cybercriminals: *"These organized-crime operations are in a way just well-run businesses; they have a clear profit-and-loss mindset. Like any business, their strategy is to maximize their return for the least possible investment."*

Mr. Päivänsalo noted that there recently has been an alarming trend of more attacks targeting healthcare industry and particularly COVID-19 research. Mr. Dargue noted a rise in data exfiltrations, in which cybercriminals remove data from computers.[4] Unlike ransomware, in which the cybercriminal typically encrypts data and demands a ransom for its decryption, in an exfiltration, the cybercriminal threatens to publicly expose the data it has obtained.[5] The threat of public exposure adds reputational risk to the financial risk of ransomware.

Company responses focused on innovation and risk management

Members and guests shared their observations on how companies were able to most effectively handle the new technology risks that arose during the pandemic. They noted that principles-based, company-wide responses were critical, especially when complemented by specific tactical measures like adjusting controls to keep up with innovative systems changes.

Early action helped companies respond effectively

The fast-changing nature of the pandemic-led crisis required IT and cyber teams to take decisive actions, even before they fully understood the extent of the problem. Those that acted fast with strong, independent thinking when COVID-19 first emerged in China were better prepared as the crisis spread globally. Both guests said their companies used values-based leadership. According to one *Forbes* writer, values-based leadership means "leading the team and evaluating performance—both your own and the team's—based more so on the organization's set of values than specific metrics and milestones."[6]

Health and safety for employees and customers is a value common to nearly every company during the pandemic. Mr. Dargue said, *"We called it a crisis early and enacted our crisis-management procedures, all of which were effective. Global companies with a presence in China that were able to take the learnings there and use them beyond China fared well. On the back of China, we called it a crisis early for the rest of the [company's global operations]."* Mr. Päivänsalo said that Nokia also benefited from its early crisis experiences in China. *"Our executives helped make things happen fast with values-based decisions from the beginning. The company focused on values, not dollars, and didn't rely solely on governmental guidance. This helped create employee confidence and a sense of security. Have the boldness to make principled decisions without getting bogged down by politics and governments."*

Both guests said that consistent, centralized approaches to crisis response and internal communication helped their companies. Mr. Päivänsalo emphasized that a well-established, centralized, and cross-organizational security crisis management process was used as a model in Nokia to put in place rapidly a solid health and safety response to COVID-19. Mr. Dargue said that enhanced technology made it easier for companies to centralize key internal communications. He explained that collaboration tools (Microsoft Teams, Zoom, etcetera) with large audiences allowed WPP to bypass the "cascade" approach to internal communications. Rather than conveying talking points to regional leaders, who communicate to lower-tier managers, who then convey a version of the message to front-line employees—the cascade—executives could now communicate directly to the entire workforce. *"Cascading doesn't work,"* Mr. Dargue said. *"We've been using the new collaboration technology to eradicate the need. Collaboration tooling delivered the messages to the end audience in one effort, consistently."*

These overarching crisis strategies helped WPP with its tactical decisions. Foreseeing widespread lockdowns after the initial outbreak in Wuhan, the company ordered large quantities of the IT hardware it would need for remote work, like laptops. *"From learning from China, when the pandemic hit Europe and the Americas, the transition was much more smooth,"* Mr. Dargue said. The company saw that it was in unfamiliar territory, so it leveraged technology to identify network risks: *"We used big data and artificial intelligence to look at patterns. It's what we already wanted to do, but now the scale is huge. Security logs and data lakes have helped us spot bad behavior well in advance. Crisis management helped us break down barriers to innovation and data."*

Controls and training accompanied innovative solutions

New conditions and processes required companies to update controls in response. Rapid innovation and heroic efforts to maintain business continuity, Mr. Dargue said, created this need: *"Companies now need to compensate for the rhetoric and can-do attitude with new or amended controls."* Members agreed, with one saying, *"You need to coordinate controls and compliance functions and rapidly transition to a more structured framework."* Mr. Dargue said that WPP adjusted controls on an ongoing basis: *"We reviewed processes that had changed* *with the controls team, putting in controls to compensate for new practices on a temporary basis, if needed."*

Mr. Päivänsalo noted that making training available also helped employees deal with remote-work challenges and the cyber threats that emerged: *"When people started feeling OK about working from home, they wanted more information about good practices and were willing to invest time in it. The attendance numbers to our trainings and security accreditation program jumped."* A member agreed about the importance of complementing new processes or procedures with training: *"You must ensure that people working remotely are appropriately trained and understand the current expectations."*

Cloud technology and other packaged solutions called for caution

Some companies saw the transition to remote work as an opportunity to accelerate their adoption of new technologies. IT transformations can bring great value and facilitate business continuity, but they carry risks, especially during a time of crisis. Members and guests focused on the consequences of accelerating the use of cloud-based IT solutions as more people work remotely. Many stressed that the swift adoption of cloud technology increases near-term risk, creating oversight challenges. One member said, *"We're doing a cloud migration. I haven't seen particularly well-structured agendas for this issue. There will be some major governance problems with this technology."*

Mr. Päivänsalo said that thinking about the cloud in the right way can reduce risk and facilitate smooth implementation: *"The cloud isn't really a strategy, and it's not a product; it's a delivery mechanism with many variations. It can be very damaging when used as an extension of existing services. If you're considering the cloud and don't have earlier experience with it, develop a business case first and then take baby steps. Take time to develop not only the technology but an organization and processes to match it."* A member whose company was undergoing a cloud transition agreed: *"These things take a while to put in place. Multiple years might be too pessimistic, but it does take time to make sense of the transition."*

Risks associated with transitioning to cloud-based systems include the following:

- **Less customization.** Cloud providers' security efforts are not always customizable to companies' requirements: *"We've seen that cloud services aren't always configured with the right security parameters,"* a member reported. Mr. Dargue concurred: *"When we examined our cloud environments, we found that compliance with basic IT controls was lacking in some instances. Developers somehow thought their technologies didn't need to comply with basic IT controls."*

- **Stakeholder pushback.** Many stakeholders, including consumers,[7] do not trust the cloud and may resist a company's adoption. Companies that put sensitive information like health data on the cloud may meet more resistance. In some instances, companies are prohibited from placing certain information in the cloud because it may cause them to run afoul of contractual terms or compliance measures.[8]

- **Too much or too little cloud diversity.** A security expert said the single-cloud model risks downtime and vulnerability to attacks: "If a cloud provider experiences a major issue, it could lead to a single point of failure that takes down network access and resources … If a single cloud provider environment is somehow exposed to vulnerabilities, this could have a ripple effect on anyone hosted there."[9] However, using multiple cloud providers increases complexity. A multicloud strategy creates "more work to prepare and look for security control options that can work across more than one environment."[10]

Third-party risks received renewed focus

The pandemic has caused boards and audit committees to reconsider their appetite for the risk that comes with relying heavily on third parties for key tasks. Mr. Dargue suggested companies reassess their third-party relationships and their attendant risks: *"Over time, there has been a slow but sure movement of key business processes to third parties. Some businesses are not really aware of how dependent on third parties for basic operations they now are,"* Mr. Dargue said.

Swift adoption of innovative technologies, combined with cybersecurity breaches at third-party providers, contributed to a renewed focus in this area at many companies. One member noted with concern a recent class-action lawsuit against a company whose cybersecurity breach and subsequent forensic investigation left data exposed to the public. The member was also concerned about a recent ransomware attack and the risks associated with cloud computing. *"We talk a lot about third-party risk management, but what tools and assurances can we get?"* the member asked.

Mr. Päivänsalo said mandatory security controls for third parties can help. Contractual requirements, mandatory trainings, security risk assessments, security audits, and third-party risk monitoring solutions can align risk tolerances with actual risks. *"Third-party risk-monitoring and audit solutions help you to rapidly capture a basic picture of your supply base and the security risks it might have. This way you can slice and dice your supply portfolio into risk buckets and understand what's important. And then take targeted actions to reduce your risks. You can also require your most important suppliers to provide your company with a critical information protection plan. In it you ask them to describe what exactly are they doing to ensure that your most sensitive data is safe with them. And then audit them against it,"* he said.

Board oversight requires engaging on the details

The combination of multiple pandemic-related IT issues creates a complex governance challenge. The crisis has led audit chairs to rethink how best to engage with management on critical issues, including those related to IT and cybersecurity. Guests and members said they have had to provide more granular oversight in a range of areas:

- **Reassess cybersecurity practices.** Cybersecurity might not be on all executives' minds during an operational and financial crisis. However, IT disruptions and transformations and new cyber threats call for extra cyber-risk vigilance by functional and operational executives—not just IT, cybersecurity, and other technology executives. *"Ask your executives if they have evaluated any extra risk posed by cybersecurity. It doesn't have to be a technical conversation; just get a basic concept of how they manage security and risk,"* Mr. Dargue said. The question may prompt executives from different disciplines to communicate about emerging risks and the company's responses.

- **Check on controls.** Focusing on the controls adjustments helps audit chairs understand where risk is elevated. *"Audit committees should check if the executives know company key risks and what are the main controls in place to mitigate them,"* Mr. Päivänsalo said.
- **Learn more about cloud providers and other third parties.** Board members are taking a closer look at the risks of third-party relationships, including those with cloud providers. Mr. Dargue encouraged audit chairs to ask management what critical data is stored in the cloud: *"Determine if sensitive data is involved. We would consider paying extra for private cloud versus public cloud because that suits our risk profile."* Since the pandemic has affected every company's operations to some degree, checks on data held by other third-party providers may also be in order. A company's business continuity may depend on a suite of third-party providers—which themselves are weathering the crisis. Mr. Dargue said, *"Ask management, as they look back on the early stages of the pandemic, Where were the supply chain failures that affected business continuity?"*
- **Consider assessing the board's technological expertise.** All of the technology issues raised by the pandemic led some members to again consider whether their boards need more technical expertise. One member's board initiated a special cybersecurity committee during the pandemic, with the expectation that the chief information officer report to the board on a regular basis. Another member, noting the rapid IT changes, said it is *"more important than ever"* to have technical knowledge on the board: *"You should have a board member who understands cybersecurity and is able to ask the right questions. For digital accounting, auditors are engaged. I look to myself—I'm finance, accounting, M&A, but I'm not an IT specialist. Do you have enough knowledge on the board?"*

Conclusion

Many companies were fortunate to have technology teams that maintained business continuity while keeping networks, data, and processes secure. Innovation and higher risk tolerances helped many companies manage through unique circumstances, but innovation also necessitated new controls, heightened awareness, and selective caution. The unprecedented change environment required a holistic understanding of how technology, threat actors, third-party risk, and business continuity intersect. It also raised questions about the role of the board and how best to achieve these goals. Developing the right mindset and following up with controls, training, and effective communication helped companies move forward with purpose, confidence, and security.

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.

The perspectives presented in this document are the sole responsibility of Tapestry Networks and do not necessarily reflect the views of network members or participants, their affiliated organizations, or EY. Please consult your counselors for specific advice. EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Tapestry Networks and EY are independently owned and controlled organizations. This material is prepared and copyrighted by Tapestry Networks with all rights reserved. It may be reproduced and redistributed, but only in its entirety, including all copyright and trademark legends. Tapestry Networks and the associated logos are trademarks of Tapestry Networks, Inc. and EY and the associated logos are trademarks of EYGM Ltd.

Appendix 1: Guest biographies

Robin Dargue is the CIO of WPP. Robin's focus is to execute the transformation of WPP's IT environment to enable the company's strategic future.

Robin joined WPP in 2014 from Alcatel-Lucent, where he was Executive Vice President, Business & IT Transformation and a member of the Alcatel-Lucent Management Committee. Prior to that, Robin was a business leader at both Royal Mail and Diageo, in charge of Business & IT-based transformation programs. At Royal Mail, he oversaw the introduction of a number of new technology-led products and services for customers, whilst leading the modernization of the organization's technology assets.

Robin has a degree in Computer Science from Strathclyde University.

Antero Päivänsalo is a security and technology executive with 15-plus years of experience in senior leadership positions. For the past five years, Antero has lead Nokia's information security function as the group CISO. He is also the secretary for Group Leadership Team quarterly security reviews and leads the company-wide response for major security events.

Before moving to Nokia's security organization, Antero held multiple roles in Nokia's IT leadership team as head of operational excellence, head of performance and assurance, head of project management center, and head of IT region Greater China.

Antero has an MBA in finance and an M.Sc. in industrial engineering and computer science. His studies include a semester in Gwangju Institute of Science and Technology (South Korea). He is an active speaker. His engagements include a lecture series at the Chinese Academy of Sciences (China) for a postgraduate program and presentations at the Information Security Forum global conferences.

Antero works at Nokia headquarters in Espoo (Finland). He was born in Finland and has worked in China, Singapore, and India. In his spare time, he enjoys jogging, comics, trying out new gadgets, and tinkering at his summer cottage.

Appendix 2: Participants

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

- Jeremy Anderson, UBS
- Werner Brandt, Siemens
- Julie Brown, Roche
- Carolyn Dittmeier, Assicurazioni Generali
- Eric Elzvik, Ericsson
- Edgar Ernst, TUI
- Byron Grote, Tesco, Akzo Nobel, and Anglo American
- Margarete Haase, ING
- Marion Helmes, Heineken
- Liz Hewitt, Novo Nordisk
- Arne Karlsson, Mærsk
- Dagmar Kollmann, Deutsche Telekom
- David Meline, ABB
- Hanne de Mora, Volvo Group
- Marie-José Nadeau, ENGIE
- Sarah Russell, Nordea Bank
- Guylaine Saucier, Wendel
- Erhard Schipporeit, RWE
- Carla Smits-Nusteling, Nokia
- Alan Stewart, Diageo
- François Thomazeau, Bolloré

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 EMEIA Assurance Leader
- Julie Teigland, EY EMEIA Area Managing Partner

Appendix 3: Discussion questions for audit committees

- How has the pandemic affected your company's IT and cybersecurity infrastructures?
- What cyber threats did the pandemic create for your company?
- Has your company responded effectively to the cyber risks that have emerged during the pandemic? What has made the difference?
- How does your company benchmark cybersecurity performance in the current work environment?
- How did your company ensure that employees were adequately aware of the unique cybersecurity risks created by the pandemic?
- What innovative technology solutions did your company adopt during the pandemic?
- Did your IT or cybersecurity team accelerate any new initiatives in the first weeks and months of the pandemic?
- How has your company monitored and mitigated third-party risks related to the pandemic?
- How has your company adjusted controls for new business practices, logistical processes, and remote-work environments?
- As your company responds to its pandemic-related IT needs, is it ensuring close coordination with the information security team?
- How have the audit committee and full board changed their IT, cybersecurity, and risk oversight practices?
- Have technological innovation and cyber risk created the need for more technology expertise on your audit committee or board?

Endnotes

[1] This document 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 and other participants in connection with the meeting.

[2] Tanya Powley and Tim Bradshaw, "EasyJet Says Hackers Accessed Travel Details of 9m Customers," *Financial Times*, May 29, 2020.

[3] Margaret Rouse, "Advanced Persistent Threat (APT)," TechTarget, accessed July 7, 2020.

[4] "What is Data Exfiltration?" Infoblox, accessed July 15, 2020.

[5] "The Marriage of Data Exfiltration and Ransomware," Coveware, accessed July 15, 2020.

[6] Brent Gleeson, "How Values-Vased Leadership Transforms Organizational Cultures," *Forbes*, March 10, 2017.

[7] Cameron Coles, "9 Cloud Computing Security Risks Every Company Faces," McAfee, accessed June 6, 2020.

[8] Coles, "9 Cloud Computing Security Risks Every Company Faces."

[9] Dave Shackelford, "The Risks of Multi-Cloud Security Compared to Single Cloud," TechTarget, May 7, 2019.

[10] Shackelford, "The Risks of Multi-Cloud Security Compared to Single Cloud."