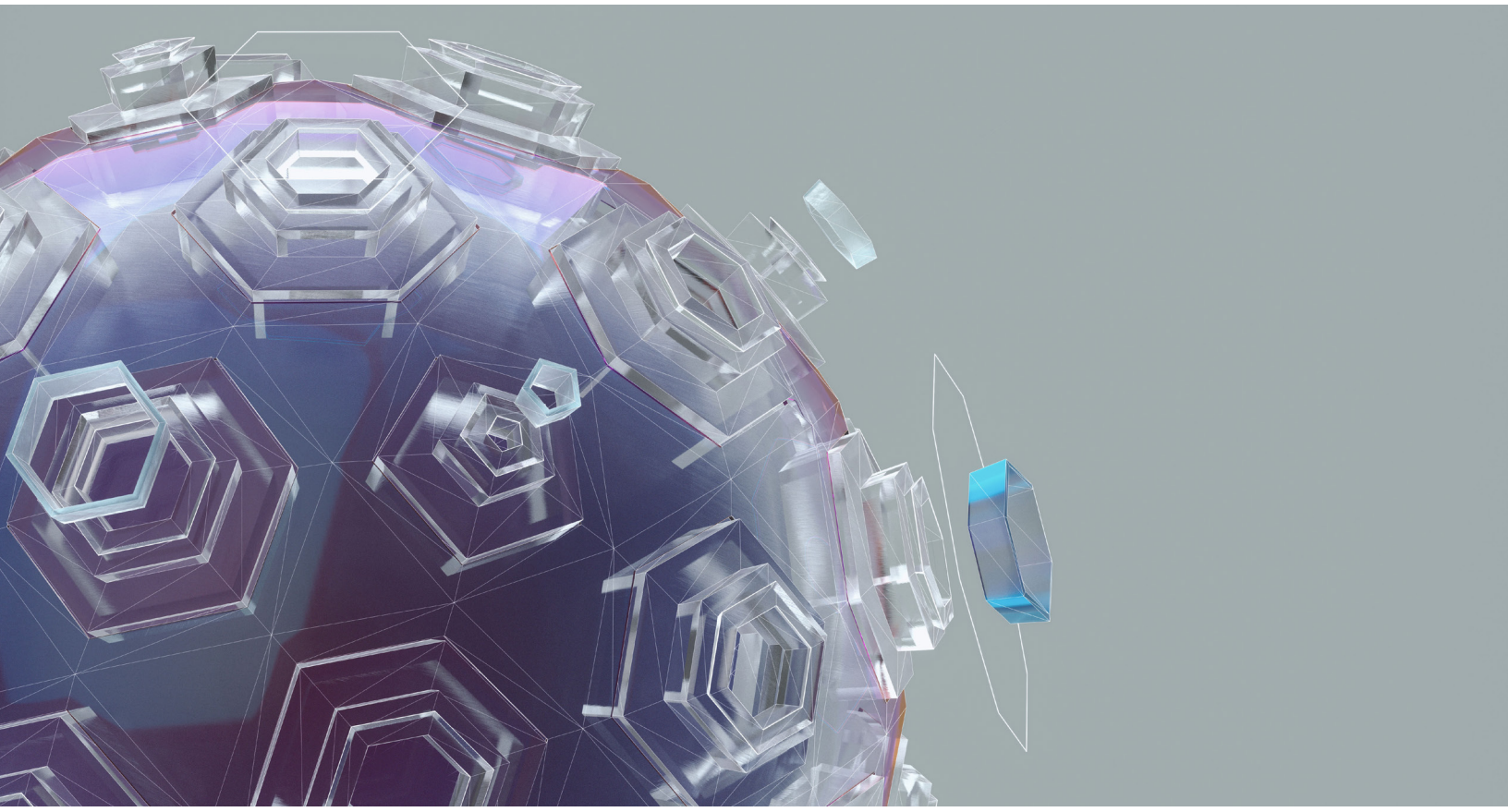
McKinsey & Company

Strategy & Corporate Finance Practice

Boards and cybersecurity

How boards should prepare for the rising cybersecurity threat



February 2021

The board agenda has been crowded since the start of the pandemic, and many issues have acquired new urgency. In this episode of the *Inside the Strategy Room* podcast, Frithjof Lund, the leader of our board services work, speaks with two cybersecurity experts about how boards of directors should help their organizations ensure they are prepared for potential cyberattacks. John Noble is the former director of the United Kingdom's National Cyber Security Centre and a board member of NHS Digital, the national information and technology partner to the country's National Health Service. Wolf Richter is a McKinsey partner who helps chief information officers (CIOs) capture the benefits and mitigate the risks of tech-enabled transformations.

Frithjof Lund: Cybersecurity has been on the board agenda for some time. In our latest global board survey, participants rated it among their top four priorities. However, when we ask board members about their key challenges today, only one in five mentions cybersecurity. Have you seen a shift in how companies are approaching this issue?

Wolf Richter: It used to be mainly the regulated industries—particularly banks and insurance companies, as well as utilities and public-sector entities on critical national infrastructure—that prioritized cybersecurity. After the WannaCry ransomware attack a couple of years ago, however, many others realized that even without being on the high-target list, they could fall victim to a cyberattack. Retailers and manufacturing companies in particular have become a lot more aware of the vulnerabilities that digitization brings to their operations. Now that working from home has become the norm, and given the massive increase in ransomware attacks that we are seeing, most companies realize how vulnerable they are in an environment where most of their business and employee interactions are conducted through online channels.

Frithjof Lund: You mentioned an increase in cyberattacks. What is driving it?

John Noble: There are two things. One is the change in the business model among the people carrying out these attacks. Cybercrime is becoming industrialized. Vulnerabilities are identified by one set of groups that then share the information with criminal groups. Those criminal groups can, in effect, lease the ransomware in exchange for a percentage of the profits and employ it against victims. That has enabled a massive increase in both the volume of attacks and their sophistication. Ransomware can not only affect the availability of your systems but also result in the release of sensitive data.

Frithjof Lund: Are companies sufficiently prepared to handle this rising threat?

Wolf Richter: It's a mixed bag. It is becoming apparent who has been thinking about cybersecurity systematically and who has just recently woken up and is starting to improvise. On the one hand, we have seen a massive acceleration in digitization as companies have moved their operations to the cloud and granted remote access to employees. Needless to say, very few had the time to think through the cybersecurity implications. On the other hand, those who have spent the past couple of years preparing—identifying their critical assets and processes, testing the procedures with employees, putting in place emergency plans and fallback scenarios—are seeing those investments pay off.

Frithjof Lund: What approach should boards take to this topic, especially those whose companies are less prepared?

Wolf Richter: The board of directors and the executive leadership need to engage in a critical conversation. The board's responsibility is to make sure that the executive team has a plan, is prepared, and is preparing the whole organization

> “Cybercrime is becoming industrialized. Vulnerabilities are identified by one set of groups that then share the information with criminal groups.”
>
> —John Noble

for the eventuality of an attack. The question is not whether the attack is going to happen and how to prevent it. The real questions are, when will it come? Is the organization prepared to detect it? Is it prepared to stop it? Can it mitigate the effects and get back to normal operations as quickly as possible?

John Noble: Cybersecurity is an issue for the whole organization. Whether it is in advance of or during an incident, you should not just leave it to the chief information officer and the technical team. Leaders need to decide how to manage the tensions between usability, security, and cost, and that is very much where we need the board challenging and testing processes.

Frithjof Lund: What should a board do when an incident happens? John, you have seen that up close in many situations.

John Noble: Going back to preparedness, there is a big difference between how an organization reacts if it has exercised its processes around dealing with an attack in advance and one that has not. Communication is essential. There needs to be a single version of the truth, so everybody both within and beyond the organization understands how the incident is being handled. The board has a crucial role there in supporting the executive team. As I saw during the 800-odd incidents while I was at National Cyber Security Centre, the executive teams are under tremendous pressure and they need the board’s support and guidance.

The WannaCry incident in May 2017 had a very big impact on the UK National Health Service, where I am now a nonexecutive director on the NHS Digital board. The important thing at the board level was communicating with the vast number of stakeholders across the healthcare system. I can’t say that the NHS got everything right, but it certainly learned a tremendous number of lessons. This meant that going into the pandemic, the board was much more prepared, understanding the vulnerabilities we are carrying and asking the right questions around how those are being mitigated.

Frithjof Lund: Any caveats you would highlight for boards or management teams?

John Noble: Generally, the incident response will go badly if it is just left to the CIO and the technical team. They have a critical role in resolving the incident, but the consequences go beyond the immediate damage. There will be reputational, legal, and operational issues. You need the whole senior-management team to come together.

Wolf Richter: A cyberattack tends to elevate and exacerbate tensions that already exist within an organization. I have seen things go particularly poorly in decentralized organizations with no central leadership team or where it was unclear who would lead during a crisis. When people are not used to working together, establishing trust during a crisis is extremely difficult. Finger-pointing starts, and people fight each other instead of the enemy attacking them from outside.

Frithjof Lund: How do you build cybersecurity capabilities within the organization? What are the key areas boards should focus on?

Wolf Richter: First and foremost is awareness among the whole leadership team. We often see a concerned board member and the CIO but a vast amount of ignorance in between. There should be a shared sense of urgency about this issue within the executive team and the level below. It's about the awareness that this is not something that affects others but is an existential threat to the organization in the digital world.

The second step is to develop the concepts and tools. This is the hard, unglamorous work that has nothing to do with the folks in black hoodies building some new cybersecurity incubator. It's about checking, which are the critical assets and processes? Are there procedures in place in case of an attack? It is important during this phase to balance the controls and red tape you put in place so it does not stifle internal innovation, which can give cybersecurity efforts a poor reputation. That's why these initiatives should be led by people with a business mindset, not just a control or technology mindset.

That leads to the third part, which is building capabilities. This affects the whole company—the process architects and marketing and salespeople when they negotiate with customers, who more and more are asking about security features, especially in engineering and high-tech industries. All these folks need to know whom to turn to for information. When cybersecurity becomes a joint capability, the whole organization becomes more cyberresilient.

John Noble: I would add that with ransomware, one of the big risks is around legacy equipment, which almost every organization has. It represents a vulnerability that attackers are exploiting. We have to treat legacy equipment as untrustworthy and put in place controls to manage it. But only some of those controls are technical, and the business and IT teams need to engage to see whether some of the risk can be managed in other ways. Is that equipment needed? Can it be segmented? Maybe the answer is to migrate to the cloud, which will have investment implications.

Frithjof Lund: If I am a board director concerned about cybersecurity, how do I best understand how well my organization is prepared?

Wolf Richter: There are a couple of ways to measure this. Ideally, an organization would measure the business value at risk from a given incident. However, most companies lack the transparency or a reliable model to translate and collate the business impact of an incident. Many companies turn to what is called a maturity-based approach, using outside benchmarks to assess their controls' relative level of maturity. While that is better than not managing cybersecurity at all, sometimes it leads to the wrong incentive to simply invest in more controls.

If I was a board member, I would ask which assets or parts of the organization the cybersecurity team and the leadership team focus their attention on. Have they identified employee groups that are particularly vulnerable, such as field service agents or customer service representatives? Do they know how many people have privileged user rights? We live in an environment of scarce resources, and the executive team needs to balance the investments in cybersecurity with investments in all other parts of the business. The more specific they are

> “You need to expect attackers to be equipped with almost military-grade weapons. It’s like placing machine guns in the hands of burglars.”
>
> —Wolf Richter

in targeting initiatives toward specific systems, infrastructures, processes, and people, the better I would feel as a director.

John Noble: I think that’s so important. We cannot just rely on KPIs such as the percentage of service that has been updated. You need to have that engagement. Another way the board can get further assurance is through a third-party challenge, such as penetration testing of critical assets. When was the last penetration test carried out? What did it reveal? What recommendations have been taken forward? But before you do that, you have to identify what is critical and needs to be protected.

Frithjof Lund: Are there cybersecurity investments you see companies making that are poor uses of resources?

John Noble: The cybersecurity market is still immature, and many people are trying to sell boxes that promise to “fix” all your cybersecurity problems. There is no single solution for cybersecurity. It needs to encompass a range of measures, and the most effective measures tackle the basics that make companies vulnerable around security updates, authentication, and how you access and configure the systems.

Wolf Richter: I often see companies doing one-time capital investments but shying away from operating investments in the people. We evaluated one insurance carrier that had a beautiful security operating center, all the licenses and sensors in place, but they lacked the staff to make it run 24/7. You need to have somebody processing the information, but they had one guy who was tasked part-time with translating and sharing the data with the rest of the organization. Of course, it didn’t happen. Companies are overinvesting in some parts but not thinking about how to bring those investments into the day-to-day decision making.

John Noble: To build on that, I saw a case study presented recently by one of the leading companies in this area, around how their detection system that uses artificial intelligence had flagged a system compromise. It turned out that there was nobody to interpret this data, so despite all that investment in a very expensive and sophisticated detection system, nobody took action to prevent damage.

Frithjof Lund: What about the capabilities within the board itself? Where are the main gaps?

John Noble: I think it’s essential that somebody on the board has cybersecurity expertise to provide a challenge for the CIO and the chief security

officer [CSO]. They can also help with building up the overall board's knowledge, because leaving cybersecurity to one person is absolutely not the answer. You need the whole of the board to engage, to bring their experience of other areas to provide the right challenge in this space.

Wolf Richter: We need to demystify cybersecurity. The typical reaction of a board that has low cybersecurity skills is, "Ooh, that is not a topic for us. Let's call the CSO or the CIO and they can explain what is happening." But cybersecurity is not rocket science. It is somebody tinkering with your processes, systems, assets, and data. This realization usually comes easier if a board member says, "It is our job to make sure the organization is prepared. We don't have one guru or wizard who will fix all our problems."

John Noble: I very much recognize that description. The organizations that are not cyberliterate want to leave it to the CIO and the CSO. But those executives want to share some of the risks and to expose the critical issues to the board, not least because these issues often require investment and difficult trade-offs between cost, usability, and security.

Frithjof Lund: John, you mentioned that even having one cyberliterate board director could help build the capabilities of the entire board. Can you elaborate?

John Noble: I have seen companies organize exercises that serve as both teaching opportunities and opportunities to highlight the risks the organization faces: giving the board a briefing on the threat and then looking at how best-in-class companies address it.

Wolf Richter: We insert cyberexercises into Silicon Valley trips we do with boards. The directors visit high-tech companies and then we show them the dark side of digitization, demonstrating what can happen if you don't pay attention to the risks that come with the opportunities that technology provides. Getting their attention when they are doing something special outside their normal duties has proven tremendously effective in making it memorable.

Frithjof Lund: Wolf, you mentioned at the start an acceleration of attacks. What will be the big cybersecurity threats in the coming years?

Wolf Richter: We see a massive professionalization as more organized crime discovers cyberattacks as a profitable activity. You need to expect attackers to be equipped with almost military-grade weapons. The large military organizations have invested heavily in building those cybertechnologies, and we have seen more than one event where one of these military-grade attacks had leaked out onto the dark net. It's like placing machine guns in the hands of burglars around the corner.

The big difference is that these digital machine guns are tremendously hard to control and extremely easy to replicate. This is simply code—coding tools that you can copy and share with others. On the other hand, the goal of many attacks we are seeing, particularly involving ransomware, is to make money, so at some stage there is a negotiation over the ransom. That combines cybercrime with good old-fashioned crime that police and private investigators have experience with.

Much is happening on the technology side as well. The shift to the cloud poses a whole new set of risks. While, by and large, the infrastructures of the large-scale cloud providers are much more secure than what most companies can impement in their own data centers, it is naive to believe that the cloud service provider will take care of all your security needs. On the contrary: we are seeing a massive increase in breaches of cloud-hosted applications for lack of proper configuration. Your IT department needs to acquire a new set of engineering skills to manage cloud environments.

John Noble: The cloud, as you say, Wolf, is a great opportunity, in particular to move off legacy infrastructure, but issues such as authentication remain your company's responsibility. It's very important that the board understands that however secure cloud service providers may be, the company still holds a great deal of the risk. And, sadly, we see some very large-scale breaches as a result of people simply not understanding how the cloud works.

Frithjof Lund: Do you have any advice for board directors on how they can stay on top of the battle against cyberattackers?

Wolf Richter: Any digitization program should have a cybersecurity budget. Companies need to drive digitization in a secure manner. Haphazard digitization just creates legacy infrastructure of the future, so you need to use best practices now in terms of secure coding, secure agile, secure DevOps. Companies need to make sure there is a security mindset across the whole life cycle.

John Noble: I don't think it is inevitable that companies will be compromised. There are opportunities to get this right and they are around recognizing the genuine threat. We are building national economies on something that is inherently unsafe—the internet—and we have to mitigate that by taking a series of measures. The board has to ensure that executive leaders are looking at both the worst-case and best-case scenarios and are prepared to make some compromises to ensure a secure infrastructure.

Frithjof Lund is a senior partner in McKinsey's Oslo office, and **Wolf Richter** is a partner in the Berlin office. **John Noble** is a senior adviser to McKinsey and a nonexecutive director on the board of NHS Digital, the national information and technology partner to the United Kingdom's health and care system.

Designed by McKinsey Global Publishing