ISTARI

UNIVERSITY OF OXFORD

Saïd Business School

The CEO Report on Cyber Resilience

Dr. Manuel Hepfer
Rashmy Chatterjee
Professor Michael Smets

03 • 2023

Illustration by: Kouzou Sakai

Contents

Executive summary

AUTHORS:

DR. MANUEL HEPFER
RASHMY CHATTERJEE
PROF. MICHAEL SMETS

COVER ILLUSTRATION BY:
KOUZOU SAKAI

> “Whenever I speak to a group of CEOs to share my learnings from the cyber attack, I start by saying ‘put down your phones for 15 minutes, you’ll want to listen carefully to what I have to tell you’.”
>
> CEO of a $4 billion U.S. company

Ask any CEO to name the issues that keep them awake at night and cybersecurity risk is likely near the top of the list – with good reason. With the accelerating digitalisation of business models comes vulnerability to cyberattack. And while spending on cybersecurity increases every year, so does the number of serious incidents. Even the largest and most technologically advanced companies are not immune.

CEOs must formally answer to regulators, shareholders and board members for their organisation’s cybersecurity. Yet the majority (72%) of CEOs we interviewed as part of our research said they were not comfortable making cybersecurity-related decisions.

Our CEO Report on Cyber Resilience draws on 37 interviews with CEOs of large global enterprises. It explores the role chief executives need to play in successfully managing cybersecurity risks.

The overarching takeaway from those CEOs is that they want to move beyond simply hardening their enterprises’ cybersecurity defences to creating cyber resilience: the ability to **anticipate**, **withstand**, **respond** and **adapt** to cyberattacks, with the goal of minimising impact, expediting recovery and emerging stronger.

Our interviews with CEOs reveal that this shift to thinking about cyber resilience requires fundamental changes in approach: how they think about cybersecurity (their mindsets) and how they act (their playbooks).

We explore four CEO mindset shifts that are required to build resilience. First, rather than thinking of themselves only as **accountable**, CEOs should think of themselves as being **co-responsible** for cyber resilience with their chief information security officer (CISO). Second, to build resilience, CEOs should move from a position of **blind trust** to **informed trust**. Third, CEOs should embrace what we call the **preparedness paradox**: our findings suggest an

inverse relationship between preparedness and resilience – the better prepared CEOs think their organisation is for a serious cyberattack, the less prepared it could be in reality. The fourth and final mindset requires that CEOs adapt their communication style to **regulate stakeholder pressure.** CEOs have to move flexibly and swiftly between the four styles – sometimes acting simply as a *transmitter* of information, sometimes *filtering* it, sometimes *absorbing* anxiety and pressure, and sometimes *amplifying* positive or negative messages.

> “
>
> Cyber is one of these long-term things that might not produce immediate results or, if you don’t do something, it produces immediate negative results. But on those things, the CEO should be more involved. The more something has a longer-term impact, the more important it is for the CEO to be on top of it. Like climate change, for example.
>
> ”
>
> CEO of a $4 billion U.S. company

Developing these four mindsets empowers CEOs to take action toward building cyber resilience. Our research provides a playbook outlining steps CEOs can take to anticipate, withstand, respond and adapt to cyberattacks. To anticipate, CEOs have to revisit traditional approaches to risk management, budget allocation, board engagement, strategy execution and the meaning of cybersecurity awareness.

When an attack occurs, the CEO enables the organisation to withstand the attack by making themselves available and acting quickly. To respond – keeping the business running in some form or another while recovering systems and processes – CEOs need to reinvent their organisational structure. And lastly, they have to foster adaptation, because they know that cyber resilience is not just about avoiding losses: it also can create opportunities and unlock better ways to run enterprises.

Introduction

> “
>
> We are a big company but this was life-threatening. You can’t produce, you can’t ship, you can’t sell, you can’t invoice, you can’t communicate with your employees and customers. We realised that we had no record of people’s phone numbers or any other way to reach them. So we were scrambling for hours that afternoon just asking, ‘Do you have the phone number of the general manager in Argentina? Do you have the phone number of this other guy?’ It took the entire afternoon to get a list of all the general managers and it was only that night that we had the first set of WhatsApp groups up. And then we basically ran the company for nine days on WhatsApp.
>
> ”
>
> CEO of an $8 billion European company

CEOs are beginning to change their views on cybersecurity. Whereas they once viewed it as an operational expense associated with IT management, they are now starting to see cybersecurity as a strategic risk to their enterprises. And a few executives, typically those who have managed their companies through a serious attack, are beginning to think of it as a strategic opportunity – a driver for value creation and innovation.

The CEOs we spoke with who endured a serious attack highlighted the agonies of making existential decisions based on imperfect information under extreme pressure. Some described it as the grimmest experience in their careers. They found themselves having to bring their businesses back from the brink of extinction, while navigating insistent pressure from shareholders, regulators and customers. They discovered that although their company had spent significant resources on technological defences, it often lacked basic forms of organisational resilience.

That is partly why we wrote this report. The impacts of a serious cyberattack go far beyond IT: they are company-wide, instantly global and, in some cases, deeply damaging to reputations and key stakeholder relationships. Managing cybersecurity risk and building resilience has become a core part of any CEO’s leadership responsibility. Yet, perhaps because it is a relatively new experience to live through, there is no playbook.

To fill that gap, ISTARI and Oxford University’s Saïd Business School, with support from Temasek, conducted an in-depth research project. Our guiding research question was: ***what is the role that CEOs play in managing cybersecurity risk?***

We conducted 37 interviews with CEOs of global corporations across geographic regions, of whom nine had experienced significant cyberattacks. They spoke with remarkable honesty about their feelings, frustrations and regrets. They painted a rich picture of what it’s like to lead an organisation in today’s “permacrisis” environment. Above all, their stories, successes and mistakes generated valuable insights that top executives can use to enhance their resilience toolkit.

Their overarching takeaway is in the title of this report. Enterprises today need to move beyond simply shoring up their cybersecurity defences to the more complex but critical task of building organisational cyber resilience. Meeting this challenge requires, above all, CEO leadership.

The changing view: From cybersecurity to cyber resilience

Cybersecurity risk continues to appear at the top of the World Economic Forum's global risk register and takes a similar position in most enterprises[1]. Attack vectors are multiplying. Attackers become more sophisticated every day. Cyber space is now a contested military domain occupied by a mix of state actors, intelligence agencies, hacker groups and private companies.

In their quest to gain advantages over competitors and capture value from digitalising operations and business models, organisations expose themselves to the perils of cyber space. To avoid harm, companies traditionally have relied on the idea of cybersecurity defences. But this is an overly narrow framing of today's cyber risk landscape, because it implies that always protecting the availability, integrity and confidentiality of computer systems and data is achievable. That simply is not the case. It also implies that a possible solution to the problem of cyber insecurity is purely technical in nature. Acronym-heavy language associated with cybersecurity is daunting for most business executives and creates barriers for understanding. For many of them, the path of least resistance is to delegate responsibility and understanding of cybersecurity to their technology teams.

Companies that have fallen victim to a serious cyberattack come to understand that attacks cannot be prevented, as one CEO recalled:

"I learned the clear truth that all CEOs must know: You can never stop a cyberattack, you just do your best to limit the damage. The idea that you could ever actually stop it is nonsense because sooner or later, something will get through."

CEO of a $4 billion European company

—

Evidence confirms that thinking: corporate spending on cybersecurity increases every year, but so do serious attacks. Even the largest and most technologically capable companies are not immune.

What matters in a digital world is resilience: an organisation's ability to anticipate, withstand, respond and adapt to cyberattacks to minimise impact, to expedite recovery and to emerge stronger. Still, CEOs report that they are often pushed in a different direction.

"The advisers were pushing us on backing up the data. Don't let it be breached or compromised; make sure you can recover if there's a flood, a fire, a destroyed building where one of the systems are located. But they didn't push us on how are you going to recover if it happens, when it happens? We were all into prevention and not enough into resilience and that's the mistake that we made."

CEO of a $4 billion U.S. company

—

Our core insight is that moving from cybersecurity protection to building cyber resilience requires a fundamental change of perspective, by which CEOs come to view cyber resilience as a top leadership imperative.

1) *The CEO Report: Embracing the Paradoxes of Leadership and the Power of Doubt*, Saïd Business School, University of Oxford, 2015

"The biggest change for me is that I now totally accept it can happen. And that doesn't sound like much but trust me, there is a fundamental difference in approach between organisations that accept it could happen and those that think they can repel it. Because if you think you can repel it, you do what we did before the attack, which is you have no adequate plans in place as to what you're going to do."

CEO of a $4 billion European company

Many of the CEOs who had personally experienced a cyberattack highlighted the importance of building cyber resilience. Recovery, to them, did not simply mean restoring data and IT systems. It meant organisational evolution. To achieve that, they emphasised the need to align cyber resilience with all of the company's other resilience efforts, such as cultural, financial, operational and strategic resilience.

Why is a cyberattack different from other crises?

Cyber is an emotive issue. That comes through loud and clear in the language our interviewees used. Those CEOs who had endured an attack recalled it as being "intrusive," something that caused people to "panic" and 'run around like headless chickens'. The CEOs described themselves as reacting "instinctively" and with their "gut".

A serious cyberattack is the ultimate corporate crisis: it occurs unexpectedly, creates high levels of uncertainty, and can threaten the very survival of an organisation.

But a serious cyberattack differs from other crises. Unlike, for example, a pandemic, an attack is malicious. It feels personal to be attacked, yet enterprises do not know who is behind it.

They happen fast and are global – the damage can be done within half an hour, crossing borders and jurisdictions, and affecting global operations.

They lack visibility – the theft of a machine from the factory floor is obvious immediately; manipulating the software that runs it might not be.

They are dynamic – sometimes it's an offensive-defensive grapple, involving negotiation and game theory-esque like speculation about the adversary's next move.

The predominant feeling is loss of control. And yet the CEO has to be a reassuring presence for all stakeholders.

Four mindsets every CEO should adopt

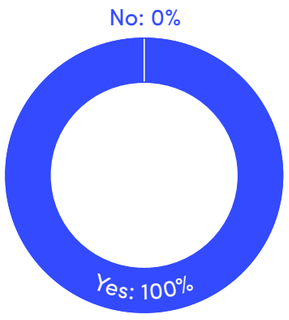
1. *Be co-responsible, not just accountable*

When we asked the CEOs in our study if they felt accountable for cybersecurity, all of them – without exception – insisted that they did.

> *"The buck stops with me. If anything goes wrong in cyber for whatever reason, customers will not excuse me because it is in an area I can say somebody else is looking after."*
>
> CEO of a $6 billion Asian company

But interestingly, we came up against a conundrum. While conducting the CEO interviews for this report, we also asked 37 CISOs who participated in ISTARI's executive education programme in Europe and America about their perceptions of their CEOs' accountability. Fifty percent of the European participants did not think that their CEOs felt accountable and thirty percent of U.S. participants felt the same.

Do you feel accountable for cyber resilience?



The likely reason for this gap in perception between CEO and CISO lies in the subtle but important difference between taking accountability and being responsible. Accountability is associated with ownership of mistakes after a crisis has occurred or with being "the face of the mistake." It does not, however, mean ongoing engagement and ownership of tasks, something people tend to associate with responsibility. The mismatch in perceptions seems to be a symptom of the perceived lack of engagement in cyber resilience.

One CEO comment lays out a critical mindset change that bridges this gap. Instead of CEOs seeing themselves as merely accountable, he suggests, they should consider themselves as co-responsible with their CISO.

> "I am what I call co-responsible. If you asked our CISO whether he feels responsible for cybersecurity, he will say very much yes. But I think it's important that we as leaders also feel responsible, not just accountable. You cannot delegate this to experts. If you don't feel responsible, then you don't get involved enough and then certainly I think this will weaken our resilience."
>
> CEO of a $4 billion European company

Co-responsibility requires doing much more than just being the public face of a crisis after it happens. It means taking action and playing an ongoing role to prepare for a cyberattack. It requires much closer engagement with the CISO and cybersecurity team, irrespective of reporting lines.

Another CEO stressed the importance of being proactive: *"Even if it's managed by experts elsewhere in the company, I see it as part of my job to assume responsibility and thereby know enough about it to take on such responsibility."*

The concept of co-responsibility is important for cyber resilience because it reframes the CEO's role as part of a continuous conversation, rather than taking blame after an attack. Sometimes the CEO takes the traditional role of sponsor and champion of the CISO office. At other times, particularly if there is an attack, they need to act as a shield *"to get everyone else off their backs."*

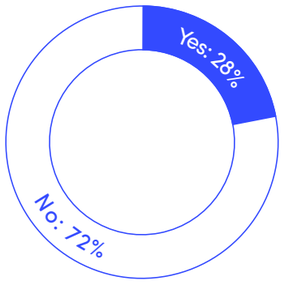
2. *Move from blind trust to informed trust*

Again and again, CEOs told us that they feel more uncomfortable making decisions about cybersecurity than in other areas of the business. In all, 72% of our 37 respondents declared "no" when we asked if they feel comfortable making decisions in the area of cybersecurity. What makes this particular decision domain so unsettling?

In part, the answer lies in the technical aspects of it, which seem difficult to comprehend for most business executives. But we found another related cause that came up repeatedly in our interviews: the nature of trust.

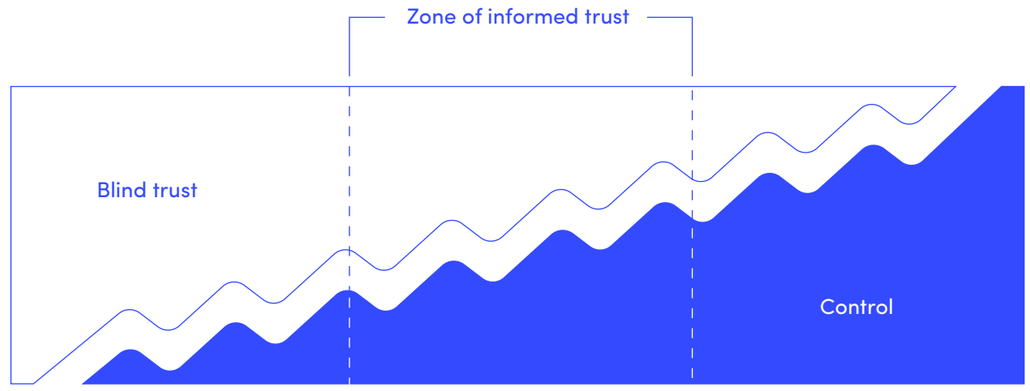
In any organisation, trusting others' expertise is something CEOs must do all the time. No one can expect to be an expert on every topic. As one interviewee put it: *"The first thing about being a CEO is you've got to have people around you that you trust. You trust them not only to do their job well but to come to you when there is a specific issue or when they need to check things with you."*

Do you feel comfortable making decisions in the area of cybersecurity?



On one level, that kind of trust applies to cyber. Our interviewees consistently talked about the need to trust their CISO and technical team. After all, as one CEO noted, *"that's the point in having them."* On the other hand, the technical aspects of cybersecurity, in contrast to more traditional areas (such as finance, marketing or operations), make the degree of trust required daunting. When a cyberattack unfolds, it suddenly puts the fate of the company on the shoulders of people who normally are much further down in the decision-making hierarchy. As the CEO of a $10 billion European company explained, *"At that moment of an attack, you put the company into the hands of supply chain people and IT people. And those are not groups you would normally, or intuitively, give that kind of confidence and trust to."*

The answer, many of our interviewees concluded, is to find ways to reinforce such essential trust by informing



themselves better before an attack occurs. Otherwise, as one noted, you end up, *"relying too much on the experts without being able to fully comprehend what they are talking about. There's also a risk of not knowing what good looks like and therefore there's all kinds of so-called cyber experts who at the end of the day will not give you what you really need."*

To become more comfortable making decisions in the area of cybersecurity, CEOs should move from blindly trusting their technical teams to a state of informed trust. CEOs who had experienced a cyberattack said that in hindsight, they wish they personally had known and understood more.

> *"You've got to be curious because the technology is constantly changing. You need a lot of humbleness. So you've got to be aware, you've got to ask questions but you've also got to have the humility to keep asking to learn."*
>
> CEO of a $10 billion Asian company

—

Another CEO told us something similar:

> *"The CIO came to present at an executive meeting and asked us how many servers we thought the company had. The lowest estimate in the room was four, the highest 250. The reality was more than 4,000. That was an incentive for all of us to understand more. We realised that we spend millions each year on this kind of technology but don't really understand it."*
>
> CEO of an $8 billion European company

—

One way CEOs can develop informed trust is by learning from their internal teams. After having to lead his company through a crippling cyberattack, a CEO of a large company ($80 billion in revenue) spent ten full days with his technology and cybersecurity teams simply to educate himself. The resulting learning curve, in turn, often leads to a change in behaviour.

> "The more I came to understand the way threat actors behave and the more I've understood about cyber, the more I've become concerned. I understand just how important it is for me and the leadership team to get right. It's not a technical matter – I mean of course it is a technical matter – but it requires direct attention from the people who are running businesses and building businesses."
>
> CEO of a $12 billion European company

Another way to reach a state of informed trust is to seek unbiased advice from external advisers who report their findings directly to the CEO – and to have formal and informal conversations with peer CEOs of other companies.

3. Embrace the preparedness paradox

During the interviews, we asked CEOs to rate their companies' preparedness for a serious cyberattack on a scale from one to ten. Only a few could be persuaded to give a number; many either dodged the question or openly said that they did not know.

On a scale from 1 to 10, how would you intuitively rate your organisation's preparedness to respond to a serious cyberattack?

"Idon't know": 10

Of those who responded, the majority rated their preparedness relatively high. And therein lies a problem. As it turns out, the CEOs with cyberattack experience acknowledged that they, too, had previously believed they were well prepared – before recognising their error in hindsight.

> "It quickly dawned on us how ill-prepared we were and how little we actually knew about the real risks of being hit by something like that. We did not understand how severe the risk could be. We couldn't even imagine it.
>
> CEO of a $5 billion European company

Paradoxically, our insights point to an inverse relationship between preparedness and resilience: the more prepared CEOs think their organisation is for a serious cyberattack, the less prepared it could be in reality. The reason? A misguided perception of high preparedness can lead to overconfidence and complacency, ultimately jeopardising the organisation's resilience.

The best way to approach the preparedness paradox is to embrace it: to think of preparedness not as an end state but as an ongoing set of activities and processes that continually challenge the organisation's preparedness.

> *"As a CEO, I have to try to get some understanding of how serious this risk is and I have to spend enough time digging into cyber risk to really understand how important it is to prepare for such a situation."*
>
> CEO of an $11 billion European company

—

By cultivating a mindset that constantly assumes under-preparedness, CEOs can encourage and challenge their organisations to increase their actual readiness. That means, for example, encouraging employees to overreport, instead of underreporting potential cyber risks (within reason), without fear of repercussions. There should be no fear of "crying wolf." Near misses or minor incidents should be seen as learning opportunities, not as an invitation to find and to punish mistakes. It also means staying on your toes and remaining alert, despite whatever trainings, simulations and war games have previously taken place. Perfection is the one thing never to assume.

> *"We've done war games to know what we would do if, God forbid, there was an attack. But it's never enough, because who the hell knows what could happen? Cyber is something that is so scary – it's extremely scary – and you just don't know what to do with it."*
>
> CEO of an $18 billion European company

—

As soon as a feeling of "ticking the boxes" settles in, alarm bells should ring.

> *"We have an enterprise risk management function. And cyberattack has been identified for a long time as one of our top 10 enterprise risks. But of course, in hindsight, what we had to realise was that we were just ticking the boxes. It's a risk, we have done some things to look like we are doing something about it but it was much more a box-ticking exercise instead of really understanding it."*
>
> CEO of an $80 billion European company

—

In short, organisations should always be ready, but never feel prepared.

4. Adapt your communication style to regulate stakeholder pressure

During a serious cyberattack, the spotlight is on the CEO. Uncertainty about the scale of the impact, where the attack originated and how quickly it can be resolved creates high levels of anxiety and pressure on the CEO. One CEO highlighted the need to "*get yourself to a place where you understand what both your internal organisation and the market is expecting of you.*" Shareholders are concerned about the financial impact; the board requests information; customers and suppliers want to know what is going on; and regulators are keen to investigate.

But even in the absence of a cyberattack, a core part of a CEO's job in building resilience is to deal with different – and seemingly competing – demands from internal and external stakeholders.

"I feel a sense of obligation to our stakeholders because they rely on me to ensure that we take this seriously and that cyber is an integral part of our strategy. So I feel the weight of responsibility to take a visible leadership role in making all our stakeholders see the importance of this."

CEO of a $35 billion Asian company

—

Interestingly, some regulatory environments are making CEOs personally responsible for cyber resilience. As one explained:

"We are considered part of critical infrastructure, which makes me personally liable for cybersecurity risk. And I don't have a choice. I don't like it, I don't think that is the way business should be run. But because the government has a very high standard when it comes to cybersecurity risk, it certainly has my attention."

CEO of a $3 billion Asian company

—

What makes the CEO's job in managing demands from different stakeholders even more challenging is that some stakeholders are not well-versed in cybersecurity themselves. One CEO gave the example of regulators:

"

Regulators are sort of off the charts concerning cybersecurity and they don't really know anything about it. They just know that they're afraid and then they're quite right to be because obviously, this is a thing that could bring down the system.

"

CEO of a $13 billion European company

Investors have started to pressure CEOs on the status of their cyber resilience efforts, sometimes at a surprisingly detailed level.

"Our largest shareholder will say, 'hey, what are you doing, why don't you have a chief security officer?' And I said, 'yes, yes, we'll find one.' Of course, they are extremely concerned about the reputation and risk to them because if we don't do well, it doesn't reflect well on them."

CEO of a $3 billion Asian company

—

All CEOs described reporting regularly to the board on cyber issues. Yet, those who had undergone a cyberattack revealed an additional complication: the need to manage their often intensely emotional response during an attack. As one CEO recalled: *"The board was sitting there panicking and just saying, 'we have to do this, what about this, have you got this?' But of course, it doesn't really help."*

Internally, the IT and cyber teams, which might see an attack as a challenge to their own expertise, need psychological safety and encouragement to convey the truth to the CEO. Without that, technical teams will default to either saying too little or too much before they know the facts. *"I began to be concerned about whether the IT leadership really did know what was going on or if they were not telling me the full picture,"* recalled one CEO. In contrast, another noted that his *"biggest problem"* was that his IT team kept overpromising: *"They would say, 'It'll be alright. In half a day, we'll be back.' They said it would be up and running on Friday morning and we got to Friday morning and plainly it wasn't going to happen."*

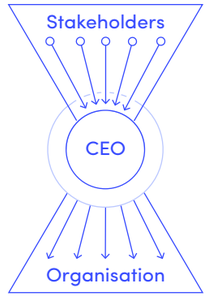
Balancing these demands and the pressure is, first and foremost, a communication challenge for the CEO. Although the specific demands seem to be conflicting or competing, what all stakeholders ultimately care about comes down to one thing – seeking reassurance from leadership about the organisation's resilience.

To balance these pressures, CEOs should adopt four different communication styles depending on the stakeholder and the situation.

CEOs may find themselves playing all four of these roles concurrently while interacting with different stakeholders, or they may switch roles depending on the situation and stakeholder. During a cyberattack, the speed of development and the number of stakeholders involved may aggravate the chaotic feeling. The art of the CEO's leadership is to be able to judge how and when to adopt each of these roles and to switch seamlessly between them.

Speak with the Author

Communication styles to regulate pressure from stakeholders, such as the board, shareholders, regulators, customers and suppliers

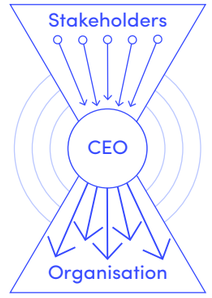


Transmitter

The CEO transmits pressure and demands to the organisation without any barrier. The transmitter is the most passive role that also feels the most comfortable to adopt. Many CEOs intuitively take on this position, delegating pressure, demands, understanding and responsibility on cyber to their organisation.

"

There was no filter between the IT people who were trying to work out what had happened and how they could fix it, and the executives and the board coming down on them, saying 'when is this going to be fixed? This is an IT issue, right? Can you fix it by noon? Because we need to go out and tell everyone. By 5 PM? By 10 AM?' A lot of pressure was being put on the IT team. So, the IT team, as you are when you are faced with such full force, just said 'okay, okay, this will be ready by tomorrow. We'll stay in our corner and fix it.' We then issued communications on the back of that saying 'this is a little blip, there has been an incident, it will be back up and running by 12.' And we would miss that deadline. And then at 5 PM. And we would miss it. And then 10 AM the next morning. And we would miss it.



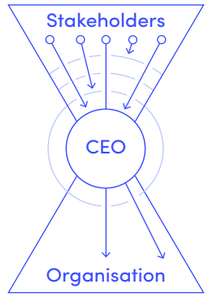
Amplifier

The CEO amplifies the power of messages and information. This is especially important in times when pressure from other stakeholders is low during day-to-day operations, or when new risks emerge. By amplifying these lower levels of pressure, CEOs can create a sense of urgency, further embracing the preparedness paradox.

"

When people went to work from home and they took their machines home, we needed them to download a particular new software which they had to download themselves. We had to make them aware that they have to do it in the next 24/48 hours. Making a hundred thousand people across the globe do it with discipline requires communication, so I made a video – because all it takes is one person making a mistake and the whole company's reputation could be at stake.

"



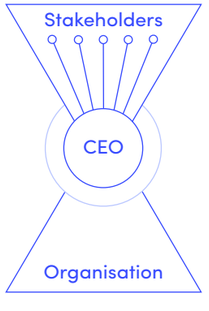
Filter

The CEO judges what kind of pressure to transmit or to absorb. In doing that, the CEO decides who needs to receive what information and distributes it. This role is crucial to helping people and teams maintain focus, especially in the aftermath of an attack, when uncertainty and a stream of new information can cause people to become distracted.

"

I would get formal reports from the IT team and our consultants twice a day. I would have an executive meeting in the morning and I would then have a board meeting. I'd report to my board on a daily basis because they wanted a report of what was going on. So, I put all of that in place and then I systematically started doing my best to speak to offices or groups of people.

"



Absorber

The CEO does not pass on stakeholder pressure but absorbs it. This role is particularly important during a crisis, when emotions and anxiety are high. Interviewees described being a shield for their organisation, absorbing panic from the board and acting to reassure both internal and external stakeholders while not feeling confident themselves.

"

"Publicly I always had a plan and I was focused on people following the plan. But privately I was suffering because you're carrying everyone else's fears. Everyone else in your room is going, 'I'm worried, I'm worried, I'm worried.' So I had to say, 'it's okay, don't worry.' You carry all of that burden alone as a CEO, you just have to. Then when you actually get home at night, you're still dealing with it, without sleeping, because people need you all the time. It felt like someone was consistently reaching inside of me and pulling my guts out. It was the worst situation I've ever faced in my career."

"The following day after the attack I set up a town hall at our headquarters and I opened it by saying: 'You may be aware that we have been hit by a serious cyberattack that has shut down all of our global operations. I want to emphasise that this is not the fault of our IT team. They are putting in heroic efforts to help us get back on our feet again. If you see anyone from IT walking around the corridors these days, give them a hug."

"

A CEO's playbook for building cyber resilience

No CEO comes to work in the morning expecting a cyberattack, so when it happens it feels surprising and random. But in reality, no organisation is immune, and cyberattacks are "predictable surprises" to which any organisation can fall victim.

CEOs play a critical role in building cyber resilience – the ability of an organisation to anticipate, to withstand, to respond and to adapt to cyberattacks. The goal of cyber resilience is to minimise impact, to expedite recovery and to emerge stronger.

To achieve these goals, CEOs can contribute with a specific set of actions. From the interviews we conducted, we distilled the rich, lived experiences from the CEOs into actionable insights within each of the four stages of cyber resilience noted above: anticipate, withstand, respond, and adapt. The sections below outline tactical, operational and strategic best practices for CEOs to build more cyber-resilient organisations.

Anticipate – by revisiting existing approaches

Anticipating means having the awareness to correlate changes in the external environment to their likely impact in the cyber domain, and then to take action – before a cyberattack occurs. Our core insight here is that the domain of cyber resilience requires CEOs to revisit traditional approaches that are common in other business domains. Revisiting means questioning previously held assumptions and acting on new ways of thinking. To anticipate and to build cyber resilience successfully, CEOs need to revisit their existing approach to risk management, budget allocation, board engagement, the meaning of culture, and strategy execution.

Revisiting risk management

Cyber risk is different from other risks in two ways. First, cyber risks are not confined by geography, department or physical location but can materialise globally; second, this can happen instantaneously. The combination of these two factors makes assessing cyber risks more challenging than assessing other enterprise risks.

CEOs answering our questions about risk fell into two main camps. The first group talked about cyber risk as just one among many other risks their organisation faces, and described rational formal processes for categorising and assessing all of those risk factors:

"We measure our risks at a granular level. We have 52 risks that we monitor and measure and these are divided into 11 risk categories. Out of these 52 risks, 27 are quantifiable; the others are qualitative. It is really the strength of our risk systems that allows us to run this business efficiently, effectively, be on plan, be on budget, be on time."

CEO of a $35 billion Asian company

—

One CEO described "*getting a sheet saying what is the likelihood of these cyber risks materialising, what is the impact if they actually materialise,*" suggesting a relatively hands-off approach on their part. This approach – confident that you have a strong risk system and that you know what the risks are – is potentially perilous, as it could lead to complacency.

The second group was much more open about not knowing how to assess the risk and described the urgent need for the CEO to "*spend enough time digging into cyber risk to really understand how important it is to prepare for such a situation.*" Although not every CEO in this group had experienced a cyberattack, those who did responded to the question of risk in a similar way:

"I find it really hard to assess the likelihood and impact of a cyberattack because the people who you employ to counsel you on this don't underestimate it, let's put it that way. So you get a lot of stuff about how it's just a racing certainty that, within a short time, you'll get an attack and you need to spend a lot but that'll never be enough. So, you get all of this stuff really thrown at you. The honest answer is that I found it very hard to assess. Obviously, it keeps you awake at night, because arguably nothing could damage the business more. How likely do I think it is? I really don't know."

CEO of a $3 billion European company

—

An additional factor that makes assessing such risk difficult for the CEO is a suspicion that the cybersecurity team and/or professional advisers can exaggerate the risk of an attack in order to extract more budget or consultancy hours. One CEO was explicit about this:

> "Everybody comes and scares the hell out of me. They told me 'you should be very scared.' I said 'I'm already very scared, what do you want me to do?'"
>
> CEO of an $18 billion European company

One way to avoid an empty box-ticking exercise is to focus on a few key questions about cyber risk. Specifically, CEOs should ask themselves:

- Am I confident about the risk capacity and appetite of my organisation, specifically in the context of cyber risk?
- What are our three to five most critical business processes? What technology underpins them? How vulnerable is each to a cyberattack?
- Can we quantify the most likely and impactful cyber risks?

Revisiting budget allocation

Years ago, chief executives saw investment in cybersecurity as a lose-lose situation. If their company was attacked, they would lose reputation and profit and the upfront investment in cybersecurity had proven ineffective. If their company was not attacked, investments in cybersecurity would be seen as wasted and warnings unduly alarmist.

Today, that seems like yesterday's wisdom – CEOs are starting to revisit their approach to cybersecurity investment. The CEOs we interviewed rarely viewed cyber resilience as an area of operational IT expense ripe for cost savings. Instead, several gave the impression that they are willing to allocate an unlimited budget to cybersecurity with one noting, *"we don't consciously limit our cybersecurity budget."* Another CEO added: *"I give my CISO whatever he wants."*

One, who is founder and CEO (and thus is spending his own money), observed:

> "I have a lot of say in how things are in my company and what I've told my CISO is that you've got an open budget, whatever you need, just do it. Of course, he comes back to ExCo for approval on expenses and projects, but for me there should be no imposed limit.
>
> CEO of a $2 billion U.S. company

Another CEO described what happened in 2020 amidst the uncertainty of the pandemic:

"We had a series of cost-reduction initiatives, so that if the net market and the capital market seized up and froze up, we could operate. The only function – there are 18 functions in the company – the only function where I did not cut budget but increased the budget was cybersecurity. Every other function, such as HR, manufacturing and sustainability, everybody had to reduce cost; the only one that we didn't reduce cost was cybersecurity."

CEO of a $35 billion Asian company

—

One respondent noted that, to a certain extent, today's largesse may be down to his lack of knowledge, admitting, *"look, the problem is that I'm not in a position to really say no."* Even if the pendulum has swung toward erring on the side of over-investment, the challenge remains for most CEOs to strive to make sure that they are spending enough but not wasting money ("*spending smartly*," as one put it).

CEOs should ask themselves:

- *Are we spending our money on the right things?*
- *Are we spending the right amount of money?*

Revisiting board engagement

Engaging the board has long been an important part of cybersecurity. Although members of the board do not have day-to-day management responsibilities, they have oversight and fiduciary duties. In many companies, the focus of the board and that of the cybersecurity teams diverge: the board is concerned about business risk, continuity and reputation, whereas the cybersecurity teams tend to concentrate on the technical, organisational and operational aspects.

By assuming co-responsibility, the CEO plays a role in bridging that gap, which starts by engaging the board on cyber resilience.

> *"I sit on the board and the issue of cybersecurity had never been a top priority until the attack that we had. It's not that people had never heard about it or had no idea. But in general, it's something that, as with IT in a lot of companies, as long as everything works, there are no questions and then the focus goes onto other things. From the discussions I have had with fellow CEOs, that's no longer the case, not just among companies that have been affected but also among those that have simply witnessed or heard about it. That has inspired all of them to take more affirmative action to put it higher on the agenda."*
>
> CEO of an $8 billion European company

Instead of simply adding cyber to the general risk oversight requirements of corporate governance, CEOs who had experienced an attack highlighted a bi-directional way of engaging the board outside the formal governance structures. Rather than just reassuring the board or reporting measures or progress to them, they advocated for education and active engagement. One CEO described how he created and now chairs a quarterly cybersecurity advisory forum, to which he invites members of the board, his management team and the cybersecurity function. The forum lies outside of formal governance processes – it is supposed to be a safe place to learn and exchange ideas:

> "Because it's outside of the formal governance channels, it's okay to ask dumb questions. We're not there to satisfy a board obligation. The board is there because they want to learn, the management team is there because we want to learn and contribute."
>
> CEO of a $13 billion U.S. company

CEOs should ask themselves:

- *How can I prepare my board so they know their role in the event of an incident?*
- *How can I create a safe space for the board, management team and cybersecurity team to engage and learn from each other?*

Revisiting the meaning of cybersecurity awareness

CEOs know that cyberattacks often are the result of human error, and our interviewees were unanimous in believing that building cyber resilience is a whole-company effort. Cybersecurity awareness is a good starting point and CEOs play a role in raising it within the organisation.

> *"You need a company culture that takes cyber seriously. We have very clear rules on the dos and don'ts. We really try to encourage people to understand what it means to do something stupid and we need a culture that understands each of us has a role to play and that each of us can make the whole system less secure if we violate all good practices in how you talk about confidential matters, how you use your technologies, how you avoid all the things that these e-learnings tell you not to do."*
>
> CEO of a $4 billion European company

When cybersecurity awareness standards are not met, one CEO highlighted that you need to walk the talk:

> *"I come down heavily on divisions with staff that do not meet the standard of the awareness of cybersecurity. And I personally decide on the people who consistently fail awareness tests – the repeat offenders. I have a very detailed interest in our cyber KPIs."*
>
> CEO of a $6 billion Asian company

Another echoed that:

> "When we have a phishing attempt or when there's an unusual threat actor or an identified gap in some of our software allocations, I'm very likely to go five or six levels down in the organisation and ask questions."
>
> CEO of a $13 billion U.S. company

However, to build cyber resilience, we found that CEOs need to revisit their approach and adopt one that goes beyond simply building cybersecurity awareness. That directive was highlighted especially by those who had endured an attack. Although enforcing awareness drives compliance, it does not lead to cultural change. Annual cybersecurity awareness trainings, for example, rarely lead to the lasting behavioural and cultural change that is critical in preventing and responding to a serious attack.

The most important task of the CEO in developing a truly cyber-resilient culture is to create the right attitudes, behaviours and feelings, and to anchor them deeply in the minds and processes of the organisation. These can range from forging a feeling of psychological safety that encourages people to voice doubts and deliver bad news amid the pressures of a crisis to fostering a willingness to step out of comfort zones and work across traditional functional lines and roles when necessary. One CEO mentioned that they purposefully chose one particular country as the centre for crisis management, because of the location's crisis culture. Another CEO explained:

> *"Your culture has to be where people are resilient. That is about their mindset, their agility and their ability to actually handle pressure. In our case, we were very fortunate to have people who were totally dedicated and willing to actually work beyond their immediate area of responsibility to help each other out. It's not just sticking to your job, it's about actually being able to, at short notice, cross-train and be there to reinforce an area where we are most vulnerable at a particular point in time."*
>
> CEO of a $3 billion Asian company

CEOs should ask themselves:

- *What can I do to drive our cyber awareness as a first step?*
- *How can I foster a culture that contributes to organisational resilience in the wake of a serious cyberattack?*
- *Do we have a culture in which people feel comfortable speaking out, voicing doubts and delivering bad news – especially in times of crisis?*

Revisiting strategy

All CEOs emphasised the importance of having a cyber strategy.

> *"We are scrutinising every other CapEx that is going into the accounts and we have to prioritise all the time but I think the importance of having a cybersecurity strategy cannot be underestimated."*
>
> CEO of an $11 billion European company

Strategy traditionally focuses on creating superior performance through competitive advantages – doing things better than others. But building cyber resilience requires revisiting that fundamental assumption of strategy. In the field of cyber resilience, gaining advantages over competitors is the wrong objective. Although opportunities in the cyber domain exist (see the section on "Adapt") they should not primarily be used to gain an edge over competitors, especially not if that leads to actions like withholding timely insights on shared vulnerabilities.

Many of the CEOs we spoke to saw cyber resilience as a domain of non-competition between companies – one where companies work together for a greater good and compete collectively against malicious actors. Instead of competing against others in cyber resilience, they compared themselves to who they were yesterday.

> “I think the nature of the cyberattack is there but for the grace of God. So most people didn't see it as 'it's great to see a competitor disabled.' I think it was a case of 'next time, it might be us, so we're actually going to be supportive.'”
>
> CEO of a $4 billion European company

“Lots of customers, suppliers and even our competitors actually offered to help. Their CEOs reached out to me, because when you see such a situation at a different company then you automatically think, 'it could have been me.' We borrowed software engineers to help rebuild our state.”

CEO of an $80 billion European company

—

The main mechanisms in pursuing a rethought strategy of collaboration are sharing information, best practices and lessons learnt from attacks. This can and should occur at all levels in an organisation, including peer-to-peer learning among CEOs.

"Cyber is not a competitive issue. In fact, it's one of these things where companies are faced with a similar threat but it shouldn't be competitive at all. You might think that when your competitor is hit it is going to help you but that's a very short-term view. So there are a lot of discussions between CEOs on where you are, what you are doing, what you see, how you solve these things.”

CEO of an $8 billion European company

—

CEOs should ask themselves:

- How can I facilitate collaboration with suppliers, customers and even competitors in driving collective cyber resilience?
- What support can I give to other companies that are under attack?

Withstand – by acting swiftly

Sometimes the computer screen turns black. Sometimes it is a phone call, informing the CEO of anomalous activity in the computer networks. But the cause is the same: a cyberattack.

At first blush, it might seem there is little a CEO can do once an attack has occurred. Certainly, at a technical level, any CEO's abilities are limited. This CEO of a $4 billion U.S. company captures that sense of helplessness. *“I was having dinner with my family on a Saturday night when one of my team members called me and said we're under attack,”* he recalled. *“Within half an hour, we stopped the attack and in the next 10 minutes shut down the entire system. But the damage had already been done in those 40 short minutes.”*

Although the operational damage to the IT systems might *“have been done,”* in reality, the overall extent of the damage to the company is not yet determined at that point. What matters to the organisation financially and reputationally is how the company is able to respond and to adapt afterward. Actions in the early hours after an attack becomes known set the enterprise up for success or failure in its response and resilience efforts. Organisations that respond poorly to an attack accumulate losses that far exceed those of firms showing no signs of poor response.

It may sound obvious but the first and most powerful action that CEOs can take when informed of a cyberattack is to make themselves available. One of our interviewees described having just flown to a major conference when they received the phone call: *“Because I didn't know what was going on that Sunday morning and evening, I took the red eye back east and skipped the conference so that I could help manage and supervise and be available to make decisions around what happened.”*

In the initial phase following a cyberattack, that process is nsified and accelerated. Interviewees who described their experiences conveyed the sense of pressure piling on the organisation – and thus on the CEO. In such an environment, there is little time to reflect and plan before acting, so CEOs rely on their instincts.

The following story of the CEO of a large European multinational who endured a cyberattack vividly captures the importance of taking the right actions in this critical initial phase — and its impact on enhancing or diminishing shareholder and stakeholder confidence.

CEOs should ask themselves:

- What can I do now to prepare myself so I can act swiftly and decisively in the first hours of an attack to avoid losing valuable time?
- What can I do now to anticipate and shape the response from our stakeholders and shareholders?
- How can I quickly activate the appropriate crisis management team with the right team members?

The story of a CEO who endured a cyberattack

“My CIO called me while I was in my car on the way to the office. Once I got there, I saw handwritten messages at the headquarters that said 'don't touch or start your computer, we are experiencing a cyberattack.' Shortly after I started to understand that this is a really heavy attack and also global – company-wide.

I was happy that we had already prepared for general crises, as we had a couple of incidents previously and we had also done exercises for the corporate emergency team – but we never had exercises on such an event. Funnily, the internal communication was more difficult than external communication because externally, we had journalists that could help us to disseminate our messages. But internally, of course, it's important for us to get access to the people working around in the different locations around the world.

We established the corporate emergency team immediately and the head of the corporate emergency team was the CFO. As the CEO, I needed to make sure that we have an overview of the situation. So I had meetings with the business unit managers, the EVPs that have responsibility for the operations in 35 countries in the world. But I also had to make sure that we could allocate resources to keep the operations running as much as we could in this difficult situation.

We decided very early that we were going to be completely open and transparent about it. Because the hackers demanded a ransom, I talked to the legal counsel and we had a meeting in the management team and we agreed that we were not going to pay anything. We didn't know if it was one single attack or if something else could happen later. You never know, even if you pay, there could still be problems in the system. I talked to CEOs afterwards who also had heavy attacks and they paid money to continue operating.

We also were very suspicious of everything that happened around our IT systems and even outside our headquarters. I remember, we noticed a person with a computer was sitting outside the head office and we brought him in and interviewed him on what he was doing. It turned out that it was a student who wanted to enjoy the nice weather outside his home. There was another case: two tourists were also walking outside the head office and we had to bring them in, interview them and it turned out they just didn't find their way to the city centre. So we were really suspicious. In one of our production plans, one of the programmable logic controllers exploded and we were discussing if the attackers had been able to come into that level of our systems. And of course, later it showed that it had no link at all but in this situation, you get really suspicious.

I had meetings with our country's minister of IT and we had good support from the police. We were informed that some of the best competence of batting off cyber attacks is in another country; so we asked for support from there. So I think we got the resources in place fairly quickly and started very constructively.”

Respond – by reinventing the organisation

Once the initial dust of the first hours has settled, many companies make the mistake of trying to draw a line under the attack and IT engineers are eager to work on solutions as fast as possible. However, our research shows that it pays to pause. Many CEOs who have endured an attack told us that jumping to conclusions too quickly will often lead to setbacks.

> We had more than 100 people working day and night, sleeping and eating in the office. After four days, we were feeling good. We had recovered most of our applications and wanted to start them the following day when we realised on day five that the attackers had cloned some administrator accounts that we had also recovered. This meant we were back to square one and had lost almost one week. We ran too quickly. So we paused, created a plan, upgraded our technical advisers and restarted our recovery efforts.
>
> CEO of a $5 billion European company

CEOs who have endured a serious cyberattack know that the worst part is not on the first, second or third day. The worst part comes after the first week, when the realisation settles in that this is not going to be over anytime soon. The first days are usually a sprint – when crises hit, employees want to work extra long hours and over the weekends with little sleep to help the organisation get back on its feet. But after the first few days, this hyperactivity takes its toll on people.

Reinventing the organisation

The CEOs we interviewed highlighted the importance of organisational agility: to reinvent the organisational structure so that it supports enduring response efforts. Our research suggests that an effective action plan is to divide the response efforts into different workstreams. For example: one workstream conducts a forensic analysis of the attack vector; the second workstream concentrates on recovering systems and processes; and the goal of the third is to keep business operations running as well as possible. Each stream works independently, without worrying about the progress of the others. In addition, our interviewees advocated for a shift system within each workstream, such as three six-hour shifts, with one-hour handovers at the beginning and end of each shift. Such an organisational structure might seem cumbersome to set up on the first or second day but it will pay off after a few days.

A cyberattack often leaves frontline workers and other employees without access to technology, preventing them from conducting their work. Instead of sending people home, some CEOs have kept their business running by decentralising decision-making authority. One CEO said: *"One thing I did that was very important was that I went out globally and told employees to focus on what customers needed without waiting for top-down instructions – we'll accept the cost. Do whatever you can for the customer and we will clean up the mess afterwards."* Those employees who are truly unable to conduct their normal work can be used to set up a customer service team, dedicated to informing customers and suppliers. Alternatively, they can spend their time conducting team-building workshops that do not require technology. One CEO said that *"keeping the company running as best as we could in such a crisis was quite important."*

CEOs should ask themselves:

- How will my organisation adjust in case it has to respond to a serious cyberattack?
- How can I reinvent my organisation now so it is prepared for a potential prolonged period of cyber crisis?
- Will frontline workers and employees across the business do what is right for our customers?

Reconciling conflicting business priorities

Beyond ensuring such structured systems are in place, another vital job for the CEO in the response phase, according to our respondents, is prioritisation of efforts and allocation of resources. For example, when systems and applications need to be recovered, at some point there will be a question about which servers, data or applications should be recovered first.

Ideally, the most critical business processes should be determined upfront to avoid last-second discussions about which functions take priority. But even when that has been done, the dynamism of some cyberattacks requires the CEO to make crucial decisions about a range of resource allocations. In such cases, having already defined the three most critical business processes (and the key here is thinking in terms of business processes, not IT systems) saves time and energy.

> We had 1,000 managers around the world screaming and shouting that their business process or application is the most important. And we had to have someone who decides what goes first and what can go second.
>
> CEO of an $80 billion European company

CEOs should ask themselves:

- *What three to five most critical business processes should we prioritise in our response and recovery?*
- *Have I defined principles that guide organisational response – such as: employee safety first, customer success second, shareholder returns third?*

Communicating

Finally, a critical role of the CEO is to take the lead on communications after an attack.

> Communication was a bottleneck and there was an enormous need for information: internally for me and for my team but also externally quite a lot of press and journalists pressing us from the outside. They wanted to have information. And as a big company, it was all over the news channels.
>
> CEO of an $11 billion European company

The tendency of many companies is to keep the attack under wraps. Although some cyberattacks reach a level of sensitivity that makes transparent communication inappropriate, most of the CEOs we interviewed were in favour of open and transparent media communications for two reasons. First, as one noted, *"I thought that our customers have the right to know because they should be able to make decisions on that basis. And they truly appreciated that and even offered to send help."* Second, keeping an attack that has a company-wide impact a secret is difficult. We came across examples of employees tipping off outsiders or posting about the attack on Twitter. Being proactive in media communication helps shape the narrative around the story and can protect the company's reputation.

CEOs should ask themselves:

- *If normal forms of communication are disabled, how can I communicate with my management team and the entire organisation?*
- *Am I willing to be open and transparent about the attack to the media, customers and shareholders?*

Adapt – by capturing opportunities

Cyber resilience is not just about avoiding losses – it can also create opportunities for value creation. This can mean capturing operational opportunities by changing outworn business processes, exposing previously unnoticed weaknesses, and uncovering new strengths. It can also mean capturing strategic opportunities to build stronger business foundations for the digital era, or discovering ecosystem opportunities that help uplift the resilience of an entire industry. Adapting, therefore, does not happen solely after a cyberattack has occurred – it should happen before, during *and* after.

Operational opportunities

Finding operational inefficiencies is a good place to start.

> *"We used to have 350 system administrators, which we now have reduced to 150. We also used to have more than 1,400 applications, which we want to get down to 400 or 500. I now use the same rule for cyber and IT in the company that I use with my family at home when it comes to our basement: anything that we haven't touched or used for a year can go."*
>
> CEO of a $5 billion European company

When done well, eradicating these inefficiencies can help pay for increased investment in cyber resilience, as this CEO further explained:

> *"We are trying to offset our cyber budget increase by reducing inefficiencies in our operations: for example, the 30% fewer servers, merging all of our active directories into three, or combining three versions of our ERP system into one. All of these custom-built solutions we had are great, but in a cyberattack, you need experts for each specific custom-built system."*

That kind of benefit stems from top executives getting deeper into the tech weeds and serves as an example of the mindset shift from blind to informed trust noted in an earlier section of the report. One CEO recalled that he should have been more focused on the details, *"for instance, how many servers and applications we have, which antivirus software we're using or the fact that we don't have a register of all our hardware."*

CEOs should ask themselves:

- *Are we suffering from operational inefficiencies that, if eradicated, can save us money and make us more resilient?*
- *How can we standardise our technology landscape while making it more resilient?*

Organisational opportunities

Cyber resilience efforts can be used as a diagnostic tool to eradicate other organisational weaknesses and capture organisational opportunities. One CEO noted: "*We saw this as an opportunity for closer integration and understanding between business and IT. Even in HR, people now better understand how time is tracked and how wages are paid at the end of the month.*"

The opportunities extend to rethinking leadership and team composition. "*One of the things this attack showed is where you have strong leadership and weak leadership,*" recalled the CEO. "*We had a feeling of this already before the cyberattack but it highlighted explicitly those pockets of weakness.*" Another CEO noted that there is no need to wait until a crisis hits to focus on teams and people. As part of mending the roof while the sun is shining in the pre-attack phase, they admitted that in hindsight, they should have listened to their gut sooner.

> "I've heard this before and never really believed it but the attack made me realise that we have significant inefficiencies that cost us money. I learnt that through the lens of cyber, you can achieve big cost-saving opportunities. And you're plainly stupid if you're not capturing them, because they save you money and make you more resilient."

> *"Was I happy with the management team I had before the attack happened? The answer is no. But I didn't do anything about it. I wish I had. Not because it would have prevented the cyberattack but because I think I would have gotten to a resolution quicker. We wasted two or three days by people just telling me stuff that wasn't right. Many people think a lot about technicalities and buying systems and patches, but honestly you've got to have the right people and I hadn't focused on that."*
>
> CEO of a $4 billion European company

CEOs should ask themselves:

- *Do I have faith in my team to manage our company through a serious cyberattack?*
- *What do I need to do to create a team that will perform well during a cyber crisis?*

Ecosystem opportunities

A major cyberattack often ripples across industries. But even with a single attack, no one is safe unless all are safe, because many companies rely on a relatively homogenous IT infrastructure irrespective of industry. Companies can be hit as collateral damage, even when attackers do not target them directly. As a result, the CEOs we interviewed highlighted the importance of working together, even at the highest level of decision-making:

> Once the attack was over, I went to see the CEOs of some of our biggest customers to tell our story and to share lessons. They immediately said they need to do a small workshop to act on our lessons and enhance their preparedness and resilience.
>
> CEO of a $4 billion European company

Another CEO strongly agreed: "*On these types of severe risks, in order to know them well enough, you need to work together with others that are best-in-class.*"

Learning and best-practice sharing shouldn't be limited to specific industries, the CEO continued:

> If a totally different company in a totally different industry has the experience of something that almost took them out of business, we should pay attention and think that there is maybe something to learn.
>
> CEO of a $4 billion European company

CEOs should ask themselves:

- *With whom in my ecosystem can I work to become more cyber-resilient?*
- *Can I invite someone to hear the lessons learned from companies who have successfully built cyber resilience?*
- *With whom can I share my experiences of managing cybersecurity risk, or dealing with an attack if I have endured one?*

Speak with the Author

Final word: The voice of experience

Our goal with this report was to share the successes, mistakes and lessons of how 37 CEOs manage cybersecurity risk. Most of their experiences and personal stories have not seen the light of day for fear of attribution or repercussion. Our promise of anonymity allowed us to get to the raw, unfiltered thinking of these CEOs, or as one put it, *"thoughts that I have so far only shared with my spouse."*

Another goal was to offer recommendations that would help CEOs and their organisations build cyber resilience. With that in mind, we have shared both what has and what has not worked for these CEOs, ideally helping others avoid some of the pitfalls they suffered. In every interview, we asked two specific questions – "What piece of advice do you have for your peers?" and to those who endured a serious cyberattack, "what do you wish you had known?" All were keen to share their advice.

Instead of distilling their responses, we have chosen to give the CEOs the final word themselves – unfiltered.

"Invite someone in who has had that experience with an attack. Start with the mindset that if you don't take this seriously, your company might well be taken out of business one day. I know most people, even myself, without having had this experience, would not take advice like that at face value. For most companies like ours, it's a top-10 risk but I had not in my wildest dreams imagined that we could have been so close to not making it as a company. I don't think a lot of CEOs are thinking about cyber risk that way – they think about risk as something that has an impact and should be mitigated. But there's a hell of a difference between thinking about risk that could cost you money or reputation and then something that could cost your company its life."

CEO of an $80 billion European company
—

"In such a crisis, you've got to have that outward show of confidence and get your board in the right place because boards are desperate to hold people to account all the time. But that wasn't the right time to start holding anyone to account over anything."

CEO of a $4 billion European company
—

"You should not just rely on your technology team telling you that everything is okay. Just like you have audits in financial accounting, you need someone independent to tell you the state of play. You'll want unbiased advice."

CEO of a $5 billion European company
—

"Give people space and take the panic away from them, they'll start closing up and not telling you the truth. It's a big psychological game. You have to inspire confidence, you've got to be consistent, you've got to give people the space and time, you've got to make sure they don't feel they're to blame. Your job as CEO is a human job. The technical bit, there's nothing you can do about that as a CEO."

CEO of a $4 billion European company
—

"Share your experience with companies to warn and help them build resilience. And if someone is hit, reach out immediately and offer your experience and IT people. When we were hit, lots of other companies and even our competitors reached out to offer help and send resources. Cybersecurity is certainly one of those areas that is not a competitive space. Today it's them, tomorrow it could be us and we feel the best way on a topic like this is to realise that we are strongest and most resilient together."

CEO of a $10 billion European company
—

Five provocations to keep in mind

1. Don't ask what your cyber team can do for you. Ask what you can do for your cyber team.

2. Don't just rely on your technology team. Get independent, unbiased advice.

3. Don't compete with other companies in the domain of cyber. Instead, compare yourself with who you were yesterday and collaborate with others – even competitors – to become stronger together.

4. Don't let budgets bottleneck progress. Instead, focus on where you can allocate resources most wisely to achieve a reduction in risk and an increase in resilience. Don't spend $1 million to avoid $10,000 in damages. Spend $10,000 to avoid $1 million in damages.

5. Acknowledge that even you have limited power to get the organisation on board. Even with your backing, getting support and understanding from business units across the organisation is challenging. But without your support, it is close to impossible.

Speak with the Author

Method & sample

37

–
CEO interviews

1h+

–
In-depth conversations

$12bn

–
Average revenue

Highest $80bn
Lowest $0.1bn

40k

–
Average number of employees

Highest 200,000
Lowest 500

8 Years

–
Average tenure as CEO across companies

9 CEOs

–
Experienced an attack

9

–
CEOs from the USA

15

–
CEOs from Europe

13

–
CEOs from APAC

About the authors & acknowledgements

Dr. Manuel Hepfer

Speak with the Author

Manuel is the Head of Knowledge and Insights at ISTARI and a Research Affiliate at Oxford University's Saïd Business School. Before joining ISTARI, he completed a PhD in Cybersecurity and Strategic Management at the University of Oxford. His research won several awards, appeared in academic and practitioner journals, such as MIT Sloan Management Review, and was covered by the Financial Times.
Email: *manuelhepfer@istari-global.com*

Rashmy Chatterjee

Rashmy is the CEO of ISTARI. Rashmy has held several global sales and marketing leadership roles in her career. She spent over two decades at IBM, where her most recent positions included global sales leader for IBM Security and Chief Marketing Officer for IBM NA. Rashmy is passionate about building a culture of long-term client relationships and developing talent. She advocates for women in technology and is a member of several boards, including most recently that of Allianz SE.

Email: *rashmychatterjee@istari-global.com*

Professor Michael Smets

Michael is a Professor of Management at the University of Oxford's Saïd Business School. He studies CEOs and senior leaders in corporate, professional and public sector organizations. His work focuses on their leadership development and delivery of large-scale (digital) transformations. Michael regularly contributes to Oxford Saïd's flagship leadership programmes and speaks at academic and practitioner conferences. His research is published in leading academic journals, industry reports and professional handbooks, and has been featured in Harvard Business Review, the Financial Times, BBC and other global media.
Email: *michael.smets@sbs.ox.ac.uk*

Acknowledgements

We would like to express our gratitude to the CEOs we interviewed and thank them for finding time in their busy schedules, and for sharing openly their deep and personal insights.

We would also like to thank Chia Song Hwee, Stephen Forshaw, Mel Immergut, and Tom Glocer for their generous support in making this research project possible. We are also grateful to Andrew Darwin and Dr. Keri Pearlson for their thoughtful comments and valuable feedback.

ISTARI

ISTARI

ISTARI is a Temasek-founded global cybersecurity collective dedicated to helping clients build cyber resilience.

Established in 2020 by Temasek, an investment company headquartered in Singapore, ISTARI has a unique model. It is an advisory practice, investor, and educator through its Academy. ISTARI harnesses the collective power of the world's leading cybersecurity companies, experts, and knowledge to work alongside clients on their journey to becoming cyber resilient.

UNIVERSITY OF OXFORD

Saïd Business School

Saïd Business School, University of Oxford

Saïd Business School at the University of Oxford blends the best of new and old. We are a vibrant and innovative business school, but deeply embedded in an 800-year-old world-class university. We create programmes and ideas that have global impact. We educate people for successful business careers, and as a community seek to tackle world-scale problems. We deliver cutting-edge programmes and ground-breaking research that transform individuals, organisations, business practice, and society. We are a world-class business school community, embedded in a world-class University, tackling world-scale problems.

ISTARI