Print Article published in *MIT Sloan Management Review*

Authors:
Dr. Manuel Hepfer
Rashmy Chatterjee
Professor Michael Smets

Title:

The CEO's Cyber Resilience Playbook

What do CEOs who led through a serious cyberattack regret? Use this guide to learn from their experiences and take smarter actions before, during, and after an attack.

On May 7, 2021, executives at Colonial Pipeline discovered that cybercriminals had launched a ransomware attack on its IT systems. To prevent the malware from spreading further, the company took its computer systems offline, disabling 5,500 miles of pipeline that supplied 45% of the fuel consumed on the U.S. East Coast. The disruption lasted nearly a week, resulting in panic buying and fuel shortages. In a controversial decision, Colonial Pipeline paid a ransom of nearly $4.4 million in exchange for the decryption keys to get its systems back online. One month later, with recovery efforts and investigations ongoing, Colonial Pipeline CEO Joseph Blount defended that decision before the U.S. Senate, testifying, "*We were in a harrowing situation and had to make difficult choices that no company ever wants to face.*"

Blount's testimony echoes the experiences of many of the CEOs we have interviewed as part of our research into how leaders manage cybersecurity risk and attacks.[i] These CEOs shared with us similarly painful accounts of having to make existential decisions based on imperfect information, under enormous pressure, in an area where they had relatively little expertise. Serious cyberattacks thrust CEOs into the public eye, scrutinized by the media, shareholders, regulators, and other stakeholders.

We conducted 37 in-depth interviews with the chief executives of large enterprises (with average revenues of $12 billion) in the United States, Europe, and Asia. Nine of them had led their company through a serious cyberattack, which allowed us to compare their battle-tested views with those of CEOs who had not yet suffered such an attack. This article outlines strategies, based on their lessons, to help your organization stop over-relying on cybersecurity and start building cyber resilience as a strategic opportunity.

What CEOs regret after a serious cyberattack

The CEOs who had lived through cyberattacks on their organizations spoke candidly (and anonymously) about their experiences, evaluating their preparation strategies and the actions they had taken. They also shared their regrets based on lessons learned from their experiences.

They focused too narrowly on prevention. It would be a struggle to find a company that does not currently list cyber risk near the top of its enterprise risk register. Cybersecurity has become an inescapable priority for chief executives. But too often, leaders believe that it is possible to protect the confidentiality, integrity, and availability of information systems and data by preventing attacks. This has possibly never been true — and it most certainly isn't today. As cybercrime gains sophistication and is increasingly weaponized by nation states, even the most technologically advanced organizations will be breached — and they need to plan for that inevitability.

By far the most common regret we heard from CEOs was that they overemphasized cybersecurity to the neglect of cyber resilience. Only after the attack did they come to understand that trying to prevent cyberattacks is a losing game. These executives had focused on whether they would get attacked instead of on when they would get attacked and how they would respond when it happened. Although the CEOs poured significant resources into technological defenses, their companies often lacked basic organizational cyber resilience practices.

Cyber resilience describes an organization's ability to anticipate, withstand, respond to, and adapt to cyberattacks. The goal is not to simply avoid an attack but rather to minimize its impact, recover quickly, and emerge stronger. By shifting an organization's focus away from prevention and onto preparation, leaders prioritize developing adaptive capabilities, which should happen across all departments.

They felt merely accountable for cybersecurity. All of the CEOs we interviewed insisted that they are accountable for everything in their business, including cybersecurity — and yet 72% declared that they were not comfortable making decisions in that area. Notably, CEOs who had been through an attack regretted feeling merely accountable — that is, taking ownership after something bad had happened. Being responsible, in contrast, involves ongoing, proactive engagement before things go wrong.

As one CEO put it, they needed to be “co-responsible” for cyber resilience alongside their chief information security officer (CISO). That’s a development that many of the 40 CISOs we also spoke with as part of our research would welcome, given that they saw their CEOs as insufficiently accountable, let alone responsible, for cyber risk. One CEO in our study reported a tangible commitment to this co-responsibility: He spent 10 full days with his cybersecurity team after the company had recovered from a devastating attack, to show that he would be responsible alongside them going forward.

They blindly trusted cybersecurity and technology teams. CEOs trust their teams all the time. Cybersecurity and technology teams should be no different — but they are. Most CEOs have some degree of expertise in functions such as marketing or finance that helps them evaluate and challenge advice from others. In contrast, very few chief executives have a background in IT, let alone cybersecurity. After a cyberattack, many of the CEOs found themselves leaving the fate of the company in the hands of experts whose counsel they couldn’t fully comprehend.

As a result, CEOs who had been through an attack sought to develop more informed trust in their cybersecurity teams. Executives must understand enough to be able to ask the right questions, challenge advice, and make decisions. This requires both curiosity and the humility to continuously learn as cybersecurity and the threat landscape constantly evolve. The more CEOs understand about cyber resilience, the more they become concerned; the more concerned CEOs are, the more engaged they become.

They felt well prepared for a cyberattack. With the notable exception of those who had endured a cyberattack, the majority of CEOs in our study considered their organizations to be well prepared for such an event. That mindset can breed complacency that undermines efforts to continually shore up defenses and resilience planning. The CEOs with cyberattack experience admitted that only when attackers struck did they realize how ill-prepared they were and that the situation was far more dire than they had envisioned.

Crisis plans and playbooks can fuel the illusion of preparedness. While they are necessary, they aren’t sufficient preparation for a threat that is likely to unfold unpredictably. Because attackers continually adapt and develop new tactics, organizations are likely to face threats that were previously unknown: Tomorrow’s cyberattack is unlikely to look anything like yesterday’s. And while playbooks lay out procedures for managing the crisis, an attack may compromise the very infrastructure needed to do that, such as key communication channels.

CEOs who have been through an attack do not believe that organizations can be truly prepared. They adopt a mindset of constant underpreparedness to encourage their teams to continually test and evolve the organization’s ability to respond to an attack. In other words, they never feel prepared but are always ready for a cyberattack.

They reacted rather than reassured stakeholders. During a cyberattack, CEOs face tremendous amounts of pressure from all sides. Shareholders worry about the financial impact, the board wants evidence of business recovery, regulators want answers, customers worry about their data, and business partners want to know whether their systems are at risk of contagion. Faced with this barrage of competing demands for rapid responses, CEOs may default to a reactive mode in which they largely transmit information without first carefully evaluating it, such as communicating the IT team’s unrealistic recovery schedule to external stakeholders. In retrospect, many CEOs regretted not engaging various stakeholders more proactively — reassuring them rather than merely reacting.

CEOs can express reassurance in three key ways. As an amplifier, the CEO reinforces external pressures to create a sense of urgency. This is especially useful for reassuring external stakeholders that the organization is not succumbing to complacency throughout day-to-day operations and when new risks emerge. As a filter, the CEO judges what kinds of pressures to absorb or transmit. This is especially helpful during and after a cyberattack, when external pressures for accountability, and even blame, may distract people at the heart of the crisis response from recovery efforts. Finally, as an absorber, the CEO does not pass on any pressure but absorbs it and focuses on reassuring all stakeholders about the company’s resilience.

How CEOs Can Build Cyber Resilience

Drawing on our research, we developed a playbook of best practices for CEOs to help their organizations build greater cyber resilience and gain confidence in their own ability to manage all stakeholders when cyberattacks inevitably occur.

Invite an outsider CEO with cyberattack experience to speak to the CEO, leadership team, and board of directors. Hearing firsthand accounts of attacks can serve as an important wakeup call to the complacent. Executives who have managed a serious attack can share powerful personal stories and valuable experiences that are relevant to any company. This amplifies external pressure for greater cyber resilience and reassures stakeholders that the issue is being taken seriously. Hearing from executives rather than technology experts provides a more relatable perspective on how executives can anticipate cyberattacks and prepare to weather them. And, of course, CEOs themselves can gain direct insight into how their peers have contributed to limiting the damage and developed a more informed perspective.

Set up a cyber resilience learning forum. Some CEOs in our study regularly bring together the board, management team, business unit leaders, and security and IT teams for an open exchange about the most pressing cybersecurity challenges and current business priorities. The objective of these sessions is to build shared understanding — a more integrated, end-to-end perspective on business resilience that business leaders and cyber experts can draw on for both cyber planning and attack response. The CEO should chair the forum and establish the norm that the most naive questions are welcome: They help move individuals toward more-informed trust. Consider holding a forum at least annually, though quarterly may be most appropriate for this fast-moving topic. The forum sits outside formal risk governance processes and emphasizes learning. It does not replace cyber risk governance processes and committees.

Commission an independent cyber audit. Consider the value gained from financial audits. Similarly, CEOs should commission independent cyber resilience audits once per year. These specialists will report any findings directly to the chief executive and offer advice on addressing any issues they uncover. The purpose is not to get certified to some industry standard but for the CEO to gain a better understanding of the status quo, build more-informed trust with the technology team, and discover blind spots in the organization. To achieve all this, CEOs should work closely with their cybersecurity lead to analyze the results, which might range from technical to organizational and strategic depending on the focus of the audit. Unfortunately, we often find that CISOs hesitate to encourage the CEO to commission cyber audits because the CISO fears being put on the spot about the findings. But in reality, an audit often builds trust between the CEO and the cybersecurity team and forges co-responsibility for cyber resilience efforts.

Identify critical processes and priorities in case of attack. In the absence of a comprehensive response plan, when all systems are disabled, every department will insist that its business processes are critical and must be restored first. To avoid scrambling and infighting — and mount a coordinated and swift response — CEOs should sit down with their board and management team and identify the two to five business processes that are most critical to keeping the organization running. The components of each process should be mapped to the applications and servers that support them so that teams not only understand priorities for action but can make each critical process more resilient. A manufacturing company's critical processes might be taking customer orders and keeping certain production lines running; for a law firm, they might be email and time-tracking.

Agreeing on such priorities aligns the organization and informs decentralized decision-making when systems are down. However, even when organizations have carefully crafted plans and agreed-upon business priorities, the truism that "no plan survives contact with the enemy" still applies. Leaders must be ready to make bold decisions on priorities in the moment. But CEOs should not become the single point of decision-making. The CEOs we interviewed emphasized the importance of a shared set of guiding principles for the organization. This could be as simple as communicating that employee safety comes first, clients second, and shareholders third.

Seek expert assistance in advance of a crisis. Despite well-laid plans, organizations rarely have all of the up-to-date capabilities needed to deal with a serious cyberattack entirely on their own. Leaders should maintain a panel of trusted advisers to call on in the event of an attack. These might include law firms to help comply with regulations and interact with government agencies, communication specialists to protect the company's reputation, forensic investigators to discover how the attack happened, and even ransom negotiators to stall for time or, in the worst case, reduce a ransom demand.

Prepare to communicate proactively. One of the most important early decisions CEOs face during a cyberattack is what and how to communicate with employees, stakeholders, and the market. Keeping it all under wraps is not an option: It is nearly impossible to control the narrative without an open and transparent media strategy. Markets and regulators are far less forgiving of cyberattacks if the company appears to have been caught flat-footed or, worse, appears to be hiding something. CEOs should have a crisis communications plan in place so that they are ready to proactively reassure stakeholders about how the company will minimize impact and disruption.

Conduct a postmortem if the worst happens. When an organization has just survived a cyberattack, its leaders must capture insights quickly. While many in the organization are likely to be exhausted, CEOs should initiate an incident review with stakeholders from multiple business units. This discussion should focus on more than just the technical aspects of the attack and what can be done to avoid similar ones in the future. Participants must also consider elements of organizational resilience that might be improved, such as communication, crisis management capabilities, and business continuity processes. What's more, postmortem workshops can expose outdated business processes and previously unnoticed inefficiencies that impeded resilience during the cyberattack.

Look out for opportunities. Cyber resilience is not just about avoiding loss — it can also lead to value creation[ii]. One CEO we spoke with told us that the attack exposed significant inefficiencies in the organization's technology setup. Efforts to shore up cyber resilience by consolidating systems produced efficiency gains. The CEO allocated the resulting savings to building cyber resilience — a win-win.

But opportunities also exist in wider organizational structures, beyond optimizing the technology stack. A cyberattack can create a new appreciation for the criticality of otherwise hidden business processes, greater awareness of mutual dependencies, and greater recognition of leaders who stepped up at a time of crisis. This is the moment to pull the entire organization more closely together, redesign organizational structures, and reshuffle leadership teams for enhanced resilience.

These considerations should not stop at organizational boundaries. A major cyberattack often ripples across industries and pulls together otherwise competitive rivals. Capture opportunities to take more of an ecosystem approach to developing cyber resilience together with competitors, suppliers, and other stakeholders.

But most importantly, know that these opportunities will not just happen on their own. CEOs must actively look for them, treating the post-attack period as an opportunity to strengthen the very foundation of their company for the digital era.

The experience of a serious cyberattack is one that many CEOs would like to forget. While they typically find this difficult personally, they note that organizationally, memories tend to fade once normalcy returns. Therefore, while it is a painful trauma to revisit, it is important that they keep the memory alive.

To build cyber resilience beyond the boundaries of their organizations, CEOs should also share their experience with other leaders. While top executives naturally hold their cards close as they seek to outcompete and outsmart their rivals, cyber resilience thrives on mutual support and sharing information. Cyber should be seen as a noncompetitive domain where companies — even those in the same industry — work together to achieve greater levels of resilience. By sharing their stories and what they have learned with other industry peers, executives contribute to the resilience of the entire ecosystem.

———

About the authors

Manuel is the Head of Knowledge and Insights at ISTARI, a cybersecurity platform established by the investment firm Temasek to help companies build cyber resilience. He is also a research affiliate at Oxford University's Saïd Business School.

Rashmy is the CEO of ISTARI. 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. She is a member of several boards, including that of Allianz SE.

Michael is 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.

[i] M. Hepfer, R. Chatterjee, and M. Smets, “The CEO Report on Cyber Resilience,” PDF file (London: Istari, 2023), https://istari-global.com.

[ii] M. Hepfer and T.C. Powell, “Make Cybersecurity a Strategic Asset,” MIT Sloan Management Review 62, no. 1 (fall 2020): 40-45.