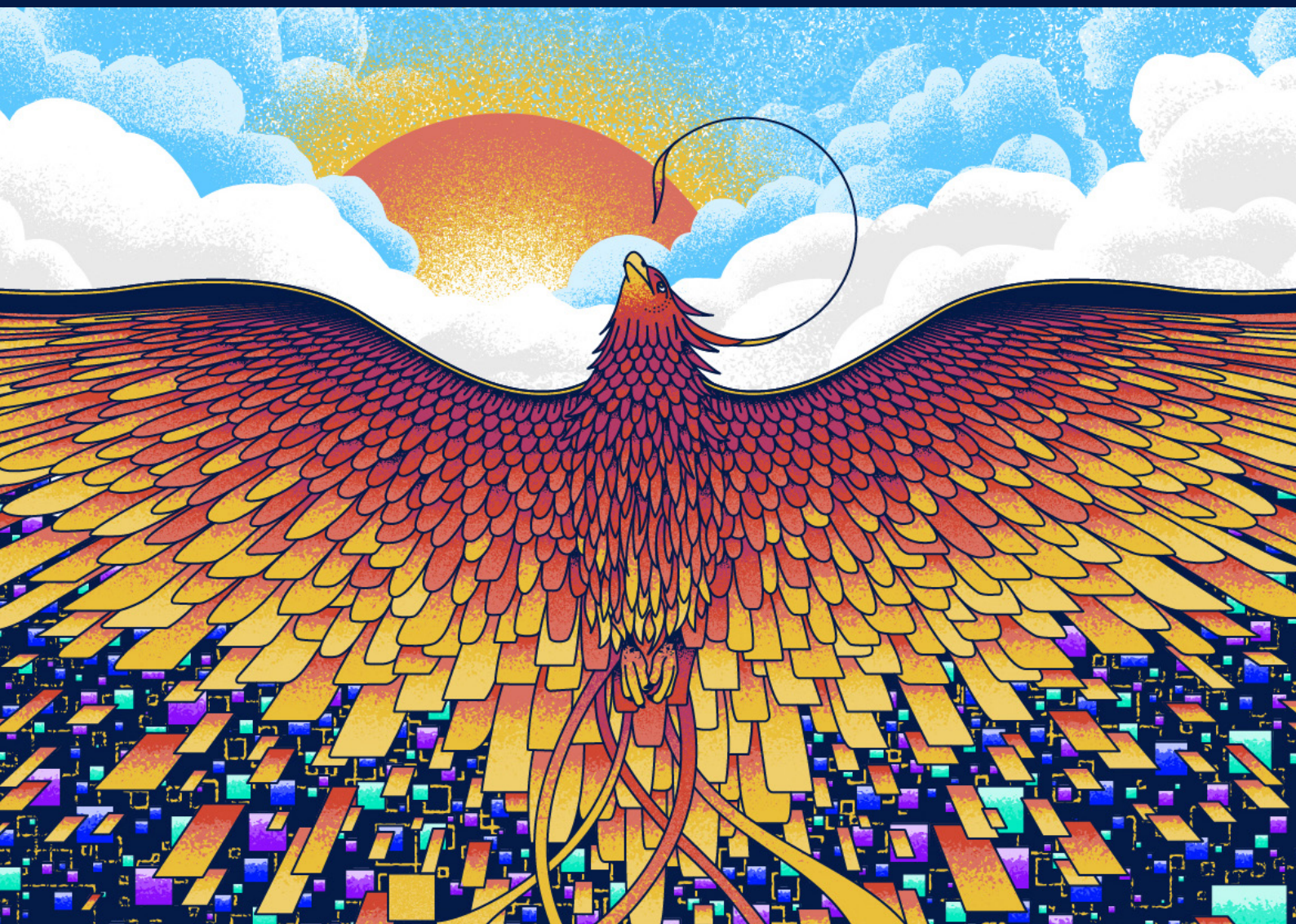
ISTARI Perspectives

Creating cyber resilience by routine

By honing a core set of primary and enabling activities that are consistent, specific and measurable, leaders can boost cyber resilience and create business value.

Rashmy Chatterjee &
Dr. Manuel Hepfer

01 • 2023



Creating cyber resilience by routine

By honing a core set of primary and enabling activities that are consistent, specific and measurable, leaders can boost cyber resilience and create business value.

On March 19, 2019, executives at Norsk Hydro, one of the world's largest aluminium producers, discovered that hackers had launched a devastating attack on the company's computer systems. The attackers had accessed the IT network, encrypting data on laptops, servers and industrial control systems. Within minutes, the malware had affected the company's operations across 170 global sites, including production plants, interoffice communications and access to documents and data.

Norsk Hydro responded to the attack by taking its computer systems offline. Executives decided against paying the ransom; instead, they planned to rebuild the entire IT infrastructure from scratch. The company shifted to manual operations to continue producing aluminium, while trying to recover key data, systems and processes. In parallel, executives held daily makeshift press conferences to update shareholders, customers, suppliers and other stakeholders on business impacts and recovery progress. Norsk Hydro was praised for its response and demonstrated organisational resilience in the wake of the attack. Its market capitalisation was up by 10 percent just one month after the cyberattack.

"The cyberattack on Hydro was a defining experience for me. It highlighted the importance of building resilience, before an attack occurs."

JO DE VLIEGHER,
FORMER CIO AT NORSK HYDRO & CLIENT PARTNER AT ISTARI

The successful and coordinated response by Norsk Hydro is a notable exception to the norm. Although cyberattacks have moved from a distant possibility to an inescapable reality, many organisations remain ill-equipped to anticipate, withstand, respond and adapt to a serious cyberattack. Leaders who have fallen victim to such assaults know that the key lies in preparation. Instead of focussing exclusively on cybersecurity protection, they prioritise efforts to build resilience. They also know that resilience does not just enable more effective mitigation and recovery.When done right, it is a source of strategic advantage.

Yet, some companies are more resilient than others. Why is that?

From cybersecurity to cyber resilience

Companies like Norsk Hydro understand that striving for perfect cybersecurity protection is a losing game. The cyber world is expanding exponentially, with millions of newly connected devices every day. As the digital surface grows, so does risk. Even the most technologically advanced organisations, such as Apple, Google, Facebook, Yahoo, JPMorgan Chase or the U.S. military, are unable to prevent all cyberattacks. Meanwhile, nation states that seek political, economic and technological superiority invest heavily in offensive and defensive cyber capabilities – and often outperform private companies that are either direct targets of attacks or suffer collateral damage.

Cybersecurity and cyber resilience are complementary but distinct approaches. Cybersecurity evolved from the discipline of IT security and its primary objective is to protect the confidentiality, integrity and availability of systems and data. That heritage results in an emphasis on technical language and acronyms like SIEM, DLR, XDR or DevSecOps that seem daunting and complicated for business executives, prompting them to delegate responsibility and understanding of cyber risk to their technology teams. The most widely adopted cybersecurity standard is the NIST framework, which provides a set of guidelines and best-practices for improving cybersecurity. However, NIST is skewed towards cybersecurity protection in its sub-categories: around 80% of them focus on identification, detection, and protection, whereas only 20% focus on improving response and recovery.[1] Moreover, many see NIST as a departmental framework

that does not place sufficient emphasis on an organisation's ability to prepare for crises and anticipate changes in the external environment, prepare for crises, or on key business elements such as organisational strategy or culture.

In contrast, the concept of cyber resilience arises out of a wider set of "resiliency" domains, which share the goal of helping organisations weather all kinds of disruptions – pandemics, wars or cyberattacks. In a volatile world, resilience is at the top of most executives' strategic agendas.

Cyber resilience is the ability of an organisation to *anticipate, withstand, respond* and *adapt* to cyberattacks. The goal is not just to avoid an attack but rather to hone an organisation's ability to minimise the impact of an attack, recover quickly and — this is critical — to emerge stronger by evolving in the process. Cyber resilience shifts the traditional cybersecurity focus from reaction to proaction, from prevention to preparedness, and from a departmental issue to an ongoing organisational endeavour.

Despite its growing importance, cyber resilience remains hard to build and even harder to measure. At ISTARI, we have developed a framework for evaluating and improving cyber resilience based on years of research. It outlines a set of essential activities that can guide leaders who aspire to strengthen their organisations' cyber resilience. The purpose of the *cyber resilience-by-routine* framework is not to reinvent existing frameworks but to complement them. The key takeaway from the ISTARI framework is that building cyber resilience requires developing a mindset of routine, which has to be consistent, comprehensive, and embedded in everyday operations.

Methodology

The framework is based on insights from three sources of data. First, we started by conducting empirical, academically rigorous, in-depth research with more than a dozen companies that had suffered a serious cyberattack. We got access to internal documents relating to the attack and interviewed their executives, systematically analysing similarities and differences in how each company anticipated, withstood, responded and adapted to the attack. We asked ourselves: what are the critical activities required for building resilience? Our analysis provided a rich baseline for a framework. We then complemented our insights from the field by conducting workshops and interviews with internationally recognised cybersecurity experts, business executives and former and current chief information security officers. Lastly, we examined existing cybersecurity and resilience frameworks to identify strengths, gaps, and common practices.

Making it happen: The fundamentals of cyber resilience

The ISTARI framework is based on activities that need to be performed repeatedly and developed into routines over time. These activities are observable, measurable, and manageable.

We categorised these fundamental activities into two areas. Primary activities are the foundational building blocks by which an organisation builds and continually strengthens its cyber resilience. Enabling leadership activities relate to things organisations perform irrespective of cyber resilience, but are critical for building a resilient organisation.

Four primary activities form the building blocks of an organisation's cyber resilience:

1) *Anticipate:* To have the awareness, insights and ability to correlate global and local events to their likely impact in the cyber domain and to take action, *before* a cyberattack occurs. This requires ongoing processes to improve predictability by tracking changes in technology, standards, regulations and geopolitics – and preparing for any effect they may have on the organisation.

2.) *Withstand:* To remain undamaged or unaffected or to offer strong resistance to a cyberattack. In practice, this means having the ability both to prevent an attack *and* to minimise material impact, should one occur. Organisations can withstand cyberattacks with preventive controls (before a network intrusion occurs) and with reactive controls (after a network intrusion has occurred). Norsk Hydro's preventive and reactive controls failed to stop the initial attack but its successful response enabled it to mitigate losses and ultimately recover from a ransomware outbreak.

3.) *Respond:* To align and to act after a cyberattack has occurred. This involves technical responses, such as computer forensics and restoring data from backup, as well as organisational responses, such as crisis management, business continuity and stakeholder communication. Working with external experts, Norsk Hydro was praised for its successful response of setting

up three working teams: one to investigate the virus corruption, one to continue day-to-day operations, and one to rebuild a new network, all while communicating transparently on a daily basis.

4.) *Adapt:* To adjust swiftly when new conditions arise. Resilient organisations adapt their routines and activities before, during and after a cyberattack. The most resilient organisations don't simply bounce back after an attack. Instead, they continuously learn and evolve – their foundation strengthens and they are better equipped to thrive in the digital domain. Companies can adapt even in the absence of a cyberattack by conducting exercises.

Putting primary activities into practice with a bow tie

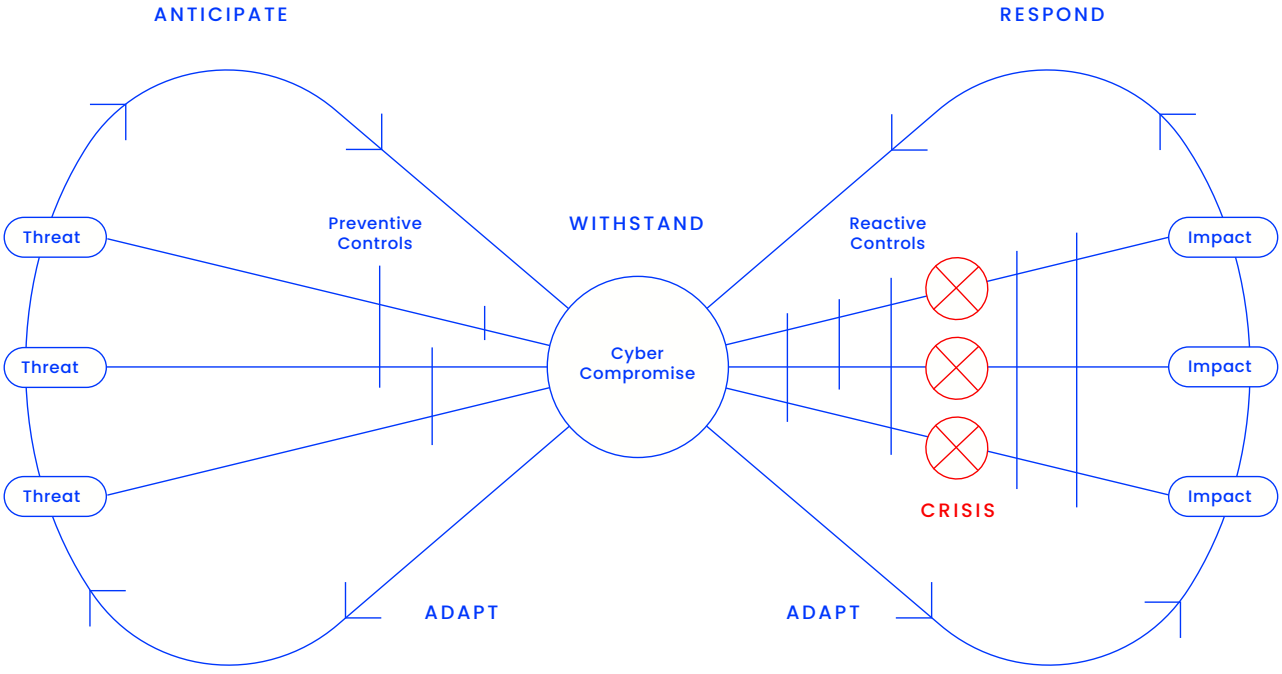
Organisations like oil rigs, railway operations or nuclear power plants have zero margin for error. Many of these high-reliability organisations put the four primary routines into practice and successfully build resilience to potential catastrophic events by using what is known as the bow-tie model.

Potential threats – internal or external – can compromise a system and cause negative impact. To do that, a threat first has to penetrate preventive barriers and successfully intrude a network. Such network intrusion is, in and of itself, unproblematic – if reactive barriers prevent intruders from moving across the network, gaining administrative credentials, and modifying, encrypting or exfiltrating data. Preventive barriers reduce the chances of a compromise, whereas reactive barriers lower the severity of any impact.

However, because of imperfections, each layer is prone to failure and has weaknesses that threats can exploit to bypass it. Stacking up protective and reactive layers so that there is no straight line through holes means threats have to penetrate multiple layers to cause a crisis and serious harm.

Failure in all relevant preventive and reactive controls leads to a serious organisational crisis, illustrated in red in the bow-tie diagram. Dealing with the crisis is now a matter of organisational response and collective responsibility: communication, coordination, business continuity, emergency plans and recovery. The right actions taken at this point can still significantly limit negative impacts on financials, shareholder confidence and operational downtime

THE BOW-TIE MODEL



Enabling activities of cyber resilience

An army can have the best weaponry and tools, yet lose a war due to poor morale, leadership or motivation. Similarly, an organisation can build excellent technological capabilities, yet remain ineffective due to the poor performance of other factors. We call those "enabling leadership activities."

Enabling leadership activities are repetitive tasks organisations already perform irrespective of cyber resilience. The five enabling activities relate to crafting and executing strategy, managing internal culture, designing the organisation, managing risk & governance, engaging with the ecosystem.

When cyber resilience is integrated into the execution of these activities, they provide essential support for the primary activities. Done poorly, they can become serious blockers to achieving high levels of resilience or make matters even worse. In other words, an organisation can have effective primary activities but will not achieve high levels of cyber resilience without the enabling activities.

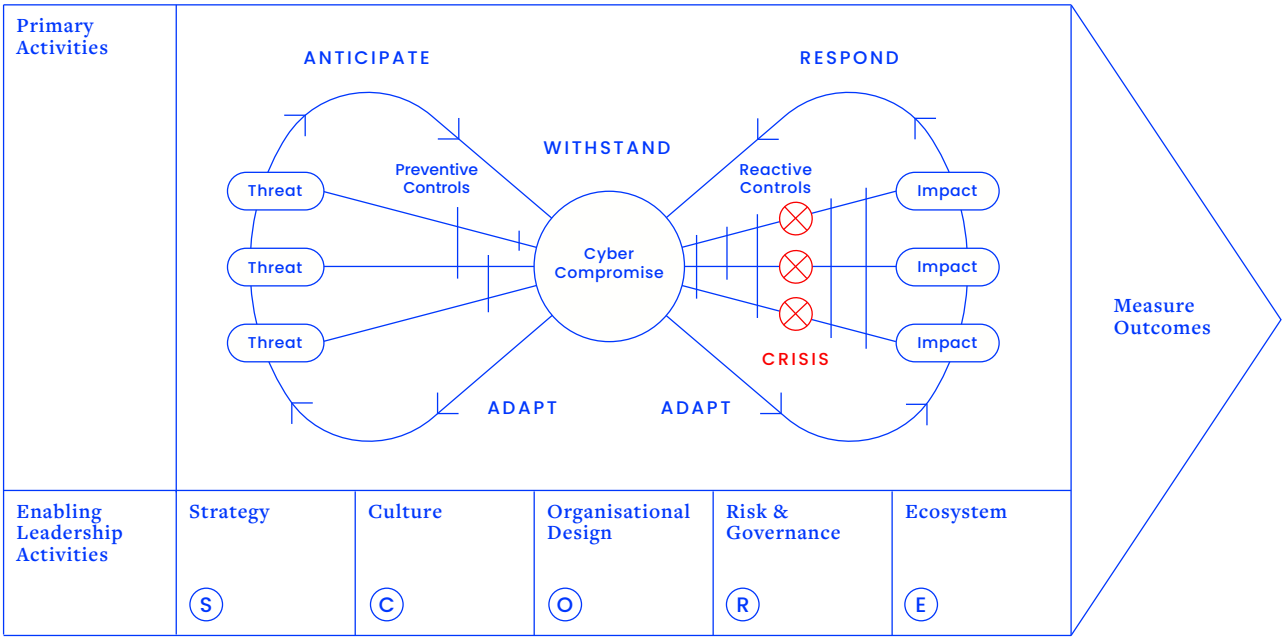
Strategy

Strategy is the determination of long-term goals and the allocations of resources necessary to achieve those goals. Every firm has a business strategy to achieve superior performance but not every firm has a formalised cyber resilience strategy. The core question, as one CEO put it to us, is resource allocation: *"Are we spending enough on cyber resilience and are we spending it on the right things?"* A well-crafted cyber resilience strategy prioritises investment and aligns people, processes, technologies and organisational initiatives while enforcing measurement.

Culture

"Culture eats strategy for breakfast," as Peter Drucker famously observed. Strategy execution will fall flat if it's not supported by the right culture. Culture emphasises the human element in organisations and strengthens resilience from within – it is the things people do when no one is watching. A CIO told us, *"We don't have a culture that values cyber resilience. As a result, our defences are weak."* Just as companies developed a safety culture decades ago, so do organisations in today's digital age need to develop a culture that strengthens cyber resilience. Attributes such as vigilance, encouraging dissent, confidence in raising concerns and fostering learning from mistakes instead of punishing them will fundamentally strengthen the cyber resilience of an organisation. Should a serious attack occur, culture gives employees a sense of purpose and helps them perform under pressure.

THE CYBER RESILIENCE-BY-ROUTINE FRAMEWORK



Organisational Design

Structure follows strategy; it defines lines of authority and communication between different business units and coordinates people, tasks and activities. The design of an organisation must enable speed of action and lay out a clear chain of command during different phases: in day-to-day operations, when a new cyber threat arises and during a serious cyber crisis. Key to succeeding in these phases is to find and retain the right skills and talent, and to make the right outsourcing decisions. *"Hierarchy completely broke down,"* one CIO told us about an attack his company endured. *"We assembled a hierarchy and structure dynamically as we needed to. What might normally take two years to change, we were changing within 18 hours."*

Risk Management & Governance

A risk-based approach to building resilience enables prioritisation on those high-value assets that are most at risk. It also ensures the right governance structure and stakeholder alignment. One CEO told us, *"It quickly dawned on us how little we actually knew about the real risks of being hit by a cyberattack, or how severe the risk could be. We couldn't even imagine it."* Managing cyber risk effectively requires identifying and prioritising critical assets and processes, aligning on risk appetite and allocating budget – all of which facilitate decisions about which risks to mitigate, transfer or accept.

Ecosystem

A connected world requires collective resilience. Every organisation is part of a geopolitical and digital ecosystem consisting of technology and non-technology suppliers, customers, shareholders and other parties. Attackers tend to look for the weakest link. Despite their limited ability to control macroeconomic factors – political, economic, technological or legal developments – organisations can still work with their ecosystem to improve resilience through public-private partnerships, mitigation of third-party risks in supply chains and shared intelligence, knowledge and best practices. One CEO who suffered an attack told us, *"The decision to openly communicate with customers, shareholders and the general public after was a really useful strategy, because customers, suppliers and even some of our competitors actually offered to help."*

Bringing it together: The cyber resilience-by-routine framework

Primary and enabling routines depend on each other. High levels of cyber resilience will only be achieved if all routines work flawlessly together. An organisation cannot compensate for persistent deficiencies in one routine by becoming extremely good in another. If culture is weak, for instance, improving other routines while completely ignoring culture will still jeopardise overall cyber resilience. All activities are connected. All routines are connected. ".

Where to start: Identify the biggest weakness

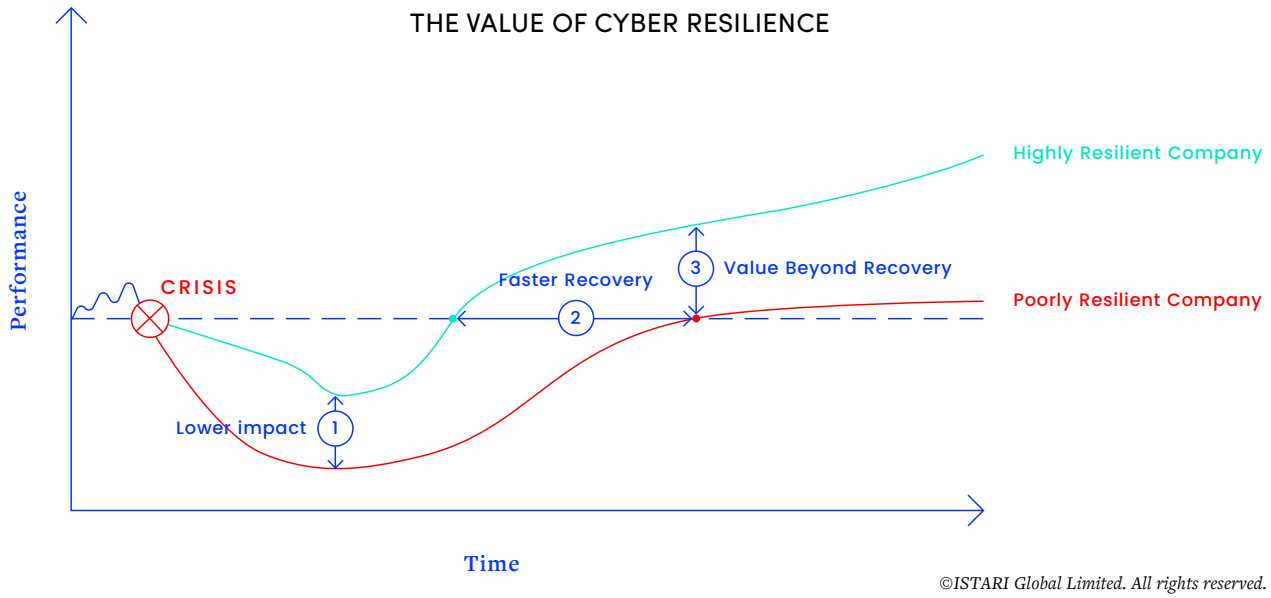
We observed that many companies tend to overinvest in strengths and underinvest in weaknesses. They do this in the belief that cyber resilience comes from strength instead of from the performance of the system as a whole. However, this is almost never the case; any source of cyber resilience can be nullified by persistent weakness in a single activity. For example, a company that is under serious cyberattack and does not have the organisational capabilities to respond will not achieve high levels of resilience.

Trying to improve every primary and enabling activity simultaneously will not achieve great results. The most successful organisations we studied prioritised their efforts by identifying those activities that achieve the greatest outcome in their organisation. Because persistent weakness in one activity can impair the company's overall cyber resilience, a good place to start is to identify and improve the weakest primary and enabling leadership activity.

Measuring outcomes

Many organisations find it difficult to correlate investment in resilience with improvements in resilience. And indeed, improving cyber resilience without measuring progress is difficult.
A well-designed measurement system that tracks progress in both primary and enabling routines should drive holistic improvement. The key is to identify specific sub-activities for each routine that can be observed and quantified with precision. For example, the enabling routine of risk management may consist of sub-routines such as identifying risks, analysing risks, evaluating risks qualitatively or quantitatively, mitigating risks and monitoring risks – all of which feed into regular risk communication and reporting using risk dashboards.

Dashboards for each primary and enabling routine and their associated sub-activities become the documentation for resource allocation and strategic decision-making. In these dashboards, managers should pay special attention to discrepancies between routines. Finally, honestly assessing the state of an organisation's cyber resilience requires that organisations continually calibrate and test their ability to perform primary and enabling routines by inducing simulated shocks.



The real resilience payoff: Unlocking new business value

The value of resilience is clear in times of crisis. Resilient companies enjoy better performance compared to their peers along three dimensions – (i) the crisis has lower impact on performance; (ii) the speed of recovery is higher; and (iii) the extent of recovery is greater. The more serious the crisis, the higher the value of resilience. However, organisations shouldn't overlook the value that arises from building resilience in good times as well. Non-resilient enterprises are seldom organisations that simply get unlucky, or that do everything right except cyber resilience. More often, poor cyber resilience exposes deeper strategic problems that manifest themselves in weaknesses all through the enterprise. Companies can use the process of improving cyber resilience as a tool to expose and eradicate weaknesses that would otherwise remain unnoticed or ignored; not just in cybersecurity technologies but also in business areas like leadership development, external communications, or process innovation.

But the value goes beyond simply eradicating organisational weaknesses to gain efficiency. Some companies use cyber resilience as a strategic asset – an asset that helps them protect and deliver value, thereby accelerating long-term digital growth, innovation, and evolution.[2] For example, focussing on cyber resilience helped executives in a logistics company recognise that their most important business asset was not their cargo – it was taking customer bookings. In their strategic efforts, they subsequently focussed on innovating critical business processes relating to customer bookings to spark further business growth.

Conclusion

As economic value-creation races ever more rapidly and fully to digital domains, companies require strong and resilient digital foundations in order to achieve long-term success. The traditional approach to cybersecurity has limitations due to vastness of the domain, the growing sophistication of attackers, the evolution of technology and shifting geo-politics. Shifting attention and action from cybersecurity to cyber resilience prepares organisations to grow confidently against a backdrop of the known and unknown.

The ISTARI resilience-by-routine framework defines the elements for building cyberresilience using a bow-tie model. The framework defines four primary routines (Anticipate, Withstand, Respond, Adapt) and five enabling routines (Strategy, Culture, Organisation, Risk & Governance, and Ecosystem). Together they define the list of activities that companies need to perform well to build high levels of cyber resilience. We believe that companies that follow the resilience-by-routine framework are more likely to thrive in good and bad times and will be better able to capture strategic opportunities along the way.

Endnotes

1.) NIST identifies 98 sub-categories; 25 relating to identification, 35 to protection, 18 to detection, 14 to response and 6 to recovery

2.) Hepfer, Powell (2020), Make cybersecurity a strategic asset, MIT Sloan Management Review

About the authors

Rashmy Chatterjee

CEO, ISTARI

—

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 she was global sales leader for IBM Security and Chief Marketing Officer for IBM North America. 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 many boards, including most recently that of Allianz SE.

Dr. Manuel Hepfer

Researcher, ISTARI & Oxford University

—

Manuel leads research at ISTARI and is 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 and appeared in academic and practitioner journals such as MIT Sloan Management Review and was covered by the Financial Times.