ISTARI Perspectives

Strengthen the CORE: A Framework for CEOs to Build Cyber-Resilient Organisations

Rashmy Chatterjee

04 • 2021

The coronavirus pandemic has accelerated the pace of digitalisation and global interconnectivity. This has exposed vulnerabilities which, when coupled with the growing sophistication of cyber attackers, can result in reputational, financial and operational loss at an unprecedented scale and speed.

In this dynamic environment, it is no longer a question of 'if' but 'when' an organisation will face a serious breach. Cyber resilience, which we define as the ability of a business to bounce back from an attack and resume normal operations with minimal loss or disruption, is of existential importance in a digital world.

There is a misconception in the industry that cyber resilience is driven solely by technology and requires a plethora of complex tools.[1] In practice, the first step to cyber resilience is to acknowledge it as a business imperative that should be led with direct CEO oversight.

Successful leaders recognise the competitive advantage of building cyber-resilient organisations. At ISTARI, we have designed the CORE-S approach below to assist leaders in meeting this objective, demonstrating that they do not need a deep understanding of technology.

THE CORE-S FRAMEWORK

This framework has been derived from conversations with chief executives, chairs, senior business leaders and our own experiences. CORE-S highlights a few simple actions that leaders can take to strengthen the digital foundation of their business, underscoring the critical elements that only they can lead.

1. CULTURE

An organisation's culture is its first line of defence. 90% of successful attacks are a result of human error and 20% are caused by insiders.[2] A workforce that has been trained with the discipline, habits and hygiene to be alert to cyber threats adds a strong layer of defence against attackers.

Actions: Role model a cyber-smart culture from the top. Provoke senior management to experience and internalise the impact of a serious cyber attack so they lead with personal conviction. Support with frequent training, testing, knowledge sharing and workforce engagement on the changing nature of threats in the context of business value protection.

2. ORGANISATION

Resilient organisations are able to operate in three modes: (i) steady-state maintenance and compliance, (ii) continuous monitoring and rapid adaptation to new risk, and (iii) crisis response. A common point of failure across these modes is an unclear chain of command. A defining aspect of resilient organisations is the speed and agility in all three modes and not just after an attack occurs.

Actions: Design the organisation and processes for cyber resilience for all three modes and constantly test to confirm you have a clear chain of command.

3. RISK UNDERSTANDING

No organisation can ever be 100% secure because the associated technologies, actors and environments are constantly changing. The process of prioritising cyber risk, based on an integrated understanding of threats, vulnerabilities, assets, controls and relative risk exposure, is a business decision which requires CEO oversight. Business leaders often ask us: "Am I investing enough in cybersecurity and am I investing in the right things?" The answers need to be underpinned by an indepth understanding of the actual risks faced and potential tradeoffs required in a business context, not a technology context.

Actions: Implement an end-to-end process to manage cyber risk. Define the digital risk landscape[3] for your business. Prioritise the most important risks for investment. Implement executive dashboards, risk reporting and annual external audits.

4. ECOSYSTEM

Cyber resilience is not a solo sport. Geopolitical tensions, a globally interconnected supply chain and the emergence of new business models mean that the security of an organisation relies on the ecosystem within which it operates. At a broader level, that ecosystem includes the partnership between businesses, regulators and policymakers and the sharing of a common language and dashboards. At an internal level, the ecosystem extends to third-party workers and the supply chain. In fact, 80% of organisations have had a breach caused by a vendor, making supply chain risk a top area of focus.

Actions: Define principles of external collaboration with governments, technology partners, customers and suppliers. Implement solutions to protect against third-party risk and secure the supply chain. Engage with your peers in the industry. Sharing threat and vulnerability intelligence reduces risk exposure.

5. STRENGTHENING

Last but not least, cyber resilience requires strengthening through persistence. Building cyber resilience is a marathon, not a sprint. A digital business is stronger when cyber resilience is central to its strategy, alongside digital transformation, with a long-term approach to people, processes and capabilities. Many gains in resilience come from making better use of current capabilities, not adding more.

Actions: Be persistent. Establish processes to continually monitor, prioritise and address risks. Strategically define your cybersecurity 'principles' for talent, technology and partnerships.

Leaders can use our CORE-S framework as a simple self-assessment tool to help track their initiatives and strengthen their organisations' cyber resilience. Having the diagnostic results is just the first step. Real value stems from ongoing leadership dialogue and the deeper understanding that this approach fosters.

At ISTARI, we believe that the collective power of our experts, technologies and know-how trumps any single tool or individual insight. Successfully navigating the threats and seizing the opportunities in a digital, interconnected world requires leveraging your own collective power by putting cyber resilience at the core of your business planning and strategy. Business leaders who make the effort to get this right can build a sustainable competitive advantage in a digital world.[4]

About the Author

Rashmy is the CEO of ISTARI, a global cybersecurity platform created by Temasek to help clients manage digital risk.

Before ISTARI, she was the global sales leader of IBM's cybersecurity business and the CMO for IBM, North America. Rashmy is passionate about building a culture of long-term client relationships and developing talent. She is an advocate for women in technology and sits on several boards. She is also a Fellow of the International Marketing Academy.

1 Hubback, J. (2020). Cybersecurity technology efficacy: Is cybersecurity the new market for lemons?. Debate Security (https://www.debatesecurity.com/cybersecurity-technology-efficacy-iscybersecurity-the-new-market-for-lemons/)
2 Hill, M. (2020). 90% of UK data breaches due to human error in 2019. Infosecurity-Magazine (https://www.infosecurity-magazine.com/news/90-data-breaches-human-error); and Gartner (2020). An Integrated Approach to Insider Threat Management (https://www.gartner.com/document/3981556)
3 Hubback, J. (2021). Navigating your digital risk landscape. ISTARI Perspectives (https://istari-global.com/our-insights/ourinsights/navigate-your-digital-risk-landscape)
4 Hepfer, M., Powell, T.C. (2020). Make cybersecurity a strategic asset. MIT Sloan Management Review (https://sloanreview.mit.edu/article/makecybersecurity-a-strategic-asset/)