ISTARI Perspectives

Navigate Your Digital Risk Landscape

Joe Hubback

04 • 2021

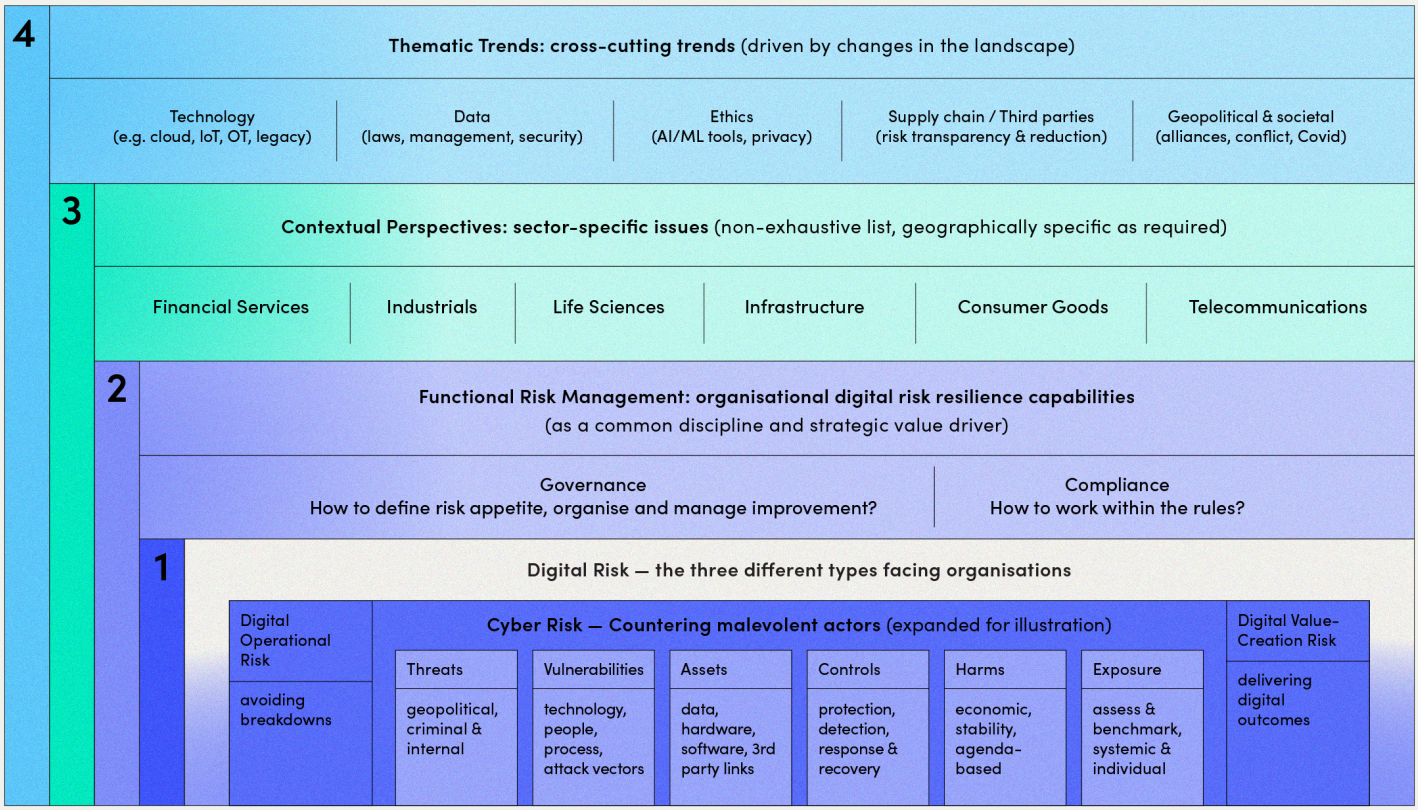
At ISTARI, we believe that by engaging your top team on four crucial questions you can understand your digital risk landscape and build resilience.

The accelerating digitalisation of how we work, shop and live is rewiring top executive mindsets. Most CEOs today no longer see technology as mainly about cost savings[i]. Instead, they understand that digital strategy, innovation and operations must be a core competency of their business if they want to delight customers, create value for shareholders and outpace their competition.

But when it comes to digital risk management, only the most advanced senior leaders recognise the business imperative. Instead of over-indexing on what can go wrong, these executives seize the opportunity to turn operational necessities into competitive advantages[ii].

This ability starts with a firm understanding of the true nature of digital risk and how it rapidly changes. Cyber threats are, of course, part of the picture but there is more to it. To help guide you, we have mapped out the digital risk landscape in an attempt to demystify it, by capturing it in four layers (see graphic, below). Although digital risk is often perceived to be complex and confusing, we show that all digital risks fall within only three categories: operational, cyber and value-creation risks. These three digital risk types (layer 1) form the bedrock of the digital risk landscape. The additional layers on top then dynamically mould and shape the contours of your company's underlying digital risk, namely: your functional risk management approach (layer 2), your specific context based on your sector and geographic footprint (layer 3), and finally, the broad thematic trends that cut across the entire digital domain (layer 4).

Each risk landscape is unique, therefore. To navigate yours — and understand what it takes to build resilience – senior leaders can begin by asking their top teams to tackle four essential questions. Answering these will help create a shared framework on digital risk, surface hidden challenges, clarify key choices and make digital business operations more secure and resilient.



"Answering these essential questions will help create a shared framework on digital risk, surface hidden challendges, clarify key choices and make digital business operations more secure and resilient"

1 DIGITAL RISK TYPES

As noted, there are only three different types of digital risk: operational, cyber and value-creation risks. Understanding this is the first step in assessing your digital risk landscape, which is why they're at the base of our graphic. Digital operational risks are those that result from failure in software or hardware. They disrupt company operations, cause operational inefficiencies or entail financial harm. Cyber risk is the most asymmetric, existential and dramatic challenge. Cyber attacks have disrupted some of the world's largest companies, such as Travelex, Facebook, British Airways, the UK National Health Service and Microsoft. Digital value-creation risk arises as part of the delivery of enterprise outcomes using digital tools and channels. If an organisation's digital tools and algorithms do not deliver the desired results to create value for the enterprise as expected, these risks materialise.

2 FUNCTIONAL RISK MANAGEMENT

At the enterprise level, successfully fending off risks depends on two key management activities. Governance addresses how risk is discussed and dealt with by leadership, how digital risk shows up (or not) in executive decision-making and board dashboards, how much attention senior leaders give to it and how much they invest in dealing with it. Compliance, the other side of risk management, ensures that regulations are adhered to and laws respected, regardless of geography or jurisdiction.

3 CONTEXTUAL PERSPECTIVES

Despite shared global threats, digital risks vary widely by industry sector and geography. Consider the recent state-level cyber espionage attacks on the pharmaceutical industry amid its race to develop valuable COVID vaccines.iii Each industry has different assets to defend, and has to comply with different regulations. Retail's digital risk from transaction protection or e-commerce site availability, for example, is very different from automotive's, which connects more to vehicle safety or manufacturing protection.

4 THEMATIC TRENDS

Although each digital risk landscape evolves along a different path, there are overarching trends that run over the whole landscape. Examples range from the ongoing evolution of privacy and data regulations to the development of artificial intelligence solutions (and the associated moral challenges, such as how algorithms price retail insurance offers) as well as geopolitical tussles like the current technology battle between China and the USA.

Managing digital risk is something no company can avoid. What matters is how well you understand all four layers of your total landscape in order to create the kind of organisation you will need — one that is prepared when risks materialise and that then bounces back and adapts effectively. Getting this right is not a one-time process but a dynamic work-in-progress. It requires engaging a broad consortium of leaders and stakeholders who share a willingness to constantly evolve. Only when both are in play will you successfully build a digitally resilient organisation, from top to bottom.

About the Author

Hubback is Managing Director of the ISTARI Academy and Managing Director for EMEA. He was previously a Partner at McKinsey, where he co-led the creation of their cybersecurity service line and, more recently, was Managing Director at Keller (UK and Nordics). Joe started his career in the industrial sector as an engineer designing and installing electronic control and robotics systems.

[i] https://hbr.org/2003/05/it-doesnt-matter

[ii] https://sloanreview.mit.edu/article/make-cybersecurity-a-strategic-asset/

[iii] https://www.bluevoyant.com/news/bluevoyant-report-reveals-biotech-and-pharmaceutical-industry-under-attack/