ISTARI Perspectives

Making risk-led cyber resilience a reality

Not all assets and business processes are equal. Companies should focus on those that matter most for their business's success.

Ashish Gupta
Scott Kannry

02 • 2023

Making risk-led cyber resilience a reality

Not all assets and business processes are equal. Companies should focus on those that matter most for their business's success.

In our daily lives, without even thinking about it, humans often adopt a risk-led approach: We consciously and subconsciously prioritise our time and efforts to nurture what we value and to protect us and our loved ones from the most severe threats. It is time for organisations to do the same when it comes to building resilience against cyber risk.

Regulators certainly think so. In the United States, the Security Exchange Commission (SEC) has proposed guidelines that will require publicly traded companies to understand their cyber risk in economic terms. Are companies, the SEC asks, spending all of their money to fend off a $10,000 event while missing a potential $1 billion event?

While the need may be obvious, executing a risk-led resilience strategy is not easy. Part of the problem is that many organisations take a uniform approach to cybersecurity, implementing a blanket set of controls without differentiating between assets and their relative importance to the business. In addition, some over-invest in preventive controls at the expense of responsive controls (the controls that allow organisations to continue operating and to recover quickly).

The bottom line: Many companies are spending more on certain areas than is justified by the threat and less in other areas where the dangers are extreme. This is a treacherous approach that could lead to misallocation of capital and implementation deadlock, which could be further exacerbated by limited internal resources, skills and management bandwidth.

A risk-led approach to cyber resilience

Organisations that successfully employ a risk-led approach to building cyber resilience recognise the need to prioritise business-critical departments and actions. They direct resources and attention to protecting what matters most to the health of the organisation. By gaining better visibility into their most valuable assets and processes and quantifying the dollar amount of potential risks, senior leadership can answer key questions,- such as "How much should we invest in cyber resilience and in which areas?" "What will the return on our investment be?" and "What residual risk can we transfer to cyber insurance?"

> "I believe that simply throwing money at the problem is not, and has never been, the answer. By using a risk-led approach to cyber resilience, we can allocate capital to reduce those cyber risks that matter most to business success."
>
> BOB DUDLEY,
> FORMER CEO OF BP

To identify those high-priority assets and processes, companies should rely on data to understand what really drives their business value – and what types of threats could cause the most harm. This can lead to surprises. For example, a leading manufacturing company discovered that one of its most important business processes in its plants was serial number assignment, which, if disabled, would lead to a global production disruption. Subsequently, the company moved swiftly to focus its efforts on reducing the risk of disablement and to improve the resilience of the entire process.

With increased regulatory scrutiny, what else does it take to get risk-led cyber resilience right?

Four key steps

Achieving risk-based resilience requires objective, data-driven methods to assess and quantify cyber risk in dollars. This is becoming ever more important in a volatile and uncertain world where every dollar spent needs to be justified. The good news is that a set of best practices is emerging.

1. Map out the risk landscape and connect it to your assets

A good starting point is to map out the organisation's risk landscape with the aim of moving from a subjective evaluation of risk to an objective calculation of the risks that pose the greatest threat to business value: in other words, identifying and analysing the largest revenue-generating functions within the organisation and quantifying the negative impact, should those functions not work as intended.

To illustrate this point, consider the Colonial Pipeline cyberattack. The malware that struck the company did not disable the operational systems of the pipeline itself but the billing system. However, without that billing system, which played a pivotal role in monitoring pipeline flows, the pipeline was effectively put out of action.

By combining such internal data with information on the wider business ecosystem and external factors (such as geopolitical shifts, third-party dependencies or regulatory drivers), decision-makers can map their internal calculations of risk against the external threats to which they may be most vulnerable. The more objective and data-driven the process, the more precise the measure of financial value at risk. Yet, in a recent survey of 30 chief information security officers, ISTARI found that only five percent of companies have implemented quantitative cyber risk assessment.

Focusing on business value as opposed to threats allows executives to more precisely define the organisation's cyber risk tolerance (the degree of risk the organisation can tolerate without toppling) and its cyber risk appetite (the level of risk an organisation is prepared to accept).

2. Evaluate the effectiveness of your controls

To assess the vulnerability of critical assets and business processes, organisations can conduct cyber resilience maturity assessments. These measure how well existing control mechanisms prevent or limit the business impact of an attack.

Controls work best when the evaluations are continuous, not occasional. For example, moving to a multi-cloud environment entails continual technology and process changes – and cloud security controls must be evaluated constantly in parallel.

Informed by a more accurate view of an organisation's defence mechanisms and working within their overall risk appetite and tolerance, executives can approve spending on new initiatives that bring down residual risk or transfer some risk by adjusting their cyber insurance coverage.

3. Take an integrated, not a sequential, approach

As described here, steps one and two may seem to be consecutive. They are not. Mapping the risk landscape and evaluating control effectiveness should be an integrated, continuous process.

In our experience, too many companies employ a sequential approach; they first map all their business risks, then identify their crown jewels and lastly assess the effectiveness of their controls. Instead, these steps should happen simultaneously and be tested against prioritised risk scenarios relevant for the business.

A risk-led approach should continuously adapt to changes in the business and cyber risk landscape. For example, the acquisition of a new business unit should immediately trigger an updated assessment of a company's overall cybersecurity maturity.

4. Communicate, communicate, communicate

Currently, many boards of directors and chief executives are unable to correlate investment in cybersecurity with reduction of risk. But being able to do so is becoming more urgent. A recent Gartner report predicts, "by 2026, 50% of C-level executives will have performance requirements related to risk built into their employment contracts." Embracing a risk-led approach to resilience will help satisfy those demands.

In a market study conducted by ISTARI, cybersecurity leaders expressed strong interest in quantifying cyber risk in dollar terms to facilitate decisions on risk remediation, transfer and avoidance. The need to communicate the results of these assessments in a unified and ongoing way is paramount; doing so will further align all stakeholders.

Organisations that deploy a risk-led approach to cyber resilience will enjoy several benefits: more effective decision-making, more precise allocation of capital to reduce risk, clearer correlation between investments and risk reduction and the integration of cyber into the full range of enterprise risks. In our complex, constantly evolving world, these firms will be better equipped to bring structure and order to what often appears to be a complex challenge.

Ashish Gupta

Ashish Gupta has over 18 years of experience in building cyber risk management programmes from strategy to execution. Before joining ISTARI as a client partner, he spent 14 years with PwC, leading the cybersecurity consulting practice in the U.S., India and Southeast Asia regions. He is an avid speaker on various cybersecurity topics and holds an MBA from Northwestern University's Kellogg Business School.

Scott Kannry

Scott Kannry is the Chief Executive Officer of cyber risk-engineering firm Axio. He is a frequent speaker at industry events and has been recognised as a "Business Insurance" magazine 40 Under 40 broker, a "Risk and Insurance" magazine power broker and an industry rising star by "Reactions" magazine.