Operational economics insights to boost cyber resilience

This article maps key cyber resilience measures to the operational realities of digitally transformed businesses

By IIM Calcutta

Last Updated: Aug 11, 2025, 13:59 IST 8 min

It is virtually infeasible for smart industries relying upon IT and IoT converged technology to be free of the impact of cyber-attacks. This is a well-researched and well-publicised fact in the cybersecurity community. Hence, it is imperatively critical for companies to focus on cyber resilience to mitigate the adverse impact of a cyber-attack. In other words, while it may be impossible to prevent the next NotPetya, Colonial Pipeline, JBS, SolarWinds, Kaseya, and Log4J-like cyber-attacks, it is possible to reduce the business impact of such events.

RELATED STORIES

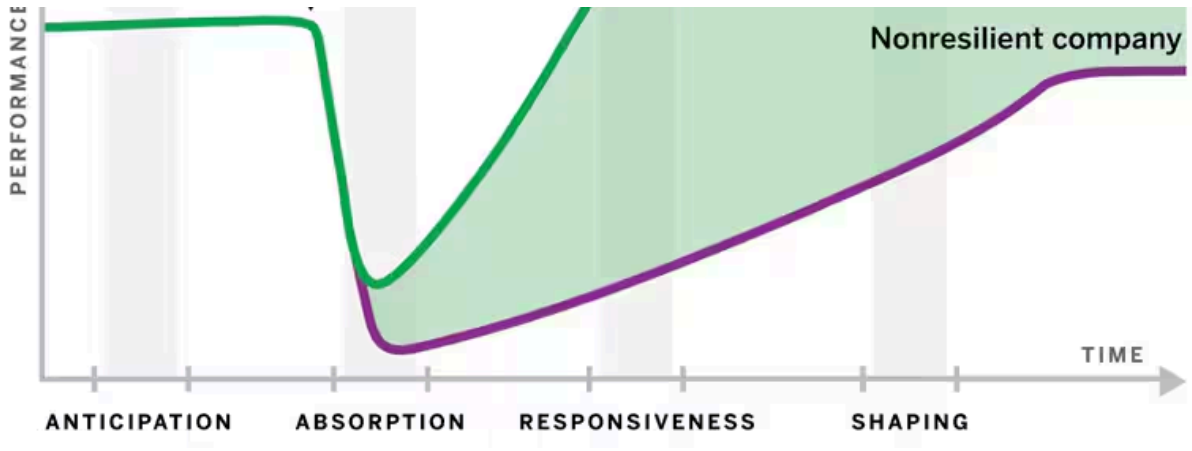
1 **How to manage GenAI cyber risk in industrial control systems**
IIM Calcutta

2 **How to manage cyber risk in AI LLM-driven pharmaceutical supply chains**
IIM Calcutta

3 **How systemic cyber risk management in software supply chains works with BOMs**
IIM Calcutta

The Concept of Cyber Resilience

The cyber resilience concept (as per the National Institute of Standards and Technology) is pivoted upon four sequential time scale ideas: anticipation, absorption, responsiveness, recovery, and shaping, as shown in Figure 1.



The Cyber Resilience Concept (NIST)[Adapted from Coden et.al. MIT Sloan Management Review, 2023]

Business enterprises should be able to anticipate cyber-attacks and subsequently build/invest in a robust cyber posture to mitigate the likelihood and lessen the adverse impact of a cyber-attack on their operations.

Post the anticipation time scale is the adverse business impact absorption ability of an enterprise in the aftermath of a cyber-attack, via implementing redundancy, diversity, and modularity of enterprise system functionalities. These implementations ensure that business performance takes a moderate hit post a cyber-attack.

The responsiveness and recovery time scale is next, which is the ability of an enterprise to recover from a cyber-attack quickly. More specifically, this ability is mostly (if not always) correlated with the quality of absorption measures. The higher the absorption ability, the faster a business can adapt to recovering from a cyber-attack.

Finally, the shaping time scale reflects (post-recovery) the ability of a business enterprise to be imaginative in figuring out what novel ways enterprises could be cyber-compromised in the future and the extent of adverse business impact such compromises can have for an enterprise. This time scale looks very similar to the anticipation time scale however, it is subtly different in the dimension that the latter is more about current and near-term futures, whereas the shaping time scale targets the longer-term future of cyber incidents.

Also Read

Items?

While the different time scales in Figure 1, with their generic action items, provide a blueprint for IT/IoT converging businesses to boost cyber resilience, the varying operational economics across these businesses dictate how each business will implement action items differently.

This article for managers, based upon the study of one small and one large IT enterprise in India, lays down a mapping between standard cyber resilience boosting action items (fitting the time scales of anticipation, absorption, and responsiveness) and the heterogeneous operational economics that drive digitally transformed business enterprises.

Economics of the Anticipation Time Scale

One could safely assume that most critical infrastructure-supported business services are being increasingly digitally driven. There is always a fixed cost of anticipatory investment in cybersecurity that involves the “infrastructure" that determines the cyber posture strength of an enterprise. The typical elements of such an infrastructure involve personnel, culture, technology (hardware/firmware/software), and insurance.

Companies that invest in high fixed costs tend to be more proactive in their cyber risk management (CRM) approach, typically due to having a large enough budget to allocate to cyber-risk management. The variable CRM costs for such enterprises are significantly low. These costs are usually sourced from technological advancements on already invested technology, or from conducting additional employee training programs, or from a marginal increase in cyber insurance pricing. In summary, these enterprises exhibit high economies of scale in their cyber posture quality and are the operational “elephants" that come “heavily" pre-loaded with proactive CRM measures.

In contrast, small IT-driven companies typically focus on their core business product and allocate a significantly smaller budget to anticipatory fixed-cost CRM, even for enterprises that prioritise cybersecurity. The variable CRM costs for such enterprises are

exhibit low economies of scale in their cyber posture quality and are most adversely affected in performance post a cyber-attack.

Economics of the Absorption Time Scale

The quality of the absorption time scale is determined by the quality of the anticipation time scale, which is further influenced by the risk tolerance and/or risk minimisation mindset of a digitally driven enterprise. This mindset (that drives managerial actions items on both the anticipation and the absorption time scales) is nothing but a cost-benefit analysis where the additional cost of cyber-risk reduction is compared to the expected benefit value.

Enterprise cyber-risk statistics can either be of the normal type (e.g., the standard bell curve) or the coconut type (e.g., signifying rare cyber-events whose chance is analogous to the chance a coconut falling on your head when you rest on the beach) or the black swan type (e.g., very rare cyber events– one example being complete city blackouts for hours as shown in the 2025 Netflix web series Zero Day the chance of which happening is analogous to the chance of seeing a black swan).

To absorb normal cyber-risks, enterprises should invest in sufficient redundancy (e.g., multiple data centres, cloud instances, cyber-personnel) and cyber insurance. Such managerial actions can be performed with a fixed cost and variable cost CRM investment allocation portfolios. Additionally, for some selected business resources, backups of backups should be implemented, which would incur greater CRM fixed costs for the enterprise. To absorb coconut cyber-risks, enterprises should adopt a quick response and recovery planning approach/strategy (see later in the article) alongside sufficient cyber insurance and an appropriate mix of backups-of-backups strategy.

Two common alternative absorption approaches for normal and coconut-type cyber-risks are diversity and modularity. Enterprises should have diverse technology, people, and processes as “duplicative" elements to whom compromised elements can offload functioning after a cyber-attack on a particular technology type (e.g., a cyber-attack on

segmented into multiple distinct “isolated" networks (via access control and zero-trust technologies), each only reachable from one another in very few ways.

Diversity, when combined with modularity, ensures healthy enterprise systems are isolated from compromised systems. Enterprises will incur heterogeneous fixed and variable investment costs (and different economies of scale) on deploying diversity and modularity strategies. Moreover, investing in strengthened security on each of multiple IT-driven enterprise system segments (islands) sparsely networked among each other boosts complete system security in a squared manner due to Metcalfe’s law.

Unlike normal and coconut-type cyber-risks, it is challenging to absorb black swan-type cyber-risks. The tricky thing about such cyber-risks is that insurance is not sufficient, as it does not help the continuity of services in the wake of a cyber-attack. When a power grid goes down, the most important thing is to bring it back up as soon as possible to prevent a major societal catastrophe (eventually, business loss coverage through cyber insurance and insurance-linked securities results). A backups-of-backups strategy is too cost-inefficient for enterprises to risk manage very rare events. The good news is that possible cyber-risk absorption strategies here can draw inspiration from managing coconut-type cyber-risks. i.e., have a very good response plan and for certain very critical business resources, adopt the backup-of-backup strategy, including analogue backups as a risk absorption strategy.

Economics of the Responsiveness and Recovery Time Scale

Time responsiveness is the most important aspect of cyber resilience, as enterprise management is usually keen to return to desired business performance as quickly as possible after a cyber-attack. However, “fast" implies operational cost, and not every profit-minded enterprise has the economic strength and/or vision to bear such costs for the greater good of society (i.e., helping supply chains that such enterprises source services/resources recover fast from a cyber-attack), not at least for cyber. As Simon Sinek puts it, most businesses only have the appetite to play the myopic finite game (where the business thinks of near-term profits), instead of the more desired infinite

Virtually every enterprise has different customer segments, each with their own heterogeneous time responsiveness demands. Very timely response demands (such as those made by enterprises with critical infrastructure reliant on the power grid) can be served by enterprises if they invest sufficiently in people, technology, and processes (PTP) that have rapid (and real-time) learning cycles from the intelligence gathered on the cyber-attack under question. Such investments incur high fixed costs (and are usually invested by big enterprises with a strong cyber awareness/vision and sufficient budget to attract top PTP to serve the cyber resilience cause) and also cater to the demands made by enterprises that do not need a fast response towards recovery. However, not every enterprise (be it big or small) in modern digital supply chains can be a strongly cyber-aware enterprise.

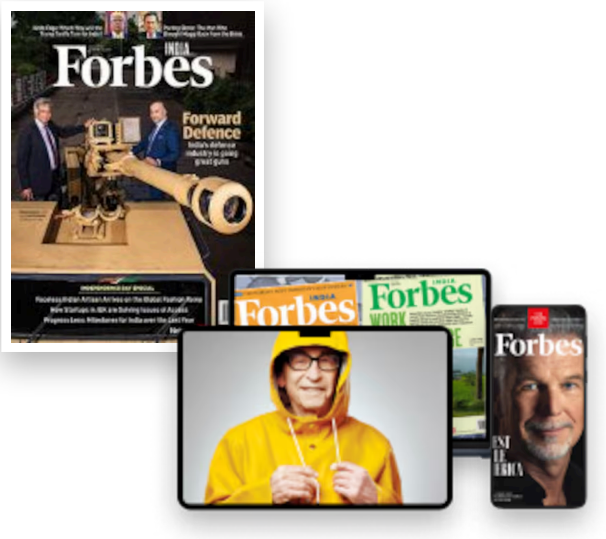
Such enterprises need to be very fast-responding to handle the impact of a cyber-attack event. Their business performance may be the most hit after a cyber-attack event (due to lack of sufficient in-house PTP) resources, but they can gather “external" resources on PTP on-demand and at high costs to recover their (and contribute to their supply chain partners also, especially if they are small and medium enterprises, i.e., SMEs with low economies of scale and majorly relying on other enterprises in a supply chain) business performance fast. Such enterprises shift their “unused" investment capacity on demand for event-driven reactive management they are prepared to do high-quality CRM to “save" their businesses and also businesses of others in the supply chain if they are SMEs (usually otherwise also).

By Ranjan Pal (MIT Sloan School of Management, USA), Saral Mukherjee (Indian Institute of Management, Ahmedabad), Bodhibrata Nag (Indian Institute of Management Calcutta)

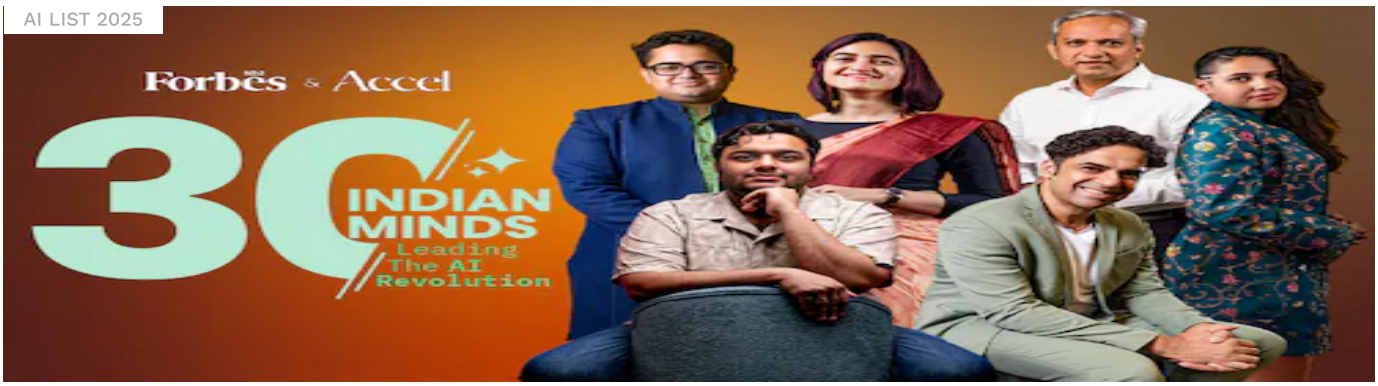
*This article has been published with permission from IIM Calcutta. **www.iimcal.ac.in** Views expressed are personal.*
First Published: Aug 11, 2025, 13:59

MIT Sloan School of Management National Institute of Standards and Technology

I **IIM CALCUTTA**



FORBES LIST



TogetherAI's Vipul Ved Prakash: Democratising AI access with open-source solutions

Naini Thaker

Creating an army of AI employees: Surojit Chatterjee

Naini Thaker

Prof Sunita Sarawagi: Helping machines make sense

Samidha Jain

Explore All List

LATEST NEWS