WHAT IS A CYBER RESILIENCE STRATEGY?

Organizations' dependence on internet-based technologies continues to hit new heights as organizations, large and small, adapt their operations and offerings around the digital economy. This dependence is exposing companies to an ever increasing and changing threat landscape, ranging from cyber-attacks, such as DDOS and ransomware, to impacts of data privacy regulation such as financial penalties and more rigorous data processing scrutiny.

McKinsey reports that consumers and business customers alike will accept nothing less than a complete assurance that the companies they engage with protect their highly sensitive data carefully in the hyperconnected information systems powering the digital economy. Having a holistic strategy for securing (and restoring) the trust of stakeholders is the only sure way of guaranteeing this assurance. So, let's define cyber resiliency and explore best practices for developing your cyber resilience strategy.

What is cyber resilience?

Generic resiliency refers to a system's ability to recover from a fault and maintain persistent service dependability when faced with faults. The aim of cyber resilience, then, is to ensure that business operations are safeguarded, so that a threat or breach does not demobilize the entire business.

EY defines cyber resilience as the seamless initiation of several approaches to maintain the ongoing delivery of operations during a disruption. Together, the approach covers the entire lifecycle of capabilities required for planning for, detecting, responding to, recovering from, and improving after

a cyber related disruption. These approaches include:

- Cyber security
- Risk management
- Business continuity
- Disaster recovery

Let's look at three angles you should consider when building a cyber resilience strategy.

Alignment to business strategy

For almost all market segments, digital transformation is central to business strategy. IDC forecasts strong digital transformation technology investment growth (between 15-20%) across all sectors over the next four years. That means your cyber resilience strategy should align with the direction of your business with regard to exploiting cyber technologies to propagate the sale of its products and services, defines what are the business priorities, targets and markets are.

The business strategy provides great insight into not only what business processes and assets are most critical to supporting the business, but also the level of exposure to cyber disruptions that these processes and assets will face. The cyber resilience strategy must cover the entire product lifecycle as well as supporting business operations including focusing on people, suppliers, and resources.

The CISO, working with the rest of the leadership and IT, needs to develop a cyber resilience strategy that supports business strategy with regard to securing the main assets and processes that underpin the strategy. Therefore, participation by both business and IT is paramount in the development of the cyber resilience strategy. Balance the controls you put in place in order to ensure there is no conflict between the level of resilience required (in terms of availability, security and continuity) and the usability of processes, products, and services. Embedding resilience in the design and development of products and services (using frameworks such as DevSecOps) can be very useful in ensuring this balanced approach.

Risk Based Approach

A cyber resilience strategy cannot be effective if risk management is not the foundation. Cyber resilience controls are best determined when a comprehensive cyber risk management approach is adopted, which understands the enterprise strategy and associated cyber risk exposure in the ever-changing business landscape. In general, cyber risk management involves the following steps:

1. Identifying cyber risks and vulnerabilities
2. Assessing cyber risks based on impact and probability
3. Evaluating cyber risk priorities based on business risk appetite
4. Mitigating cyber risks based on chosen strategies (accept, reduce, share, or avoid)
5. Monitoring and communicating risk exposure and mitigation status

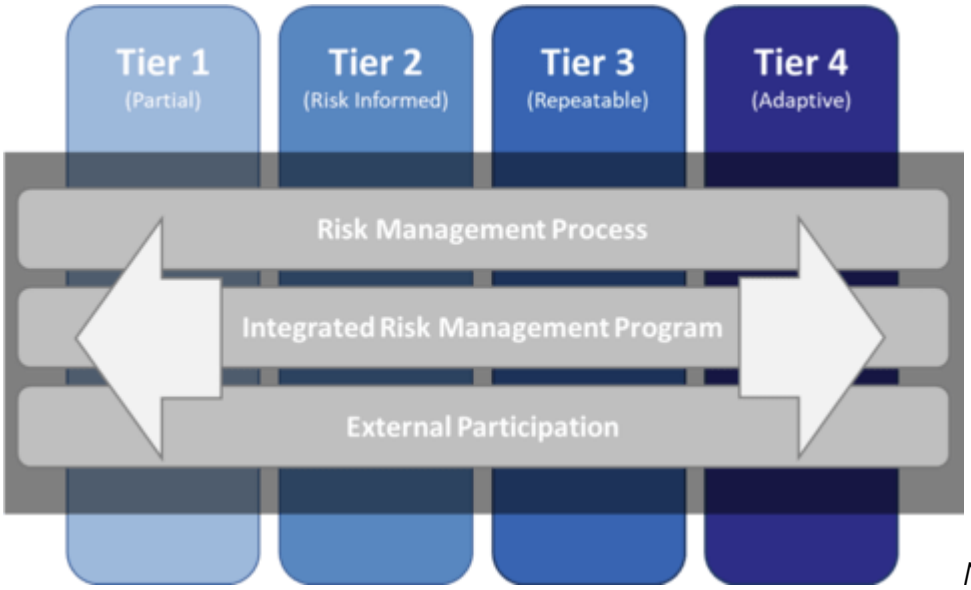
The importance of aligning your cyber resilience risk management to the organization's enterprise risk framework cannot be understated. Embed your cyber risk governance within the existing organizational governance framework to ensure consistency in directing, monitoring, and evaluating cyber risk mitigation within the entire organization.

Where the business strategy is heavily aligned to use of third-party providers, such as cloud providers and outsourced developers, there must be a greater level of scrutiny for supplier related risks. Poorly secured cyber suppliers are a huge vulnerability that can be easily exploited by cyber threats and expose the organization to significant regulatory and legal penalties, beyond derailing your digital transformation.

Target Posture

All organizations are different, and are at different stages in their operational life. The uniqueness of an organization's digital approach is determined by factors such as the level of resource allocation, risk appetite and strategic objectives.

Therefore, any cyber resilience strategy must take all these elements into consideration and determine what is the right posture for the particular time and circumstances faced. Using the NIST cyber security framework is one way an organization can evaluate itself, based on four tiers, and identify the steps required to get to its desired posture.



NIST Cybersecurity Framework Implementation Tiers

Another option for determining the appropriate cyber resilience posture is to consider benchmarking one's organization with the DOD's Cybersecurity Maturity Model Certification (CMMC). The CMMC framework defines five levels that reflect the maturity and reliability of a company's cybersecurity infrastructure to safeguard sensitive government information on contractors' information systems.

	Description of Level Practices	CMMC Rev 0.3 Practices	New CMMC Rev 0.4 Material	CMMC Rev 0.4 Practices	Rev 0.4 New Content Sources
CMMC Level 1	Basic Cyber Hygiene	17	+18 practices	35	• DIB SCC TF WG Top 10 • NIST Cybersecurity Framework 1.1 • ISO 27001:2013 • AIA NAS 9933 • CIS Critical Security Controls 7.1 • CERT Resilience Management Model® • Additional DIB Inputs • Subject Matter Experts
CMMC Level 2	Intermediate Cyber Hygiene	46	+69 practices	115	
CMMC Level 3	Good Cyber Hygiene	63	+28 practices	91	
CMMC Level 4	Proactive	10	+85 practices	95	
CMMC Level 5	Advanced / Progressive	4	+30 practices	34	

CMMC Framework

Referencing these models can go a long way in ensuring that an organization's cyber resilience is improving and continues to meet the needs of the organization and its stakeholders going forward.

Additional resources

For more on cybersecurity topics and practices, see our Security & Compliance Guide or browse our BMC Security & Compliance Blogs.