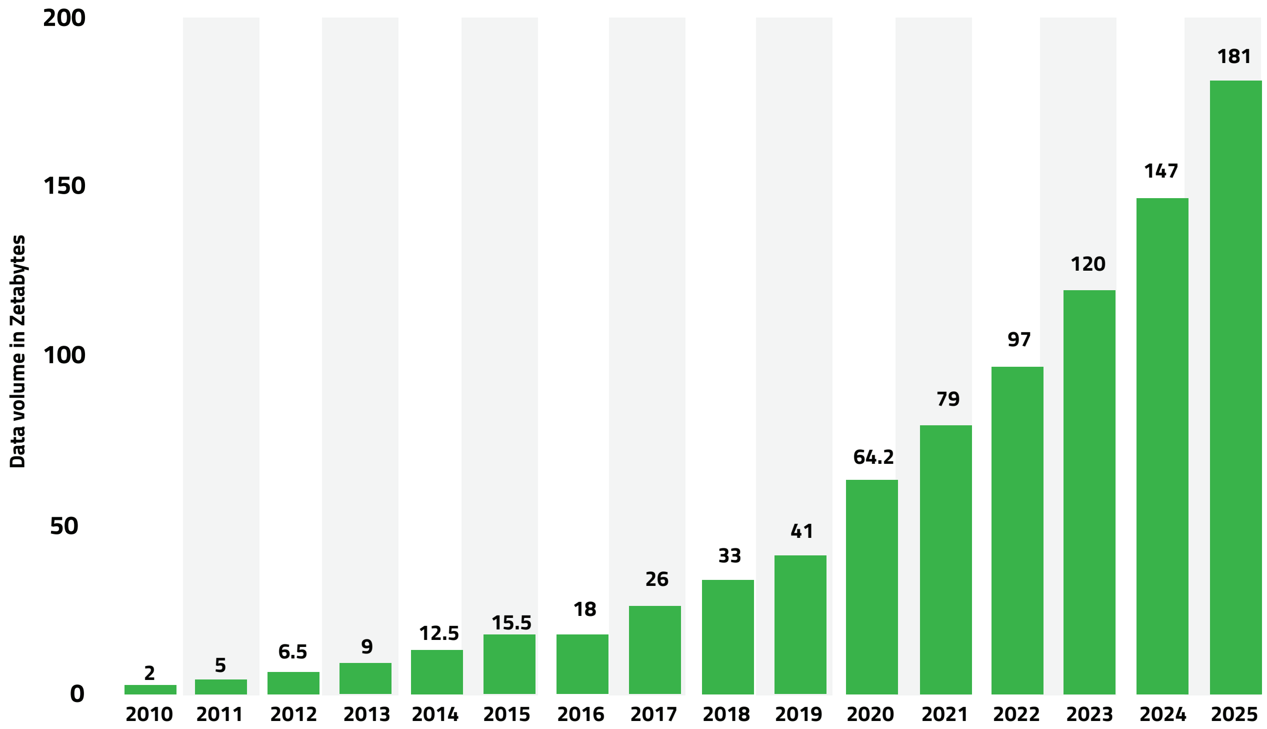
happiest minds
The Mindful IT Company
Born **Digital** . Born **Agile**

Cyber Resilience

A Framework to Secure your Digital Organization

The digital technology revolution is driving many organizations into a new world of hybrid environments, and the cloud being at the core. Most of the data, digital infrastructure and applications now reside at the center of business and society. More than 25 quintillion of data are generated across the globe through the Cloud, Internet of Everything (IoE), Mobile Computing, and other technologies that are connecting and exchanging data.



Source: Statista 2021

The nature of cyber risk automatically changes with the adoption of more digital technology, and the attack surface continues to grow. The traditional defensive and responsive approach alone is not at all enough to withstand today's sophisticated attacks. The adoption of digital technology, the innovation around it, and the changing perspective of how we work and connect makes it more vulnerable and more accessible for hackers to target. Organizations failing to withstand any data breach or inability to recover data, applications, and business processes can lead to business loss and reputational damage. It might even have to face the consequences of regulatory penalties.

This whitepaper explains why an organization must build a solid cyber resilient framework, how we can achieve this by adopting the right strategies and following the best cybersecurity practices.

Data Breach Incident and Prediction in the recent past

01 The data breach incidents in the U.S. have significantly increased from 662 in 2010 to over a thousand by 2020 - Statista

02 During 2017-2019 there was a staggering increase of 80% in the number of people affected by data breach incident in health care industries. - Statista

03 In 2020, the country with the highest average total cost of a data breach was the United States at $8.64 million (Ponemon Institute)

04 Cybersecurity Ventures expects global cybercrime costs to grow by 15 per cent per year over the next five years, reaching USD 10.5 trillion annually by 2025

The concept of Cyber Resilience and its Importance

According to RWG, cyber resilience is the capacity of an enterprise to maintain its core purpose and integrity in the face of cyberattacks.

In general, cyber resilience is the strategy implemented by an organization to prevent, detect, contain, and recover from a severe threat against data, applications, and infrastructure. The primary goal of cyber resilience is to minimize the disruptive effects of cyber threats to business or mission operations. The goal includes the ability to withstand cyberattacks and prevent degradation to a mission or business effectiveness. A cyber resilient enterprise successfully aligns continuity management and disaster recovery with security operations in a holistic fashion.

Many security decisions are made based on the principles of Confidentiality, Integrity and Availability (CIA) triad with cyber resilience focus on anticipate, withstand, recover and develop activities in addition to the CIA model. The tools integrated to prevent attacks should be used with the right combination and methodology to quickly detect and recover vital business operations. There should be a continuous approach towards evaluating the need to invest in new solutions to ensure the organization is effectively evolving.

Challenges of Cyber Resilience in purview of Digital Transformation

Considering that it takes a median time of 99 days to discover a breach and just under two days (aka. 48 hours) for attackers to gain complete control of a network. Organizations must develop comprehensive plans for keeping their on-premises and cloud infrastructure resilient to cyber threats since it is impossible to be 100 per cent secure all the time.

The significant challenges for the organizations are:

01 Dependency on more digital services across all business aspects, society, and our lives

02 Adoption of new workforce methodology

03 Internet of Things being leveraged on all platforms for smarter better connectivity

04 Cyber incidents becoming more complex and sophisticated, impacting the business continuity

05 Adoption of new technology innovative – collaborative approaches for digital transformation

06 Technology complexity with the adoption of hybrid, multi-cloud, API based architecture

Considering the above personal & sensitive data must be accounted for and protected no matter where it resides. whenever it is accessed, data from anywhere at any time, everyone's identity must be secured and managed. Organizations must build a strong and effective resilient strategy around the digital ecosystem. Both digital transformation and cyber resilience must go hand in hand with a holistic approach to orchestrate a quick analysis and respond to cyber-attack for optimal business recovery. Your cyber resilient strategy framework must have strong layers of risk management, disaster recovery and business continuity, with next-gen security strategies and approaches to survive and thrive in times of cyber incidents.

Components of the Cybersecurity Resilience Framework

Three parts of the framework that strengthens the organization's mission and cybersecurity activities

Part 1:

The Framework Core - The digital technology organizations that drive the world are moving to a hybrid environment and the cloud becoming the core. Most of the data, digital infrastructure and applications now reside at the center of business and society.

Part 3:

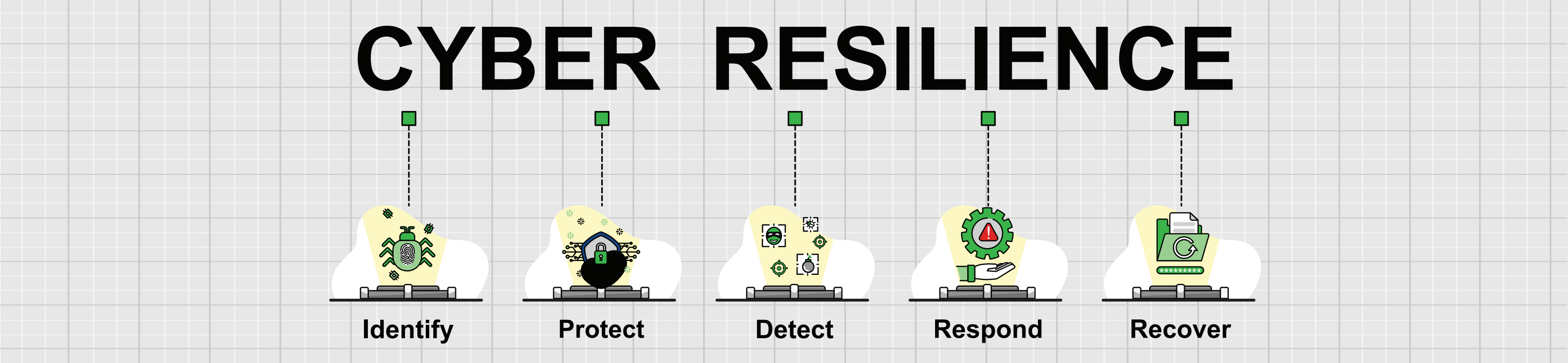
The Framework Profile - Represents the alignment of standards, guidelines, and practices to the Framework Core and opportunities for improving cybersecurity posture by gap assessment

Part 2:

The Framework Implementation Tiers - Provide background on how an organization perceives cybersecurity risks and the processes to manage these risks. The levels describe the extent to which an organization's cybersecurity risk management practices demonstrate the features defined in the framework.

Cyber Resilient Framework

Cyber Resilience Framework provides the ability to recover from any cybersecurity threats by following the below process:



CYBER RESILIENCE

Identify

Protect

Detect

Respond

Recover

Identify

The enterprises must identify the critical assets, systems, and data. They must understand the resources that support all essential functions of the business. The cyber risks' criticality allows an organization to analyze business requirements and develop a strategy for risk management, risk assessment, governance, business environment, and asset management.

Risk management - This is to develop the organization's priorities, risk thresholds, and limitations. These assist in decision-making during operations.

Governance- It is necessary to manage and monitor an organization's operational, environmental, regulatory, risk, and legal requirements. Also provide Executive Oversight, and consider bringing automation using GRC Automation Software

Asset Management - Identifying facilities, systems, services, data, and personnel used to accomplish the organization's purposes.

Risk assessment - understanding the cyber risks in all operations, individuals, and assets in an organization and build comprehensive risk register and risk measurement matrix.

Business Environment - The definition of the organization's mission, objectives, stakeholders, and activities.

Protect

This is an essential part of an enterprise where the first line of security programs restricts the impact of any possible threat. It involves a prominent role in making sure that the critical services are delivered with proper protection. This function governs the limitation and control of secure access to business-critical data or applications to block data breach incidents.

It mainly functions on the below categories:

Secure technology - It aims to protect the removable communications, media, and controls networks. It majorly covers the technical aspects of security and implementation, reviews records of log and audit.

Data Security - This category revolves around supporting the integrity and confidentiality of data while also making it available. Stakeholders continuously monitor and manage the data that suits the organization's risk plans.

Maintenance - Preventing unauthorized access to critical business data/applications should be maintained with due care.

Awareness and Training - Educating and training the organization's personnel on the cybersecurity best practices to uphold organizations security strategies.

Information Protection Procedures - Appropriate security policies and procedures are leveraged here, and it is identified under the governance risk and compliance category of identity function of a framework.

Identity Management and Access Control - Establishing a secured identity and credential management systems related to the authorized users.

Detect

This involves constant monitoring to detect data breaches or any unusual behavior and quickly assess their criticality before damaging the system. This function work on the below:

Detection Processes - This covers the organization's definition of roles and responsibilities in detecting, assessing, and maintaining activities against cyber risks. It also aids in complying with the industry standards, which is tested and improved.

Continuous Security Monitoring- In this category, vulnerability assessment is executed through secured systems. Organizations need to closely monitor all the associated information and technology, identify security issues, and measure the existing security strength.

Anomalies and Events - Organizations must effectively assess the events recognized as anomalies and understand the criticality of the effect of these events.

Respond

This framework aims to develop an end-to-end incident response plan to support the capability of an organization and ensure business runs as usual in the face of any cyberattack or incident.

This involves the five major categories:

Response Planning - Once the cybersecurity incident is discovered, the execution of the response plan begins. This response plan should be carried during or after a cyber incident.

Communications - Once the response plans have been followed, the organization's relevant stakeholders are responsible for coordinating activities and may seek help from law enforcement if required. The stakeholders must share details of the cyber-attack event among the concerned individuals inside and outside the organization.

Analysis - This process involves further investigation and examination of the incident. Organizations should analyze the impact of the incident and must take further action to contain those incidents.

Mitigation - Mitigating the potential impact of the threat is of utmost importance and requires further action to prevent the cyberattack from spreading the damage.

Improvements - Based on the incident analysis, organizations should look for improvement areas and ensure to withstand future related events.

Recover

This aims to restore any damaged services or capabilities caused by a compromised cybersecurity breach and focus on making a timely return to normal business operations.

This function can be categorized into the following:

Recovery Planning- Depending on the timing of the incident, this can occur during or after the event has concluded. Recovery plans are expected to be implemented promptly, and all affected systems are expected to be supported, restored, and treated.

Improvements - This category focuses on lessons learned during and after the cybersecurity event and how to use them to enhance its security strategies.

Communications- This calls for coordination of efforts with relevant stakeholders. All recovery plans and strategies should be shared internally and externally with the appropriate stakeholders to reduce the damage and protect the organization's reputation.

Our Success Story in Providing Cyber Security Resiliency Maturity & Ransomware Protection Assessment

Objective

Assess current cyber security & resiliency controls maturity

Ability / effectiveness of current controls to recover in case of Ransomware attack

Assess Backup & restoration capabilities in event of any incident

Derive Target State for Cyber Security Maturity & Resiliency

Identify the gaps and propose recommendations

Services Offered

Review Asset inventory and Secure configuration

Assess Access Controls and Privilege Access Management

Assess configuration of logging, monitoring, and alerting systems

Review Email and Web Security Controls

Assess Technical controls on Network and Application Security

Assess Data Protection and Data Recovery controls

Review Security Awareness and Training

Value Delivered

Performed Assessment by leveraging Digital GRC Automation Platform – Alyne

Assessment based on integrated controls based on NIST CSF, CIS and ISO 27001

Identified risk in current process & infrastructure and pragmatic recommendations remediate control gaps Articulate Roadmap to reach target maturity level

Conclusion

The above cybersecurity resilience framework is compatible with all business types: financial, health care, transport, education, and other sectors. Adopting a proper resilience framework is highly recommended. It exhibits the willingness of an organization to protect data and apply best security practices against evolving cyber risks. This eventually helps in reducing the financial and reputational damage of an organization.

A successful cybersecurity framework lies in visibility and diligence. With a hierarchical approach, organizations can enhance enterprise-wide incident response strategy that empowers them to manage threats quickly while maintaining the integrity and efficiency of their business model.

AUTHOR BIO

Sushil Kumar Nahar is a General Manager, IMSS at Happiest Minds Technologies. He is Post Graduate Certificate of Management Studies from Universitas 21 Global Singapore and a Bachelor's in Engineering (Electronics), with 30+ years of IT experience. Sushil is a tenacious business leader with unique techno-functional expertise in IT Security, Governance Risk & Compliance, and Business Resilience Consulting. Sushil steered higher customer experience, practice Competency development and deployment, focusing on reducing the cost to serve. He also represented at many conferences as a distinguished speaker.