

The Shift Towards Cyber Resiliency

Alanood A. Al-Shehry Saudi Aramco

October 18th, 2017

Are you cyber resilient?

The Definition of Cyber Resiliency

According to Homeland Security, it is the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions.

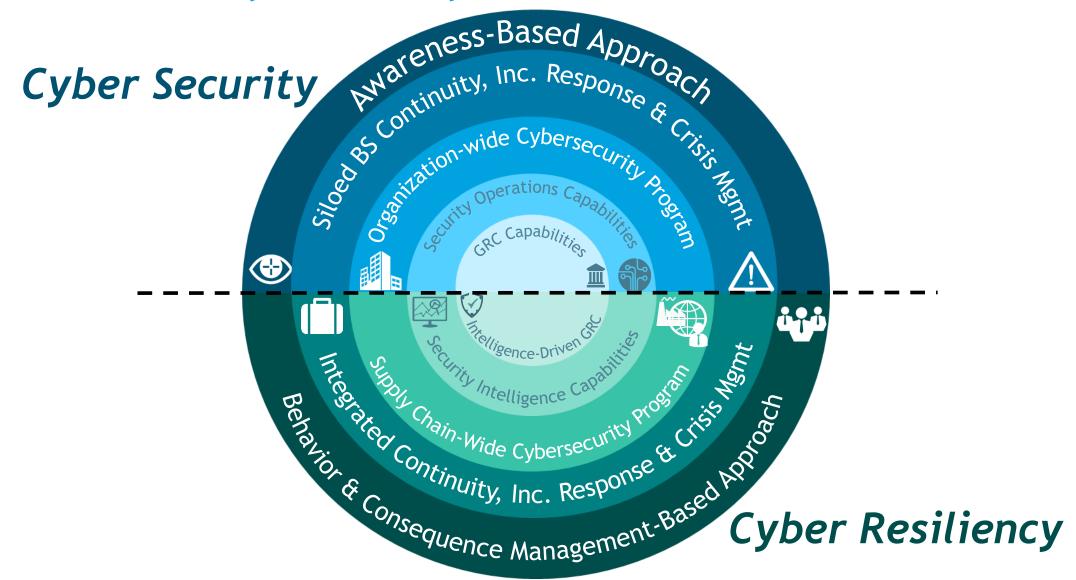
MITRE According to Mitre, it is about anticipating, withstanding, recovering, and evolving operations in the face of advanced cyber threats.

According to itgovernance, it is a broader approach that encompasses cybersecurity and business continuity, and aims not only to defend against potential attacks but also to ensure survival following an attack.



Cybersecurity Resiliency Overview

The Shift Towards Cyber Resiliency



Cyber Resiliency: Time for a PARADIGM SHIFT!

The Shift Towards Cyber Resiliency

Cyber-attackers have:



Cyber-attacks will be made against your organizations and will be successful!

The Shift Towards Cyber Resiliency The Mindset!

Cybersecurity







Cyber Resiliency

We may be targeted and an attack may occur



We are targeted and a breach is inevitable

We monitor security events to detect cyber attacks



We rapidly respond and recover from cyber attacks with minimal disruptions

We follow a compliance-based method to check against cybersecurity policies



We simulate cyber-attacks to test cyber resiliency

We focus on achieving security through management of known cyber risks and threats



We prepare to deal with severe impacts from unknown cyber risks and threats

Cyber Resiliency and Risk Management

What is False Sense of Security?

Lack of effective cybersecurity processes and undefined roles and responsibilities that could lead to false sense of security.

What does it translate into?

Technology Deployment



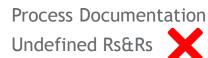
Organizational Chart





Manpower Capabilities

• Authority and Mandate





Process Management



Performance Measurement



Organization Establishment



Technology



Limited scope





Cybersecurity Resiliency Implementation

Cyber Resiliency Pillars

Identify ->

- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy

Protect

- Access Control
- Data Security
- Protection Processes
 & Procedures
- Protective Technology
- Training & awareness

Detect

- Anomalies and Events
- Security Continuous Monitoring
- Detection Processes

Respond

- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

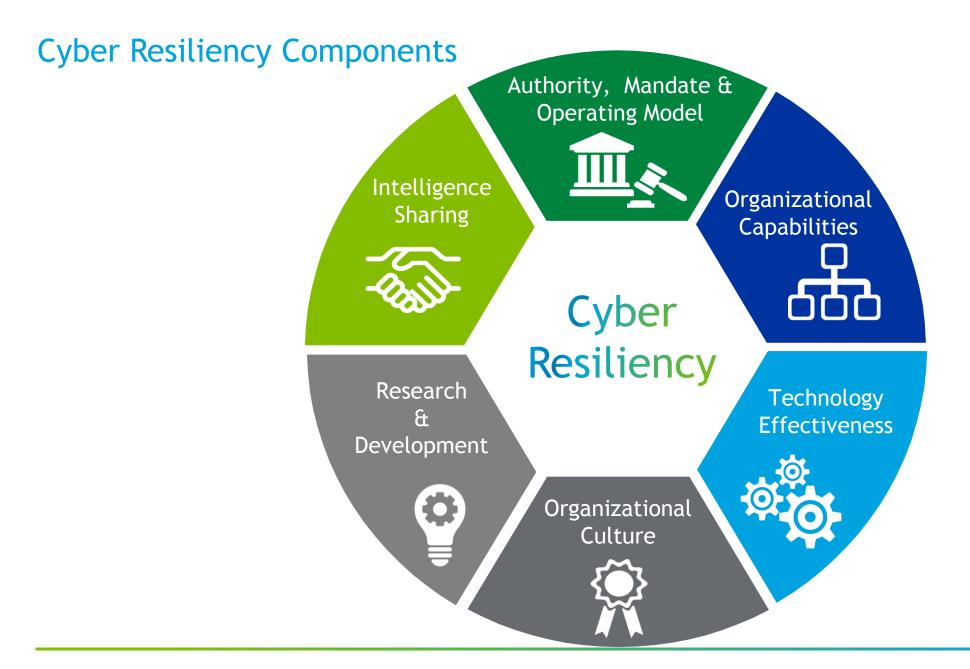
Recover

- Recovery Planning
- Improvements

-NIST Cybersecurity Framework

Communications

Resiliency



Cyber Resiliency Maturity Index

Networked Highly connected to **Pervasive** their peers and partners Leadership take full Top Down Share information ownership of cyber and jointly risk management mitigating cyber CEO has set the tone **Fragmented** risks. Developed policies for cyber risk and frameworks management Staff show Recognize potential exceptional cyber Defined **Unaware** • There is a top-down sources of risk responsibilities, and awareness risk response program reporting Siloed and • The organization is Organization sees mechanisms Does not view cyber fragmented an industry leader cyber risk as largely risk management as a approach to cyber irrelevant. competitive risk advantage Cyber risk does not form part of organization's

management process.

Paving The Road to Resiliency



Thank You