CENTRUL NAȚIONAL DE RĂSPUNS LA INCIDENTE
DE SECURITATE CIBERNETICĂ – CERT-RO

ISACA

Cyber resilience

Authors: Authors: Theodor Adam, Florin Andrei, Larisa Gabudeanu, Victor Rotaru

Cyber Resilience became important because traditional security measures are no longer enough to protect the organization. In our days, we cannot be only reactive to cyber threats. We need to build for our organizations the capability to anticipate, prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions.

Cyber Resilience is the measure of an organization’s ability to continue to work normally while attempting to *anticipate*, *prevent* and *detect* any cyber threats, applying *correct*ions to the operational environment if needed, and *respond* to, and *recover* from those cyber threats. An organization is cyber resilient when it can *defend* against cyber threats, has an efficient *cyber security risk management* in place and can guarantee *business continuity* during and after cyber incidents.

The goal of cyber resilience is to maintain the entity's ability to deliver the intended outcome despite adverse cyber events.

In order to establish and maintain cyber resilience within organization, we need to involve everyone working or doing business with that organization. In this respect, we should consider prevention as highly important for cyber resilience as well as user training and awareness. Let’s not forget that the goal of cyber resilience is to keep the organization operational even in unexpected circumstances.

In order to establish an effective cyber resilience we should have:

1. A well-defined strategy to drive properly and to improve continuously the cyber resilience implementation;
2. A clear understanding of what the organization’s critical assets are;
3. A clear view of the organization’s key threats and vulnerabilities;
4. An assessment of the organization’s cyber resilience maturity;
5. The design of appropriate cyber resilience plans using best practices and guidance;
6. An appropriate balance of controls to prevent, detect and correct issues in the operational environment;

7. An appropriate incident response process to assure effective response to security incidents and to assure proper escalation to business continuity and disaster recovery plans if required.
8. A continual review and improvement process allowing the fine tuning of the cyber resilience implementation;

A strong cyber resilient program ensures continuity of operation with minimum impact to business despite any incident. As an operational capability, cyber resilience is an iterative process providing the means to anticipate, identify, protect, and detect an attack, and respond and recover from it needed. The following mindmap depicts this iterative process:

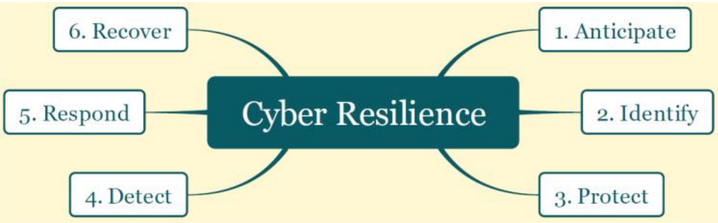


Figure 1: Cyber Resilience iterative process

The operational capability presented in the above figure is not enough to assure Cyber Resilience within our organization. We will consider them as operational objectives of Cyber Resilience, but we need more than the operational capability to build our Cyber Resilience Framework.

Moving further from the eight requirements defined above, we can conclude that for cyber resilience framework we need: strategy, design, transition, operation and continual improvement. If we look to the available frameworks, the one containing all these components is ITIL. The below figure presents the ITIL framework.

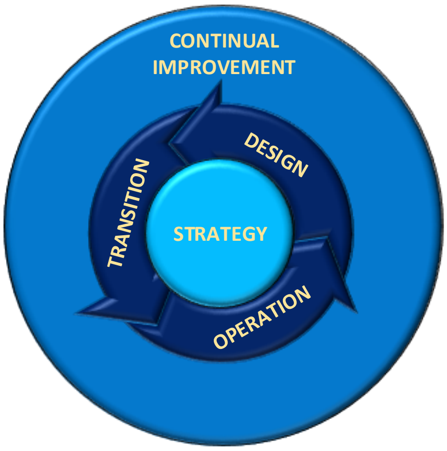


Figure 2: ITIL Framework

Many organizations have ITIL in place and are familiar with the ITIL framework. It became a standard for the IT organization worldwide and it is a strong and mature framework. Because it contains all the required elements we need to define a solid framework, it makes sense to use this framework also for cyber resilience. Our goal is to build a prioritized, scalable, and cost-effective path for our organization to be cyber-resilient.

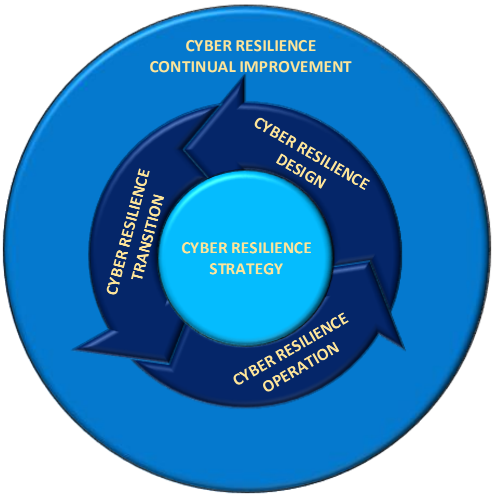

CYBER RESILIENCE CONTINUAL IMPROVEMENT
CYBER RESILIENCE DESIGN
CYBER RESILIENCE TRANSITION
CYBER RESILIENCE STRATEGY
CYBER RESILIENCE OPERATION

Figure 3: Cyber Resilience Framework

Let's depict the content of each component of the Cyber Resilience Framework presented in the above figure:

1 Cyber Resilience Strategy

The cyber resilience strategy must cover the entire product lifecycle as well as supporting business operations. Good cyber resilience is a complete, collaborative approach driven by the organization's board, but involving everyone in the organization focusing on people, suppliers, and resources. Effective cyber resilience requires an organization-wide risk-based strategy that proactively manages the vulnerabilities, threats, risks and impacts on its critical information and supporting assets.

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.

We need to ensure that cyber resilience activity is based on clearly understood objectives and supports the achievement of the organization's goals and it is aligned with the organization's strategy.

Both strategies have in common the organization's critical assets. So, we need to identify the organization's critical assets (what services, information and systems are the most important for the business) and what are the potential threats they might face.

The Cyber Resilience Strategy should outline:

- The importance of Cyber Resilience for the organization;
- The organization's vision and mission regarding Cyber Resilience;
- The organization's Cyber Resilience objectives;
- The organization's cyber risk appetite;
- The organization's stakeholders high-level requirements;
- The framework, and high-level approach to Cyber Resilience;
- The organization's resilience targets and implementation plan;
- A narrative about how the cyber resilience program will be delivered, managed and funded;

- A roadmap on how to continuously improve Cyber Resilience Maturity within organization;

The following are some representative success factors for a strong Cyber Resilience implementation:

- A clear understanding of the cyber resilience program ownership;
- A clear definition of roles and responsibilities;
- The alignment between the Cyber Resilience Strategy and the Business Strategy;
- A correct and complete identification of the organization's critical assets;
- A clear view of the organization's key threats and vulnerabilities, particularly those targeting critical assets;
- An appropriate balance of controls to prevent, detect and correct security issues;
- An appropriate incident response process to assure effective response to security incidents;
- An internal audit process helping with the monitoring and measurement of the implementation progress, adequacy and effectiveness of the cyber resilience program;
- An assessment process for the organization's cyber resilience maturity and design of appropriate plans to improve it using best practices and international standards and guidelines as guidance;
- Regular review and update of the cyber resilience strategy to ensure that organization can continue its business operation regardless the evolution of the cyber risk environment;

According to NIST 800-160 Volume 2[1] publication, "…any discussion of cyber resiliency is predicated on the assumption that adversaries will breach defenses and that, whether via breaches or via supply chain attacks, adversaries will establish a long-term presence in organizational systems. … The assumption of a sophisticated, well-resourced, and persistent adversary whose presence in systems can go undetected for extended periods is a key differentiator between cyber resiliency and other aspects of trustworthiness."

Remember that Cyber Resilience is about anticipating.

2 Cyber Resilience Design

We can consider that we achieved resilience when any of our critical assets, as were identified in the Cyber Resilience Strategy, is capable to return to its normal healthy range or one close to it regardless the security incident it faces. This capability can be achieved for the new information systems we build, but for all critical assets it cannot be achieved overnight because at least some of them are not aligned with cyber resilience practices and the alignment is not an easy task.

One of the Cyber Resilience Design's challenges is to rearchitect the current information systems (to rearchitect the existing critical assets) in order to apply cyber resilience practices. This may include redesigning and reimplementing or replacing existing cyber resources. For the new information systems we build, we just add those principles in the requirements and design phases, but for the existing information systems the changes to apply cyber resilience practices are not always applicable because of technical limitations and then we will need to replace components or even the entire technical solution.

Cyber Resilience practices are approaches that are applied to the architecture or design of business functions and cyber resources in order to achieve cyber resilience objectives.

According to MITRE Cyber Resiliency Framework PR 11-4436[2] publication, "3.2 Information Systems Security Engineering", "Some security engineering principles are specific to resilience (Stoneburner, et al., 2004):

"Principle 16. Implement layered security (Ensure no single point of vulnerability).

Principle 17. Design and operate an IT system to limit damage and to be resilient in response.

Principle 18. Provide assurance that the system is, and continues to be, resilient in the face of expected threats.

Principle 19. Limit or contain vulnerabilities.

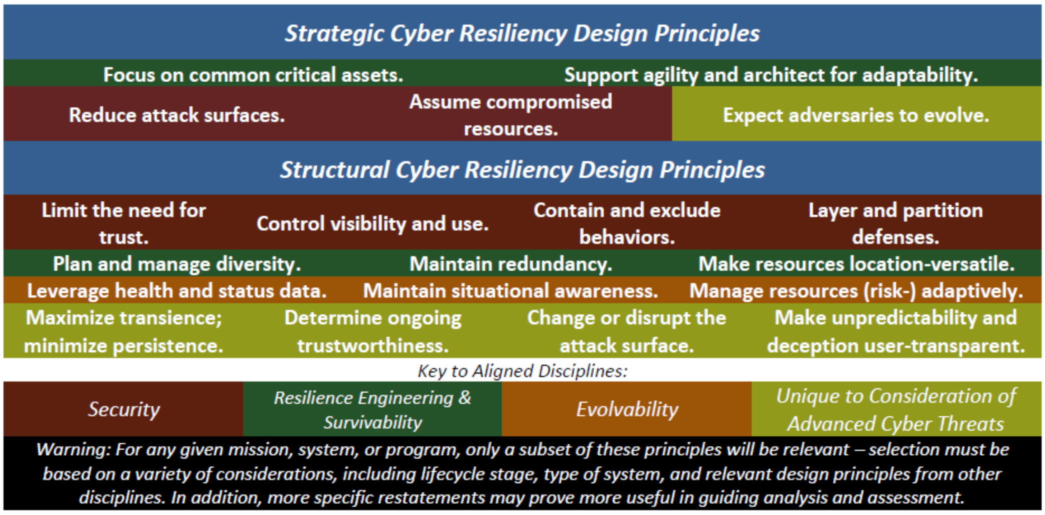
Principle 20. Isolate public access systems from mission critical resources (e.g., data, processes, etc.).

Principle 21. Use boundary mechanisms to separate computing systems and network infrastructures.

Principle 22. Design and implement audit mechanisms to detect unauthorized use and to support incident investigations.

Principle 23. Develop and exercise contingency or disaster recovery procedures to ensure appropriate availability."

As defined by MITRE Cyber Resiliency Design Principles PR 17-0103[3], "2 Representative Cyber Resiliency Design Principles", the below figure shows representative cyber resiliency design principles:



Strategic Cyber Resiliency Design Principles

Focus on common critical assets. Support agility and architect for adaptability.

Reduce attack surfaces. Assume compromised resources. Expect adversaries to evolve.

Structural Cyber Resiliency Design Principles

Limit the need for trust. Control visibility and use. Contain and exclude behaviors. Layer and partition defenses.

Plan and manage diversity. Maintain redundancy. Make resources location-versatile.

Leverage health and status data. Maintain situational awareness. Manage resources (risk-) adaptively.

Maximize transience; minimize persistence. Determine ongoing trustworthiness. Change or disrupt the attack surface. Make unpredictability and deception user-transparent.

Key to Aligned Disciplines:

Security | *Resilience Engineering & Survivability* | *Evolvability* | *Unique to Consideration of Advanced Cyber Threats*

Warning: For any given mission, system, or program, only a subset of these principles will be relevant – selection must be based on a variety of considerations, including lifecycle stage, type of system, and relevant design principles from other disciplines. In addition, more specific restatements may prove more useful in guiding analysis and assessment.

Figure 4: Representative cyber resiliency design principles, MITRE PR-17-0103

3 Cyber Resilience Transition

The scope of this phase is to test the correct operation of the technology, controls and procedures. At this stage, we can refine the incident detection for our critical assets. At the end of this stage, we will move our implementation to production (to operational use).

At this stage we ensure that the risks introduced by the change of the operational environment through the technology and/or controls we implement are minimized through rigorous testing. Testing should be based on standard testing framework (ISO/IEC/IEEE 29119 for example for software testing). In transition to production, during testing, we need to ensure that we do not introduce vulnerabilities into the operational environment, vulnerabilities that can be exploited by hackers. As a minimum, the testing should include test against the latest OWASP top 10 risks (https://owasp.org/www-project-top-ten/).

Another important aspect of the transition phase is the users and IT staff training. Without appropriate training, users and IT staff will not have good knowledge to operate the system and will cause errors, security incidents and breaches. From cyber resilience point of view, the training session should include:

- Acceptable use policy;
- Data protection and secure data handling;
- Principles and procedures for secure information disposal;
- Secure operating procedures;

4 Cyber Resilience Operation

The goal of this stage is to operate the technologies, controls, and procedures, and to detect and manage cyber security and cyber resilience related events and incidents. This includes continual evaluation of the implemented controls in order to ensure they are effective and consistent.

As presented in the above figure, the operational objectives we can consider for this stage are the following:

- Anticipate potential threats against the operational environment. Prevention is the key factor and the ability to anticipate the next move of threat actors makes effective the measures taken to protect the organization.
- Identify potential threats against the operational environment. The ability to identify from earlier moments a potential threat.
- Protect critical infrastructure services. Limit or contain the impact of any potential threat.
- Detect strange events and suspected data breaches or data leaks before major damage occurs. This demands constant security monitoring.
- Respond to a detected security breach or failure. An end-to-end incident response plan to ensure business runs as usual in the face of a cyber-attack.
- Recover to restore any affected infrastructure, capabilities or services that were compromised during a cybersecurity incident. Making a timely return to normal efforts.

5 Cyber Resilience Continual Improvement

Continual Improvement ensures that cyber resilience continue to provide the protection as needed. After each event, including incidents there are experiences and lessons learned. All these experiences can lead to modifications of procedures, design, technology, strategy and will need to update the training for users.

Effectiveness of the implemented controls should be measured continuously in order to ensure that they operate as desired.

Risk assessment should be performed on both our organization and third parties interconnected or connecting to our organization.

Improvement ideas and suggestions should be part of the cyber resilience maturity increase roadmap and should be prioritized according to urgency for improvement needs of the cyber resilience program. There are two questions you should get answer to regarding cyber resilience maturity: What maturity level do you think is appropriate for our cyber resilience? Why is this the right level of maturity?

6 Conclusions

Cyber resilience should be a complete, collaborative approach driven by the board and involving every employee and business partner.

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.

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

Let's not underestimate the potential risks regarding user training and third-party suppliers.

User training and awareness is as important as the implementation itself. Well trained and aware user will provide valuable support to protect organization's critical assets.

Poorly secured cyber suppliers are a huge vulnerability that can be easily exploited by cyber threats and expose the organization to significant damages as well as to regulatory and legal penalties.