UDC 004.056.5

Defining of Goals in the Development of Cyber Resilient Systems According to NIST

Oleksandr Bakalynskyi[1], Fedir Korobeynikov[1]

[1] *Pukhov Institute for Modelling in Energy Engineering, Kyiv, 02000, Ukraine*

Abstract

This paper introduces an approach to defining goals in the development of cyber-resilient systems, following the guidelines established in the standards of the National Institute of Standards and Technology (NIST) in the United States. This work aims to provide a roadmap for researchers and practitioners of cyber resilience in creating information systems capable of withstanding and adapting to adverse conditions, malfunctions, and attacks while ensuring the guaranteed execution of all primary cyber-system functions.

Keywords: cyber resilience, NIST, framework, goals, anticipation, resistance, recovery, adaptation

Introduction

The need for resilient systems in our era becomes increasingly relevant. With a constantly changing threat landscape, intensifying political, social, and climatic instability, total digital network globalization, and growing reliance of most of the planet's inhabitants on technologies to access basic services, standard cybersecurity strategies can no longer ensure system resilience.

Acknowledging the fact that the current level of technology essentially precludes guaranteeing full security of information assets, NIST developed standard SP 800-160, Volume 2 Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, which prescribes a new approach to system trustworthiness by creating adaptive mechanisms. These absorb the impacts of destructive incidents, attacks, or internal failures and maintain the functionality of critical processes of missions or organizations.

This research focuses on the process of defining, aligning, and developing proposals for the implementation of goals in building resilient systems according to NIST.

The aim of the study is to identify the practical aspects of the high-level construct "GOALS" of the cyber-resilience building framework developed by NIST, which encompasses: justification for implementing resilience in an organization; highlighting its key differences from cybersecurity; aligning resilience goals at all organizational levels; determining those responsible for implementation; and creating high-level mechanisms for monitoring the effectiveness of achieving these goals.

1. Concept of Cyber-resilience

The second volume of the standard 800-160 is focused around the concept of cyber-resilience. Its definition is provided as follows: «Cyber-resilience is the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources» [1].

It's also noted that «all discussions of cyber resiliency focus on assuring mission or business functions and are predicated on the assumption that the adversary will breach defenses and establish a long-term presence in organizational systems» [1]. Thus, it immediately underscores the difference from standard cybersecurity strategies that include instructions for systems designed with a focus on ensuring the confidentiality, integrity, and availability of information assets (cybersecurity goals). In the second volume of the standard, the primary focus is on guaranteeing the viability of critical systems that include cyber resources - by integrating resilience elements, it is proposed to provide the ability to anticipate attacks, withstand them, recover, and adapt to threats

(cyber resilience goals), ensuring the execution of their assigned missions, regardless of malfunctions, adverse conditions, stresses, attacks, compromises, etc.

2. Cyber Resilience Engineering Framework

NIST Special Publication 800-160, Volume 2, considers: the framework for building cyber resilience; cyber resilience constructions that are part of this framework; the concept of using the framework; as well as considerations for implementing cyber resilience into the life cycle of systems, companies or organizations. Constructions are the basic elements (i.e., building blocks) of the framework and include goals, objectives, methods, approaches to implementation, measures to mitigate risks and consequences, and design principles.

The framework focuses on cyber resilience, which, although related to cyber security and fault tolerance, has a distinctive structure for identifying its problem field and solution field.

While SP 800-160, v.2 is focused on cyber resilience engineering, the high-level concepts (i.e., goals, objectives, and methods of ensuring cyber resilience) are defined in such a way that they can be applied in a broad context. Their definitions are written in a technology-neutral manner and do not mention cyber resources.

The goals and objectives of cyber resilience define "what" cyber resilience is - that is, what properties and behaviour are inherent to cyber-resilient systems (Figure 1).

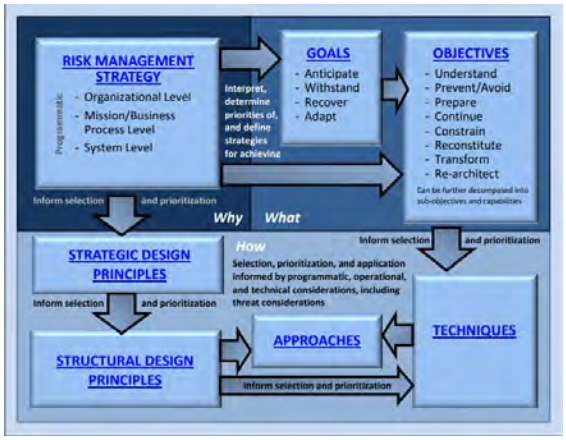

Figure 1: Relationships among cyber resiliency constructs (NIST SP 800-160, 2.1.5)

3. Goals of Cyber Resilience

Goals are high-level articulations of desired outcomes that are common to many definitions of resilience. They are included in the cyber resilience building framework to provide a link between risk management decisions at the system level, mission level, and business process level, as well as at the organizational level [1]. Organizational risk management strategies can use cyber resilience goals and associated strategies for cyber resilience integration.

Cyber resilience goals are not so much ultimate goals as they are current strategic tasks that shape the operational landscape of an organization. They are the cornerstone of the NIST cyber resilience building system and are vital for developing a comprehensive cyber resilience strategy. These goals guide risk management decisions at various levels - systems, missions, business processes, and the organization. They provide a more unified approach to risk management, bridging gaps between different organizational levels and promoting a culture of proactive cyber resilience.

In line with the definition of cyber resilience, it is important to understand that desired outcomes go beyond simply preparing for and responding to cyber threats. They also include the ability to evolve and adapt under the influence of these threats, thereby improving the overall cyber capabilities of the relevant organization. Cyber resilience is not a static quality but a dynamic one that requires continuous development and improvement.

To understand the essence of cyber resilience and how it differs from cybersecurity, it is necessary to consider each of the goals described in the framework:

ANTICIPATE: This goal focuses on proactive measures to predict and identify which system elements are most important for the organization's operations and are vulnerable to sophisticated professional attacks, unpredictable failures, or incidents. All risks with a critical level of harm, regardless of the likelihood of their realization, must be considered and processed by applying resilience solutions to them, assuming that the threat, however unlikely and complex in realization it may be, will still be realized.

Threat intelligence, risk assessment, and predictive analytics play a key role in achieving this goal. It is not enough to simply respond to

threats; organizations must anticipate them, implementing resilience elements in the most critical and weak elements of the organization's operational system.

NIST advocates a proactive, anticipatory stance on threats. This involves conducting comprehensive operations to scout for new types of threats to identify potential attack vectors and predict new threats. It also includes regular audits and stress testing of systems to detect vulnerabilities before they can be exploited. Such forward-thinking should permeate all levels of the organization, encouraging vigilance and continuous learning.

This goal also involves developing a culture of awareness, education, and constant vigilance.

WITHSTAND: The cyber resilience framework helps to create an additional protective contour for the organization that is activated when cybersecurity elements cannot cope with an attack, failure, or adverse event. The practical realization of this goal means that resilient systems should be capable of withstanding adversity, guaranteeing minimal necessary functionality (for example, satisfying critical mission needs). New cyber threats can be tested on a range or in an isolated environment with the aim of determining the system's ability to withstand them. Understanding the limitations of individual entities, organizations, and systems is crucial.

Resilience should also be achieved through protective measures to prevent cyber threats from becoming real attacks. These measures could include implementing multi-tiered defense strategies, developing secure software and systems, using reliable encryption, and maintaining proper cyber hygiene. However, this also extends to the human elements of cyber resilience: employees must be trained to recognize and resist social engineering attacks, for example. The aim here is to strengthen the organization's defense using methods that do not fall within the information security framework.

RECOVER: The ability to quickly restore normal operation after a cyber incident is crucial for cyber resilience. Swift and effective recovery can significantly mitigate the impact of the incident on the organization's operations, performance, and reputation.

Recovery is a multifaceted process. It involves not only the technical aspects of restoring systems and data after an incident, but also managing the broader consequences of a cyberattack. This could include communication strategies for managing reputational damage or legal considerations in the event of a data breach. The NIST cybersecurity framework [2] includes a "Recovery" function, which provides guidance on the development and implementation of robust recovery plans.

In line with the goals set out by SP 800-160 vol.2, systems should not only withstand and recover from blows, but also undergo iterations, as a result of which they will become even more reliable.

ADAPT: Perhaps the most important aspect of cyber resilience is the ability to continuously accumulate information about incidents, vulnerabilities, new technologies, and adversaries and accordingly adapt strategies. This can include reviewing security policies, enhancing threat intelligence, and reassessing risk management strategies, which should occur with a certain regularity.

During an attack, a resilient system must be able to quickly adapt, find new resources, and adjust (even with reduced functionality) to perform its primary tasks and minimize damage from potential threats and attacks.

Continuous learning and system evolution are keys to maintaining resilience in a constantly changing cyber threat landscape. It is precisely this adaptability, combined with a reliable approach to anticipating, withstanding, and recovering from cyber threats, that defines a truly resilient organization.

The goals are not linear stages that need to be executed one after another, but rather intersect and are interdependent aspects of cyber resilience.

A key feature of this part of the framework concept is the assumption that all four goals must be addressed simultaneously. For example, even while withstanding a cyberattack or recovering from it, mission or organization management structures should anticipate other attacks. Even when predicting, withstanding attacks, or recovering from them, mission/business segments, as well as mission or business processes that rely on them, continuously evolve to meet the changing operational and technical environment.

At all levels of the framework, the approach to cyber resilience has a cyclical and continuous nature. Regardless of the stage the organization is at - predicting future threats, resisting attacks, recovering from incidents, and adapting strategies must be constant processes.

According to NIST SP 800-160, v 2, defining and agreeing on cyber resilience goals is a collaborative work involving various stakeholders in the organization. This process should be guided by the organization's Risk Management Strategy (RMS) and be integrated into the Risk Management Framework (RMF).

NIST states that the Risk Management Executive (function) is responsible for this process, ensuring that issues related to security risks for individual information systems are considered from an organization-wide perspective in relation to the overall strategic goals and objectives of the organization in carrying out its mission and business functions. They also ensure that risk management related to individual information systems is coordinated across the organization, reflects organizational risk tolerance, and is considered along with other organizational risks affecting mission/business success.

The risk management function can be assigned to a group, which typically includes senior-level managers. They must first have full information about the organization's priority goals and the critical processes without which the organization cannot operate at a level sufficient to achieve these goals. Secondly, they must have the authority to make decisions based on risk assessments that affect the organization as a whole. All managerial roles in the organization should cooperate to perform tasks related to risk management. This includes setting and agreeing on cyber resilience goals. These goals should reflect the results of risk assessment and should be supplemented with tasks in such a way as to ensure resilience, primarily, of the most critical systems, operations, and data of the organization.

In light of the fact that objectives constitute high-level constructs of the cyber resilience framework, the metrics that evaluate the level of their achievement must hold constructively significant value for making strategic decisions at the higher echelons of organizational hierarchy. Concurrently, to ensure comprehensive understanding and acceptance of these metrics, the results must be presented in a manner that makes them accessible and comprehensible to individuals lacking specialized knowledge at all levels of the organization.

Taking these factors into account and given the lack of clearly defined metrics in NIST standards to assess high-level resilience goals, it is suggested that the metrics below be used regularly and that a longitudinal method be applied to track the dynamics of change.

For the goal of ANTICIPATE, an apt metric would be the uptime metric, which measures the duration of uninterrupted operation of critical systems.

Uptime represents the percentage of time during which the organization's or mission's critical systems are operational and available for use. It is calculated as: (((Total time - Downtime) / Total time) ×100%).

This is an indicator of effective resilience, and the better the conscious preparedness, the better the planning for unforeseen situations, the higher the value will be when calculating this metric.

To understand the success of achieving the WITHSTAND goal, organization's management needs to know what percentage of all incidents related to critical processes and systems did not cause downtime in the organization's work. For this, from the total number of incidents aimed at critical systems, subtract the number of incidents that led to downtime (critical incidents), divide the obtained value by the total number of incidents aimed at critical systems, and multiply by one hundred percent. A higher percentage will mean a higher level of the organization's resilience, and express its ability to resist attacks and adverse conditions.

The widely-used metric Mean Time To Repair (MTTR) is a vivid indicator of the RECOVER goal. Incidents are inevitable, but resilient systems must recover quickly.

The mean time to resolve an issue is the average time needed to fix a failure or the effects of an attack, and restore the operation of critical systems.

It is calculated as: Total downtime of critical systems / Number of critical incidents that led to these downtimes.

The effectiveness of high-level adaptation of an organization's or mission's systems (ADAPT) can be measured using the Mean Time Between Failures (MTBF) metric, which calculates the average time from one critical incident to the next (assuming adaptive changes are made to the systems after incidents).

MTBF is calculated as: (Total time - Downtime) / Number of critical incidents. An increase in the MTBF value indicates a higher resilience of the organization.

Conclusions

In the study, high-level resilience objectives were defined and analyzed according to the NIST framework. Definitions and purposes of each of the cyber resilience goals from the perspective of the organization as a whole were presented, as well as the key elements of interaction at all organizational levels when implementing resilience.

Metrics and a method were proposed for high-level evaluation and control of achieving resilience goals.

Key differences between cyber resilience and cybersecurity goals were explained.

References

[1] NIST Special Publication 800-160, Volume 2. Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, NIST, 2021. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf.

[2] NIST Cybersecurity Framework, NIST. 2018. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf .

[3] D.Bodeau, R. Graubart, J. Picciotto, R. Mcquaid, Cyber Resiliency Engineering Framework, MITRE, 2011.URL: https://www.mitre.org/sites/default/files/media/publication/11_4436_2.pdf .

[4] Definition of term “risk executive (function)”. Glossary of Computer Security Resource Center (CSRC), NIST. URL: https://csrc.nist.gov/glossary/term/risk_executive.