DYNAMO

Dynamic Resilience Assessment Method including combined Business Continuity Management and Cyber Threat Intelligence solution for Critical Sectors

Follow DYNAMO on:

@DYNAMO_HEU dynamo_horizon

Factsheet 3: Resilience

Organisational resilience is the ability to absorb and adapt in a constantly changing environment to meet its objectives and prosper (ISO 22316). Resilience plays an essential role in the DYNAMO project as the prime metric used to assess the effectiveness of the solutions. DYNAMO approaches the security and resilience of a critical sector from two different directions: cyber threat intelligence and business continuity management (see **Factsheet 1** and **Factsheet 2**). The aim of DYNAMO is to combine these two interdisciplinary areas to create situational awareness for decision support, thereby also strengthening resilience. What exactly resilience means and how this will be implemented in DYNAMO is explained in more detail in this factsheet.

4Rs of Resilience of DYNAMO

DYNAMO measures the effectiveness (return of investment) of resilience enhancement measures in alignment to the 4 Rs of resilience framework. The general meaning of the 4Rs of Resilience - or the characterisation of Resilience - is explained in more detail below:

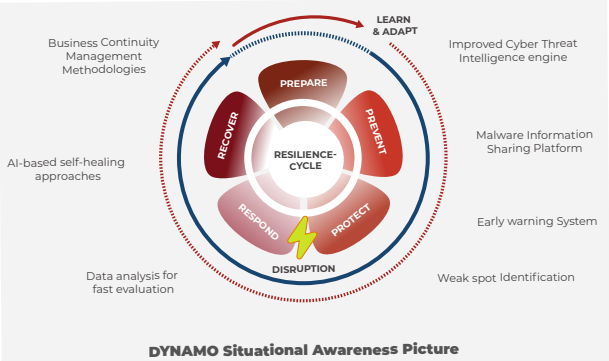
Rapidity: Ability to contain losses or prevent further degradation of the situation in a timely manner

Robustness: Ability of the system to stand a certain level of stress

Resourcefulness: Ability to mobilise resources in the event of a disruption

Redundancy: Measure of the inherent substitutability

Resilience Cycle



DYNAMO Situational Awareness Picture

The DYNAMO platform is usable across all phases of the resilience cycle to underline the benefit of the approach and solutions.

Preparation: Business stakeholders apply the DYNAMO platform to train and be prepared to respond effectively during a cyber-attack and generate shared situational awareness among platform users concerning their responsibilities.

Prevention: The existing ECHO Early Warning System will be extended to offer a C-level view support and an empowered threat intelligence collection, processing, and analysis engine, mainly with the generation and sharing of Early Warnings. Also, MISP will be used for increasing the channels and the collection of threat intelligence to be used for detecting and deterring relevant threats.

Protection: By identifying threats and vulnerabilities for critical assets, the system is protected and, in combination with the CTI that the DYNAMO platform has received and processed in order to tailor it to the user's needs, a desired level of business continuity is ensured.

Response: The BCM assessment with different levels of detail offers end-users with varying existent data a fast or detailed evaluation of a critical infrastructure. BCM response plans help to ensure the effectiveness of the response in case of an event.

Recover: Data-driven parameters from end-users helps to understand the interaction, the effect of disruptions. The use of AI solutions at this stage enhances the effectiveness and timeliness of the recovery while also meeting the requirements of the recently established NIS2 directive. This approach helps in quantifying the effectiveness of the responses and thus identifying efficient recovery methods/processes.

Adaption: The classification of system qualities, their interaction and alignment to the five resilience-phases allows the evaluation of a critical sector before, during and after a potential disruption.

The multilevel approach of DYNAMO addresses the five phases of the resilience-cycle and helps to:

- Identify critical assets and functions of a critical sector (**prepare**)
- Consider cyber-risks which are known, but also acknowledge the unknown (**prepare & prevent**)
- Save sensitive data (**prevent & protect**)
- Test the response plan to ensure the effectiveness (**response**)
- Train business stakeholders concerning their responsibilities before an attack with the simulation of a potential attack (**prepare**) and during an attack (**recover**)
- Integrate AI-based solutions to accelerate the recovery behaviour (**recover**)

The interdisciplinary DYNAMO approach characterizes resilience as basis to ensure business continuity with respect to potential cyberthreats.

The Resilience Assessment Methodology

The resilience assessment is applied within a three-level approach. Depending on the availability of end-user data and the chosen approach a fast or detailed assessment can be applied.

1. The qualitative assessment aims to get a fast result concerning the investigated critical sector. The development of a systematic questionnaire gives input to generate a balance-score card for evaluation and the identification of potential weak spots.
2. A semi-quantitative assessment helps to identify system qualities that are linked to single resilience phases. Main attributes have to be identified that contributes to single system qualities.
3. This approach gives an overview how resilient an investigated sector is in alignment to the five phases prepare, prevent, protect, response and recover.
4. The quantitative assessment is based on the determination of main performance targets that describes the critical sectors. This approach requires the development of an abstracted model. The model helps to identify and evaluate critical processes within the sector.

DYNAMO considers a systemic perspective on resilience according to which all relevant subsystems of an organisation need to be considered beyond the cybersecurity department to prevent, prepare, respond and recover effectively from threats.

Fraunhofer EMI · TECHNIKON · iti Information Technologies Institute · factorSOCIAL · LAUREA · NAVAL GROUP · Gemelli · KEMEA · KPMG Future Analytics · VISIONSPACE · telelink · RHEA · UCC · CRBC · CUBS · SystemX · Laborelec

Consortium
15 Partners
10 Countries

Budget
€ 5 Million
100% EU-funded

Duration
36 Months
10/2022 - 09/2025

Funded by the European Union under grant agreement no. 101069601. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.