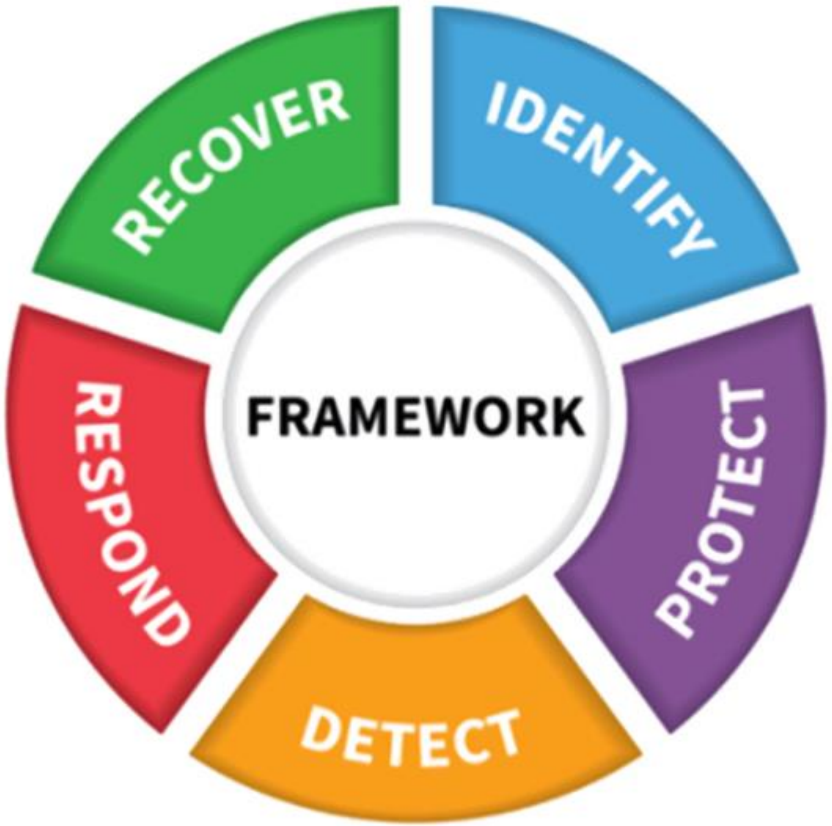
Co-funded by the
Erasmus+ Programme
of the European Union



Engine Syllabus

Chapter two –

The NIST Framework

ENGINE

Co-funded by the
Erasmus+ Programme
of the European Union

Introduction to the NIST Framework

What is the NIST Framework?

Why small businesses?

ENGINE

Co-funded by the
Erasmus+ Programme
of the European Union

What is the NIST Framework?

The NIST Cybersecurity outlines a policy framework[1] of computer security guidance to all sectors of the nation's critical infrastructure providing the access while supporting organisations that wish to use the Cybersecurity Framework CSF and improve their ability and skills in order to prevent, detect and respond to cyber-attacks at an organisation. This Framework provides an advanced cybersecurity taxonomy as well as the methodology to be used in assessing and managing the cybersecurity outcomes in an organization. Originally, the National Institute of Standards and Technology (NIST)[2], released the first Framework for Improving Critical Infrastructure Cybersecurity in February 2014, including recommended practices to various organizations and industries while today the framework documents are regularly being updated[3]. Finally, created NIST Framework is clear and reasonable to many professionals while it is flexible and can be customized to many technologies and industry sectors.

Co-funded by the
Erasmus+ Programme
of the European Union

Why small businesses ?

According to the European Union Agency for Cybersecurity[4], “Small and medium-sized enterprises (SMEs) are the backbone of EUs economy and they represent 99% of all businesses employing around 100 million people. Also, the SMEs account for more than half of Europe’s GDP and play a key role in adding value in all sectors of the EU economy”. However, Small businesses are not prepared in a best way to deal with cyber – threats (68% of SMEs have no systematic approach for ensuring cyber infrastructure) and many cyber criminals view them therefore as soft targets. Also, statistics[5] shows that 60% of all cyber-attacks or breaches were aimed at SMEs and the 60% of the SMEs which were victims, did not recover and had to shut down within sixth months. Also, nowadays small businesses are more connected to their customers, where offered solutions includes bring your own device (BYOD), home working and the cloud, and thus more open to threats. However, unfortunately small business does not have the resources (neither the personnel to deal with cyber-risks nor the budget) to invest in information security the way larger businesses can.

ENGINE

Co-funded by the
Erasmus+ Programme
of the European Union

What do small businesses need to be aware of?

ENGINE

Co-funded by the
Erasmus+ Programme
of the European Union

External Threats

Several reasons can cause cyber criminals to attack a small business (external threat), e.g., desire for easy profit, revenge, thrill of causing the mess, disclosing and accessing the SMEs valuable information, etc. For small business, the overall impact of cyber-attacks can have extremely high costs as they are often not prepared enough to handle incidents[6]. That includes:

- damages to information or information systems,
- regulatory fines and penalties / legal fees,
- decreased productivity,
- loss of critical information in running your business,
- loss of reputation and trust from customers,
- damages to your credit and inability to get bank loans, or
- loss of business income.

Co-funded by the
Erasmus+ Programme
of the European Union

Internal Threats

What must be taken into consideration is the human error and human vulnerabilities, as aspects of internal threats that result in some cyber breaches. Thus, it would be good for employees of the small businesses to be familiar with the cybersecurity basic methods and educate them in the cybersecurity practices.

It is of vital importance to consider how to protect business and balance between acquiring protection from cyber-attacks while creating proper and fair restrictions on employee device usage. However, it is not possible for any business to be completely secure, but it is vitally important to implement a program that balances security with the need and capabilities of the small business. Thus, implementing a strong information security program can help not only the organisation to gain and retain customers, employees and business partners but both customers and employees to protect their private and sensitive information from theft, disclosure and misuse.

Co-funded by the
Erasmus+ Programme
of the European Union

Sources

[1] Chapter 12 Cybersecurity framework, Security Controls Evaluation, Testing, and Assessment Handbook, Elsevier 2020 (https://doi.org/10.1016/B978-0-12-818427-1.00012-4)

[2]https://www.nist.gov/

[3]https://www.nist.gov/cyberframework/framework

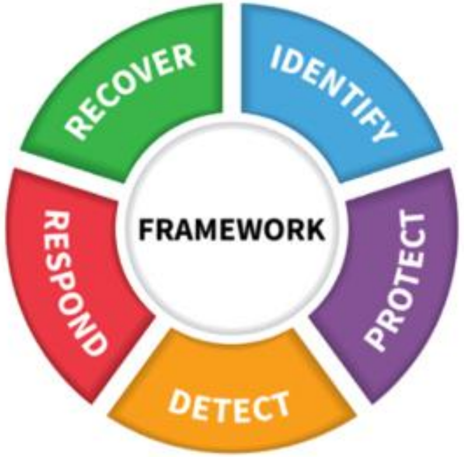
[4]https://www.enisa.europa.eu/events/workshop-on-enisa-report-cybersecurity-for-smes-challenges-and-recommendations

[5]https://docs.broadcom.com/doc/istr-24-2019-en

[6] NISTIR 7621 Revision 1, Small Business Information Security: The Fundamentals, National Institute of Standards and Technology 2016 (https://doi.org/10.6028/NIST.IR.7621r1)

Co-funded by the
Erasmus+ Programme
of the European Union

The five functions



This chapter 2 describes the Framework for Improving Critical Infrastructure Cybersecurity (the "Cybersecurity Framework"), organising the processes and various tools to be considered in protecting small business information. The specific mitigation activities in this section are grouped into the five broad categories of the NIST Cybersecurity Framework: **Identify, Protect, Detect, Respond and Recover**.

ENGINE

Co-funded by the
Erasmus+ Programme
of the European Union

1. Identify

IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER
FRAMEWORK

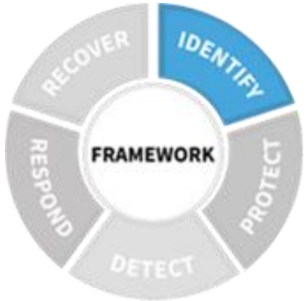
Objective

✓ Case Examples and Quick Wins

Recommended Activity Steps

Co-funded by the
Erasmus+ Programme
of the European Union

Objectiv
e

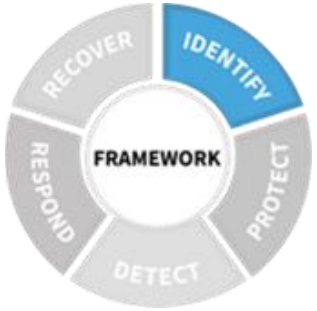


This Function, as the first category of the NIST Cybersecurity, assists to organization to understand the business context and related cybersecurity risks one can experience, while identifying the most important matters of the business that need to be protected.

Furthermore, the aim of the Identify Function is to support the SMEs with proper management of cybersecurity risks to systems, people, assets, data and capabilities and thus to enable the organization to focus and prioritize its effort, consistent with its risk management strategy and business needs.

Co-funded by the
Erasmus+ Programme
of the European Union

Case examples and Quick Wins



✓

Organization identifies physical assets and thus establishes/updates Asset Management program.

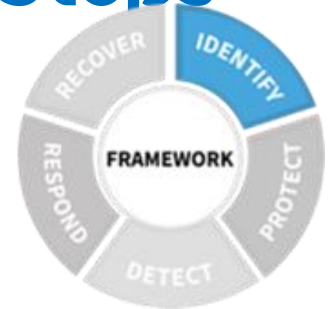
Organization identifies data and where the data and technology are stored and thus decides who has access to both.

Organization identifies Cybersecurity policy and thus the sensitive information and systems are protected.

Organization identifies the asset vulnerabilities and threats to internal/external organizational resources and thus prepares/updates organizations' Risk Assessment Procedures with risk response activities.

Organization identifies a Risk Management Strategy and thus establishes risk tolerances.

Recommended Activity Steps



Activity 1. Identify physical and software assets within the organization!

It is recommended to record the manufacturer, model, serial number and support information for hardware and software as well to know the specific version that is installed and running on the PC.

Activity 2. Determine who has the access to your business information!

It is very important not to allow an unknown or an unauthorized person to have physical access to any of business devices as they can relatively easily steal any private or sensitive information.

Activity 3. Request individual user accounts for each employee!

It would be desirable that each employee has strong and unique password on the business device ensuring no administrative privileges while they perform typical work functions.

Activity 4. Each employee controls the access to the business information!

It would be good to physically lock up the business devices when not in use, utilize the session lock feature included in operating systems and use a privacy screen or place the computer in a way that people walking by cannot see the information on the screen.

Activity 5. Establish policies and procedures for information security!

It would be best to create policies and procedures for information security describing the organization expectations for protecting the information and systems identifying acceptable practices and use it to train new employees and/or an investigation in case of an incident.

Activity 6. Carry out the background check!

It would be advisable to convey a criminal background, sexual offender and credit check on all prospective employees (especially on those handing the business funds).

Co-funded by the
Erasmus+ Programme
of the European Union

Sources

[1]https://www.nist.gov/cyberframework/online-learning/five-functions

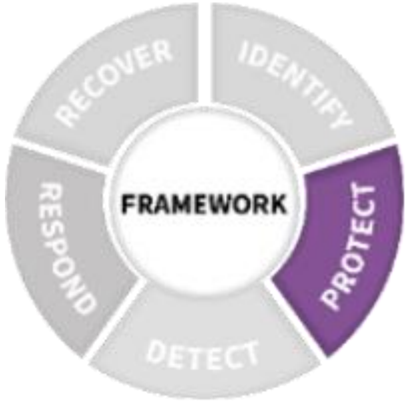
[2]https://staysafeonline.org/cybersecure-business/protect/

[3] NISTIR 7621 Revision 1, Small Business Information Security: The Fundamentals, National Institute of Standards and Technology 2016 (https://doi.org/10.6028/NIST.IR.7621r1)

ENGINE

Co-funded by the
Erasmus+ Programme
of the European Union

2. Protect



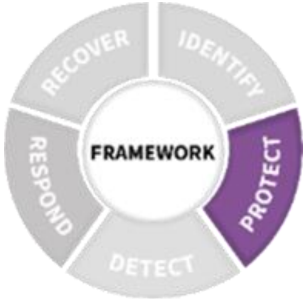
Objective

✓ Case Examples and Quick Wins

Recommended Activity Steps

Co-funded by the
Erasmus+ Programme
of the European Union

Objectiv
e

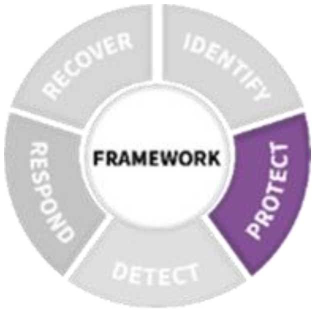


While the Identify Function of the NIST Cybersecurity is considered the foundation for an organization, the second Function of the NIST Cybersecurity, called Protect, shall be understood as a “frame” or “border line” that an organization establishes as solid and secure structure surroundings.

Thus, the Protect Function outlines appropriate precautions (know-how) to ensure delivery of critical infrastructure services. Furthermore, the aim of the Protect Function is to support the ability to limit or contain the impact of a potential cybersecurity event and protect the business.

Co-funded by the
Erasmus+ Programme
of the European Union

Case examples and Quick Wins



Organization protects physical and remote access of business data and information and thus has better Identity Management and Access Control.

Organization empowers employees through Awareness and Training and thus the staff responsiveness in cyber-attack is higher.

Organization establishes Data Security protection covering risk strategy and thus the confidentiality, integrity and availability of information is nor endangered.

Organization implements Information Protection Processes and Procedures and thus information systems and assets are maintained, UpToDate and protected.

Organization protects and maintains recourses (including remote maintenance) and manages technology to ensure the security and resilience of systems and thus organizational policies, procedures and agreements are implemented and reliable.

Co-funded by the
Erasmus+ Programme
of the European Union

Recommended Activity Steps

RECOVER
IDENTIFY
FRAMEWORK
PROTECT
DETECT
RESPOND

Activity 1. Enable automatic software updates!

It is recommended to use automatic software updates (i.e., for apps, web browsers and operating systems) as many software and security programs will automatically connect and update to defend against known threats, viruses, malware and other online risks.

Activity 2. Use strong password and passphrases!

It is very important to use strong authentication (at least 12 characters that are a mix of numbers, symbols and capital lowercase letters) to protect access to accounts ensuring only employees with permission can access them.

Activity 3. Encrypt sensitive data!

It would be desirable to encrypt all devices (e.g., laptops, tablets, smartphones, removable drives, backup tapes, cloud storage solutions) that contain sensitive personal information and make the electronically stored information unreadable to anyone not having the correct password or key.

Activity 4. Always back up the data!

It would be good to use either the cloud or separate hard drive storage and make electronic copies of the key information on a regular basis.

Activity 5.Use multi-factor authentication!

It would be best to require multi-factor authentication to access areas of your network with sensitive information that requires additional steps beyond logging in with a password, e.g., a temporary code on a smartphone or a key that’s inserted into a computer.

Activity 6. Limit access to data and/or systems!

It would be advisable to permit access to data and/or systems only to the employees who require it to perform the core duties of their jobs ensuring that when an employee leaves the business, they have no longer access to the business’s information or systems

Activity 7. Establish formal policies for safety!

It would be wise to have clear rules for employees informing them about what can be installed and kept on the work computers, pointing out not to open suspicious links in email, tweets, posts, online ads, messages or attachments (even if they know the source) while educating them how to use filters to prevent unwanted, harmful email.

Sources

[1]https://www.nist.gov/cyberframework/online-learning/five-functions

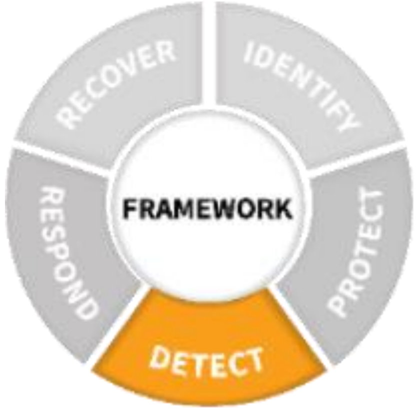
[2]https://staysafeonline.org/cybersecure-business/protect/

[3] NISTIR 7621 Revision 1, Small Business Information Security: The Fundamentals, National Institute of Standards and Technology 2016 (https://doi.org/10.6028/NIST.IR.7621r1)

ENGINE

Co-funded by the
Erasmus+ Programme
of the European Union

3. Detect



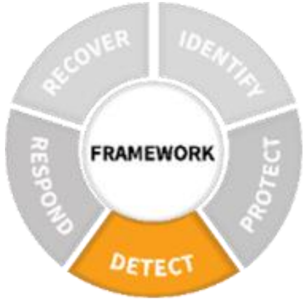
Objective

✓ Case Examples and Quick Wins

Recommended Activity Steps

Co-funded by the
Erasmus+ Programme
of the European Union

Objectiv
e

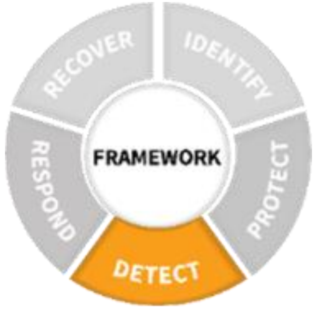


The third category of the NIST Cybersecurity is the Detect Function, that defines the appropriate activities and measures of an organisation to quickly identify the occurrence of a cybersecurity event in a timely manner while adopting the continuous monitoring solution to detect anomalous activity and other threats to operational continuity.

Basically, the Function is all about applying a know-how when something goes wrong while continuously tracking the threats as an effective way to analyze and prevent cyber incidents in Industrial Control System (ICS) networks.

Co-funded by the
Erasmus+ Programme
of the European Union

Case examples and Quick Wins



✓

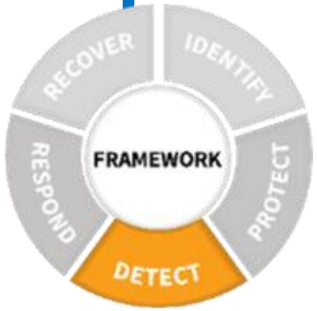
Organisation ensures Anomalies and Events are detected and thus their potential impact and consequences are understood.

Organisation implements Security Continuous Monitoring to monitor cybersecurity events and thus verifies the effectiveness of protective measures including network and physical activities.

Organisation maintains Detection Processes and thus continuously provide awareness of anomalous events.

Co-funded by the
Erasmus+ Programme
of the European Union

Recommended Activity Steps



Activity 1. Check network for unauthorized users or connections!

It is recommended to use and regularly update network monitoring service, cybersecurity tools and services (i.e., antivirus, -spyware and anti-malware programs) that helps detecting the incidents on organisation networks.

Activity 2. Monitor devises for unauthorized personnel access!

It is very important to keep an eye on devices (also USB and external drives) for unauthorized personnel access and software, and notice if someone is not following established policy and/or customers are acting suspiciously.

Activity 3. Empower the employees!

It would be good to train the employees on what incidents and attacks look like, present them unusual requests, attachments, links received through mails and how they need to react (report quickly).

Activity 4: Be prepared to investigate any unusual activities on your network!

It would be desirable to enable the capability of protection/detection hardware or software (e.g. firewalls, anti-virus) to keep a log of activity, as logs are valuable in case of an investigation and used to identify suspicious activity.

Co-funded by the
Erasmus+ Programme
of the European Union

Sources

https://www.nist.gov/cyberframework/online-learning/five-functions

https://staysafeonline.org/cybersecure-business/detect-incidents/

https://staysafeonline.org/cybersecure-business/detect-incidents/

NISTIR 7621 Revision 1, Small Business Information Security: The Fundamentals, National Institute of Standards and Technology 2016 (https://doi.org/10.6028/NIST.IR.7621r1)

ENGINE

Co-funded by the
Erasmus+ Programme
of the European Union

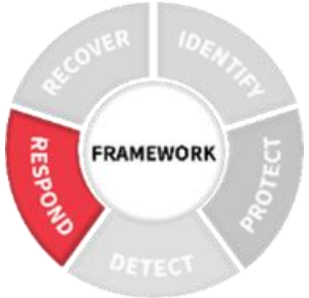
4. Respond

RECOVER
IDENTIFY
PROTECT
DETECT
RESPOND
FRAMEWORK

- Objective
- ✓ Case Examples and Quick Wins
- Recommended Activity Steps

Co-funded by the
Erasmus+ Programme
of the European Union

Objectiv
e



The fourth Function of the NIST Cybersecurity, is established to prepare an organisation to respond in a thoughtful and comprehensive manner and reduce risks to business while sending a positive signal to customers and employees.

The Respond Function is sustained plan that includes appropriate activities and mitigation measurements to be taken when incident occurs in order to minimize their impact while supporting the ability to contain the impact and maintain business operations in the short term.

Co-funded by the
Erasmus+ Programme
of the European Union

Case examples and Quick Wins

RECOVER
IDENTIFY
PROTECT
DETECT
RESPOND
FRAMEWORK
✓

Organisation develops and implements plan for disasters and information security incidents and thus ensures Response Planning processes are executed during and after an incident.

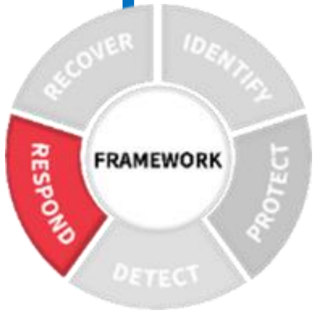
Organisation manages Communications during and after an event with stakeholders and law enforcement and thus send positive signal to customers and employees.

Organisation performs mitigation activities to prevent expansion of an event resolving the incident and thus keeps business operations up and running.

Organisation analyses effectiveness of response activities and thus update and improve the cybersecurity policy and plan with lessons learned from current and previous detection / response activities.

Co-funded by the
Erasmus+ Programme
of the European Union

Recommended Activity Steps



Activity1. Define roles and responsibilities!

It is recommended to outline who makes the decision to initiate recovery procedures and who will be the contact with appropriate law enforcement personnel.

Activity2. Specify what to do with information and information systems in case of an incident!

It is very important to act immediately when attack breaches and disconnect or lock affected computer(s) from the network, physically remove documents, utilize spares and backup and continue to capture operational data or switch to paper.

Activity 3.Report and notify that cyber-attack occurred!

It would be desirable to report the attack to the law enforcement, legal representation, cybersecurity professionals, legal professionals, service providers or insurance providers while informing customers and employees and others whose data may be at risk.

Activity 4. Update the cybersecurity policy and plan!

It would be good to update the cyber incident response and strategy with operational knowledge, experience and lessons learned after investigating and containing an attack.

Co-funded by the
Erasmus+ Programme
of the European Union

Sources

[1]https://www.nist.gov/cyberframework/online-learning/five-functions

[2]https://staysafeonline.org/cybersecure-business/respond/

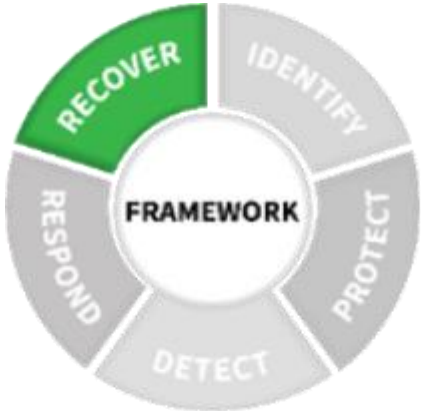
[3]https://staysafeonline.org/cybersecure-business/respond/

[4] NISTIR 7621 Revision 1, Small Business Information Security: The Fundamentals, National Institute of Standards and Technology 2016 (https://doi.org/10.6028/NIST.IR.7621r1)

ENGINE

Co-funded by the
Erasmus+ Programme
of the European Union

5. Recovery



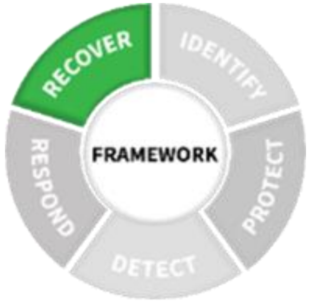
Objective

✓ Case Examples and Quick Wins

Recommended Activity Steps

Co-funded by the
Erasmus+ Programme
of the European Union

Objectiv
e

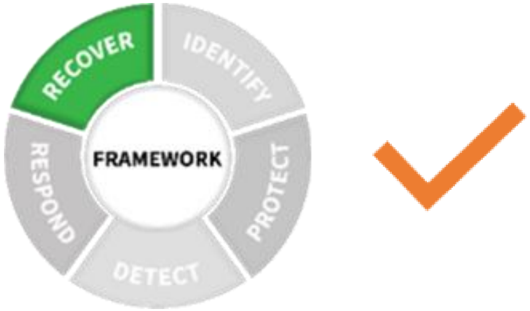


The final and fifth Function of the NIST Cybersecurity, supports an organisation to timely recovery to normal operations and reduce the impact from a cybersecurity incident. The Recover Function identifies appropriate activities to maintain plans for resilience and to restore any capabilities, services or equipment that were impaired due to a cybersecurity incident.

Finally, it fixing the causes, preventing the recurrence of a single incident and builds the cybersecurity posture across the whole organization, including increasing the focus on planning for future events.

Co-funded by the
Erasmus+ Programme
of the European Union

Case examples and Quick Wins



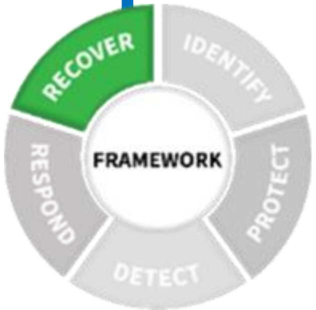
Organization ensures and implements Recovery Planning processes and procedures and thus quickly restore systems and/or assets affected by cybersecurity incidents.

Organization implements improvements to processes/procedures/technologies based on lessons learned and thus reviews and updates existing strategies.

Coordinating Communications during recovery activities and thus organization have repaired reputation.

Co-funded by the
Erasmus+ Programme
of the European Union

Recommended Activity Steps



Activity 1. Make backups of important business data/information!

It is recommended to conduct a full, encrypted backup (at least once a month) and an automatic incremental or differential backup (at least once a week) of the data on each computer and mobile device used in the organisation business.

Activity 2. Make improvements to processes / procedures / technologies!

It is very important to document lessons learned and make improvements to policies, procedures and security enhancements.

Activity 3. Keep employees informed of response and recovery activities!

It would be desirable to establish continuous training and education for the employees.

Activity 4. Repair reputation!

It would be good to communicate with external stakeholders stressing the improvements of cybersecurity policies and procedures and thus take steps and/or engage a PR firm to repair reputation.

Co-funded by the
Erasmus+ Programme
of the European Union

Sources

[1]https://www.nist.gov/cyberframework/online-learning/five-functions

[2]https://staysafeonline.org/cybersecure-business/recover/

[3]https://resources.infosecinstitute.com/topic/nist-csf-nist-csf-core-functions/

[4] NISTIR 7621 Revision 1, Small Business Information Security: The Fundamentals, National Institute of Standards and Technology 2016 (https://doi.org/10.6028/NIST.IR.7621r1)

[5]https://staysafeonline.org/cybersecure-business/