Interreg Co-funded by the European Union

Italy – Croatia

CRESPORT

CRESPORT
"Improving the Cyber REsilience and Security of Adriatic PORTs"

Cross-border training for a shared awareness and knowledge baseline on cyber security topic (D.1.2.1)

Interreg Co-funded by the European Union

Italy – Croatia

CRESPORT

Document Control Sheet

Project number:	ITHR0200152
Project acronym	CRESPORT
Project Title	Improving the Cyber Resilience and Security of Adriatic PORTs
Start /end of the project	01/03/2024 – 31/08/2026

Work package	WP1
Activity	1.2 Training on cyber resilience and security of ports as community of various operators
Deliverable name:	D. 1.2.1 - Cross-border training for a shared awareness and knowledge baseline on cyber security topic
Type of deliverable	Report
Language (s)	English
Dissemination Level	Public /website
Work Package Leader	PP6 NASPA - North Adriatic Sea port Authority (Ports of Venice and Chioggia)
External experts WP leader	IBM Italia spa
Document date	07/03/2025
Version number	Draft 03
Partners peer review #1 due date	
Partners peer review #2 due date	
Approval date deadline	
Submitted by	WP Coordinator PP6 NASPA
Final delivery date	

Index

Glossary

Name	Description
AI	Artificial Intelligence
BIA	Business Impact Analysis
CRESPORT	Cyber REsilience and Security of Adriatic PORTs
CSF 2.0	NIST Cybersecurity Security Framework 2.0
IDS	Intrusion Detection System
IoT	Internet of Things
IT	Information Technology
MFA	Multi-factor Authentication
NIST	National Institute of Standards and Technologies
OT	Operational Technology
SBQSG	NIST CSF 2.0 : Small Business Quick-Start Guide
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SOC	Security Operations Center
UBA	User Behavior Analytics

1. Executive Summary

Purpose and project's context

CRESPORT project aims to address the challenge of providing ports in the Adriatic area with a more secure and resilient IT infrastructure. Considering ports as critical and vulnerable infrastructures, CRESPORT intends to address this common problem through cooperation and joint actions, which are essential to strengthen territorial cohesion, by adopting a common strategy to ensure compliance with the main international cybersecurity standards (e.g. EU directives, national legislation, IMO recommendations).
The Adriatic ports play a strategic role in terms of logistics and commercial development. In recent years these ports have been experiencing significant growth in the maritime transport sector, both in logistics and goods handling. As known since the last decade, digitalization is growing in ports and in logistics in general and today is one of the key factors for the competitiveness of the supply chain.
Emerging technologies (e.g. IoT – Internet of Things, AI – Artificial Intelligence, ...) are generating a new digital revolution in port infrastructures
and in the logistic processes.
Given the economic and geographical relevance of the Adriatic Ports, which constitutes a joint economic and environmental resource, the big common challenge is how to empower the capacity of each port to early detect and counter cyber-attacks to make the ports of the Area more secure. In this context, strong multilateral cooperation, through the adoption of joint actions and strategy, represents the concrete response to the building of a strengthening of the port infrastructures, for sure a considerable opportunity of growth and territorial cohesion.
The Project, led by the Port Authority of Ravenna, includes also the Italian Port System Authorities of Ancona, Venice and Trieste, and on the Croatian side, the Port Authorities of Rijeka, Ploče and Dubrovnik.
The purpose of this activity is to provide training on cyber resilience and security of ports to the participating Partners and to port's communities stakeholders. This training aims to support the program's objective of enhancing awareness about the cybersecurity of Adriatic port systems. The training focused on cybersecurity risk assessment and management, addressing some of the most critical areas identified by the previous Security Assessment activity.

Overview

The previous CRESPORT Security Assessment activity, conducted in the second half of 2024, identified weaknesses in several areas relevant to the cybersecurity and resilience of the Port System Authorities (please refer to *D.1.1.1 Cross-border cyber resilience and security assessment* for more details). This training activity addressed the most relevant of those themes during two events: a training day held on January 27, 2025, in Venice, and a web follow-up session held on February 19, 2025.

2. Training Sessions on 27 January 2025

The first two sessions of training were delivered in Venice, on January 27, 2025.
The format of the event was hybrid, with attendance in person and in streaming. All the proceedings were made available in simultaneous translations in English, Italian and Croatian languages, so to overcome any language barrier and have meaningful impact on all level of practitioners.

The training was targeted for a broader audience, not only ICT Managers so to mainstream cyber security as a company/institution core value that must be conceived in all lines of work, from technical to more legal, administrative, financial and commercial departments.
On the first and second training session, 46 (forty-six) people attended in person, while 77 (seventy-seven) participated remotely for a total of 123 (one hundred and twenty-three) attendees.

The event was endorsed by the Venice Order of Engineers, which provide their members with training credits recognized at National level for the standards of the Engineering profession and certificates, and featured several notable speakers, including opinion leaders and representatives from the National Cybersecurity Agency (ACN), CLUSIT – the Italian Association for IT Security, ISACA, the global certification association for IT professionals, and the University of Padua. Technical partner supporting the Project consortium in coordination include IBM Italia Spa and IBM Cyber Academy.

This occasion was also an opportunity to address timely issues that are increasingly in the spotlight, including hackers cyberattacks on national and European institutions and businesses, the growing use of drones, advancements in digitalization, the rise of artificial intelligence, the shortage of STEM-skilled professionals, and the need for gender balance in strategic risk management sectors. In the coming years,

there will be a growing need for cross-disciplinary skills to manage the potential of exponentially more powerful computers, based on quantum computing, to develop solutions that harness the opportunities of the digital world while managing its risks.

Training sessions explored crucial topics for the future of port terminals and logistics in general, alongside a panel of internationally renowned experts, using both theoretical and practical scenario analyses.

The talks were delivered by senior 20 yrs+ professionals and academic experts representing leading opinion and policy decision-makers such as:

- ACN – Italian National Cybersecurity Agency
- CLUSIT – Italian Association for Cyber Security
- University of Padua
- ISACA – Venice chapter
- IBM Italia S.p.A.

Topics selection

The topics addressed several of the 2024 Security Assessment main findings and thus creating a *fil-rouge* between the gaps on cyber security posture of the Adriatic ports taking part to the CRESPORT project assessment and beyond that, to the various array of stakeholders that attended the training, mostly dealing with supply chain such as shipping agents, terminal operators, maritime authorities, SMEs, professionals (lawyers, engineers, Data Protection Officers, to name a few) and universities, covering following themes:

- Cybersecurity education
- The current security scenario
- The main cybersecurity standards
- Threat intelligence and the Dark Web
- The cybersecurity market
- Cybersecurity risk management
- AI & Cybersecurity
- Compliance and security, impacts and opportunities
- A strategy for transition to Quantum Safe Encryption
- The security of critical infrastructure in the port environment
- IIoT Security
- Security visibility
- Security governance and operational resilience.

Interreg Co-funded by the European Union
Italy – Croatia
CRESPORT

Agenda

Improving the Cyber REsilience and Security of Adriatic PORTs
High level training, Venice, Mo. 27/01/25 h. 9:30 – 18:00
Venezia Heritage Tower, Corso Gianni Sottana, 30100 Venice-Marghera
Moderator: Mr. Giuseppe Puleo, Security Consultants Unit Manager –Security & Privacy Services IBM Italia S.p.A.
Simultaneous translation Italian/English/Croatian available

Timing	Topics	Speakers
09.30-10.00	Guests' registration and welcoming coffee	
10.00-10.10	Institutional greetings	Mr. Fulvio Lino DI BLASIO, President, North Adriatic Sea Port Authority
10.10-10:20	The added value of CRESPORT project in the rationale of digitalization processes of NAS Port Authority	Ms. Antonella SCARDINO, Secretary General, North Adriatic Sea Port Authority
10.20-10.45	Cybersecurity education, training and awareness-raising	Mr. Paolo Azteni, Italian National Agency for Cyber Security (ACN), Scientific Coordinator of Training and Awareness Divisions
Session 1: SETTING THE SCENE OF CYBER SECURITY IN EUROPE TODAY		
10.45-11.05	The (in)security scenario - The viewpoint of the CLUSIT observatory	Mr. Luca BECHELLI, Member of Scientific Committee of CLUSIT Italian Association for Cyber Security
11.05-11:25	The cybersecurity standards of reference	Mr. Giuseppe PULEO, Security Consultants Unit Manager, IBM Italia S.p.A., Mr. Marco SILVESTRI, Managing Security Consultant, IBM Italia S.p.A.
11:25-11:45	Threat Intelligence and the Dark Web	Mr. Pompeo D'URSO, Associate Partner & Chief of Ops IBM Cyber Academy, Global Government Industries, IBM Corporation
11.45-12.05	The cybersecurity market	Mr. Giuseppe PULEO, Security Consultants Unit Manager, IBM Italia S.p.A., Mr. Marco SILVESTRI, Managing Security Consultant, IBM Italia S.p.A.
12.05-12.25	The cybersecurity risk management approach	Mr. Alberto Elia MARTIN, Vice President of ISACA (Venice Chapter)
12.25-12.50	Q&A	
13.00-14.00	Light lunch	

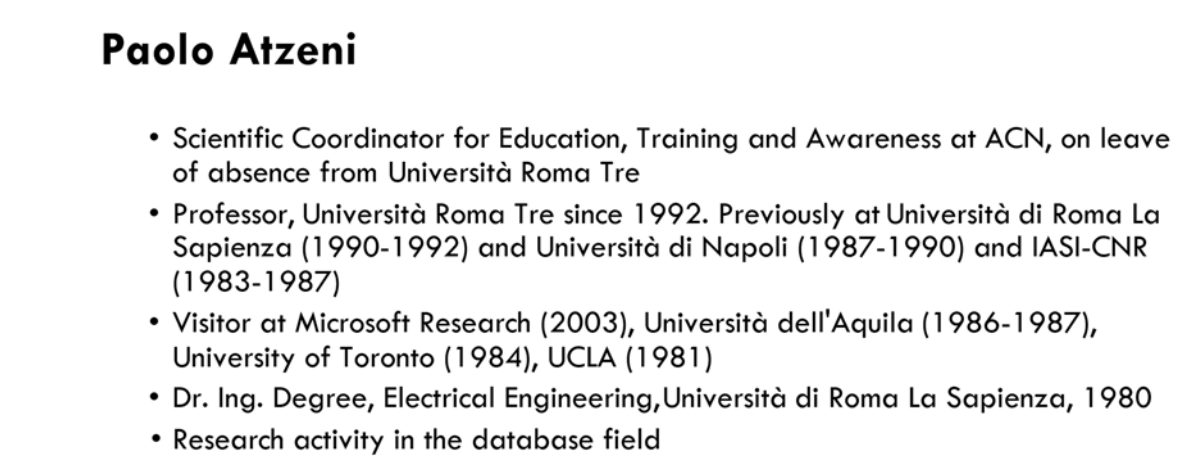
SESSION 2: CASE STUDIES AND STAKEHOLDERS ENGAGEMENT		
14.15-14:40	AI & Cybersecurity	Mr. Mauro CONTI, Full Professor University of Padua, Dep. of Mathematics and HIT Center, IEEE fellow, Associated of TU Delft University (NL) and Washington University (USA)
14:40-15:05	Compliance and security, impacts and opportunities	Mr. Luca BECHELLI, Member of Scientific Committee of CLUSIT Italian Association for Cyber Security
15:05-15:30	Quantum Safe – A strategy for transition	Mr. Francesco Perna, Senior Associate Partner, IBM Italia S.p.A.
15:30-15:55	The security of critical infrastructure in the port environment	Mr. Francesco Perna, Senior Associate Partner, IBM Italia S.p.A.
15:55-16:20	IIoT Security - Threats, risks and controls	Mr. Marco SILVESTRI, Managing Security Consultant, IBM Italia S.p.A.
16:20-16:45	Security visibility	Mr. Pompeo D'URSO, Associate Partner & Chief of Ops IBM Cyber Academy, Global Government Industries, IBM Corporation
16:45-17:10	Security governance and operational resilience	Mr. Giuseppe PULEO, Security Consultants Unit Manager, IBM Italia S.p.A.
17:10-17:45	Q&A, Conclusions	
18.00-19.00	Networking cocktail	

Presentations Experts and take-home messages

Cybersecurity education, training and awareness-raising

Prof. Paolo ATZENI, Scientific Coordinator for Education, Training and Awareness at ACN

- The shortage of cyber specialists is parallel to the one in the IT sector and even more than the entire scientific and technological world;
- All initiatives must really be inclusive, with reference to under-represented groups/sets, for example gender;
- Specific actions are needed to reduce the gender gap and unfair treatment in every context (school, university, working sector);
- Various categories of individuals need complementary skills (beside the basic ones), such officials and executives at various levels, who have responsibilities regarding the security of activities within their own structures;
- specialists in application domains (healthcare, research, finance, law, infrastructure);



ACN: Agenzia per la Cybersicurezza Nazionale

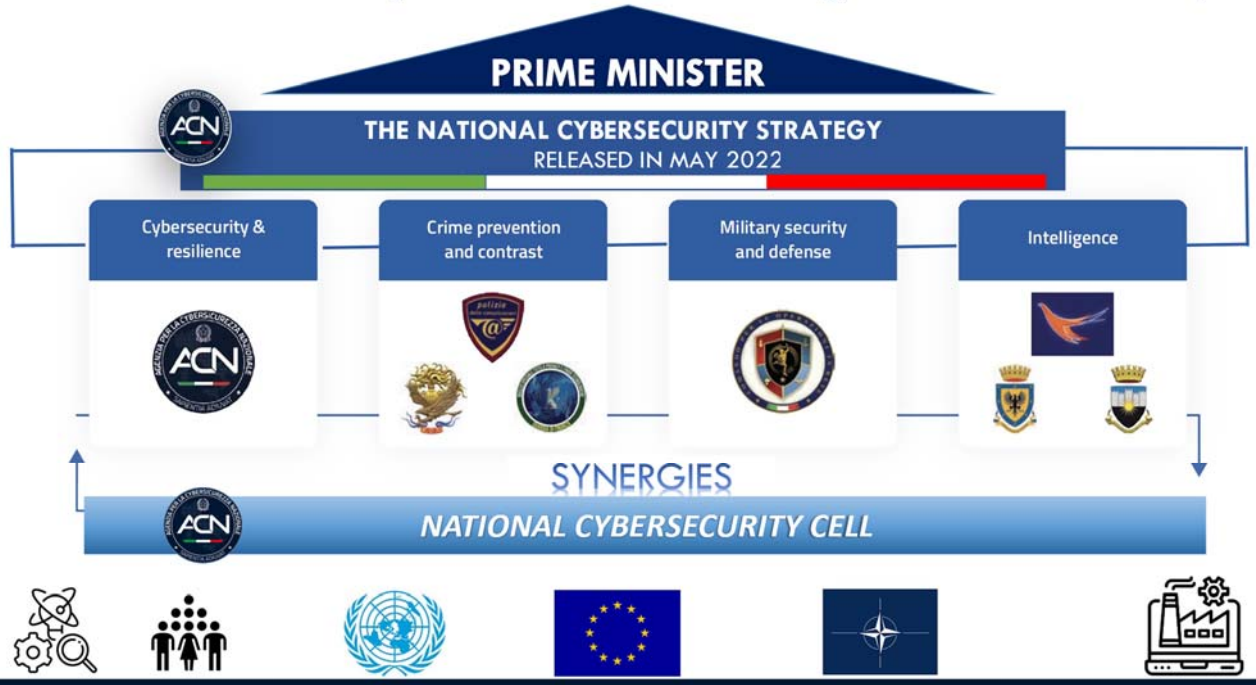
(Established, September 2021)

The Agency:

- is the National Cybersecurity Authority and [...] ensures [...], the coordination between the public entities involved in the field of cybersecurity at a national level and promotes the implementation of joint actions aimed at ensuring cyber security and resilience [...] as well as for the achievement of national and European autonomy [...]
- prepares the national cybersecurity strategy
- carries out cybersecurity awareness activities in order to contribute to the development of a national culture on the matter;
- promotes education and training [...] in particular by supporting the activation of university programs on the subject

3

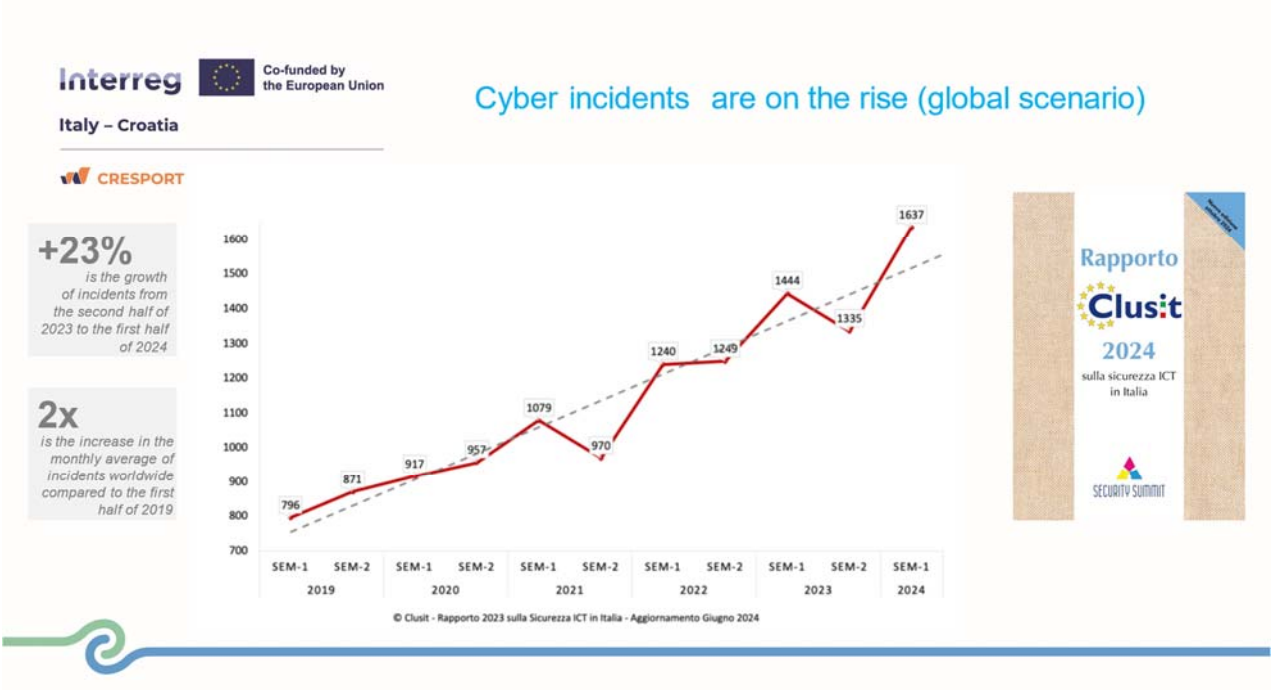
The Italian Institutional Cyber Architecture following the Law Decree n. 82/2021



6

The (in)security scenario - The viewpoint of the CLUSIT observatory
Mr. Luca BECHELLI, member of the Scientific Committee of CLUSIT

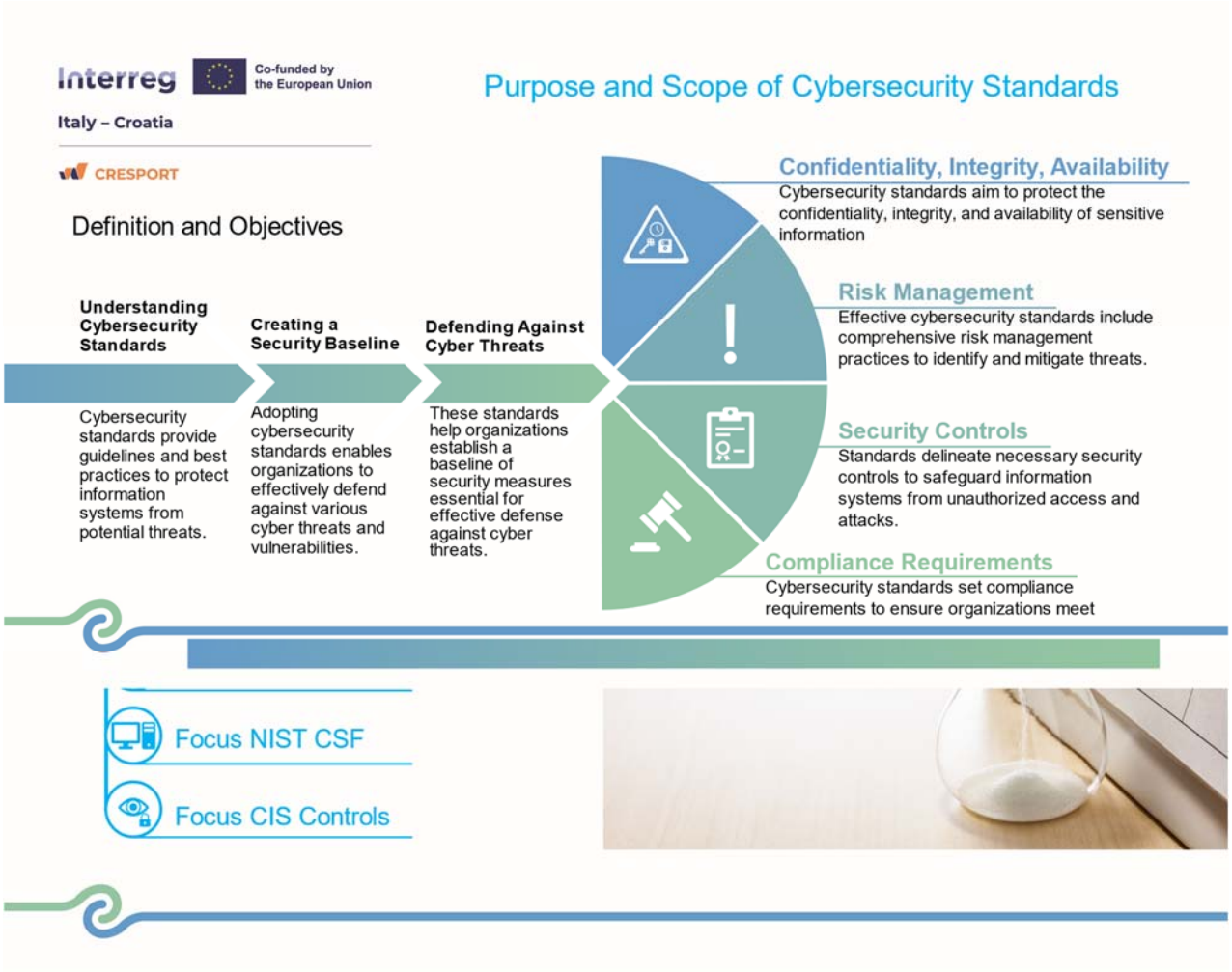
- The data that Clusit collects refer only to serious incidents and are limited to public sources with the consequence that the picture is still partial compared the phenomenon in its entirety but, in any case, that the increase in serious accidents is impressive between 2021 and 2024 is indirectly confirmed by the amount of cases we constantly hear about in the media;
- Assuming that the strategy deployed to date is useful (certainly to avoid a greater acceleration of the phenomenon), we still do not see on the horizon a retreat of the phenomenon or at least an ability of the country system to defend itself better than others;
- Many countries are lagging behind in terms of digital skills, as amply demonstrated by the European Commission's DESI index, which in its Report 2023;
- In addition to the increasing damage caused by cybercrime and 'normal' intelligence activities, since 2022 we have entered a new phase of 'widespread cyber warfare', which is also confirmed to grow in 2024;



The Cybersecurity standards of reference

Mr. Giuseppe PULEO, Security consultants Unit Manager, IBM Italia spa
Mr. Marco SILVESTRI, Managing Security consultant, IBM Italia Spa

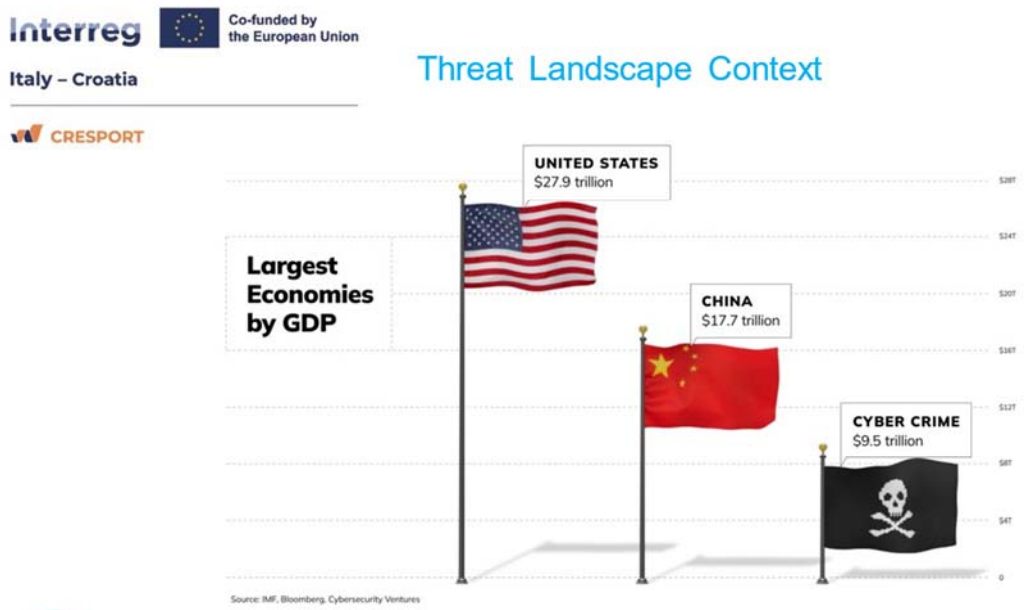
- Cybersecurity standards are essential for protecting sensitive information and defending against cyber threats in an organized and efficient way.
- Organizations can benefit from adopting standards like ISO 27001, NIST CSF, and CIS Controls, which provide guidelines and best practices for managing cyber risk
- Implementing these standards can help organizations establish a security baseline, ensure compliance with regulations, and improve their cybersecurity posture.
- Continuous improvement and global collaboration are paramount in the face of evolving cybersecurity threats



Threat Intelligence and the Dark Web

Mr. Pompeo D'URSO, Associate Partner, IBM Italia Spa

- The threat landscape context is severe: European countries account for 32% of incidents to which the IBM X-Force team responded. Europe experienced the most ransomware attacks globally with 26%
- Know your dark web exposure as it poses a significant threat
- Employ dark web capabilities that:
    - Find at-risk credentials and session keys
    - Check your executives' digital identities
    - Scan social networks, channels related to your sector, blogs and advertising for unauthorized brand use
    - Identify leaked priority, confidential and sensitive data
- The future of threat landscape assessment involves AI-enhanced threat landscape identification, continuous attack surface analysis, and AI-driven threat intelligence



Interreg Co-funded by the European Union

Italy – Croatia

CRESPORT

Interreg Co-funded by the European Union

Italy – Croatia

CRESPORT

Identiy Threat Actors

Cybercriminals

These individuals or groups commit cybercrimes mostly for financial gain. Common crimes include ransomware attacks and phishing scams that trick people into making money transfers or divulging credit card information, login credentials, intellectual property or other private or sensitive information.

Cyberterrorists

Cyberterrorists start politically or ideologically motivated cyberattacks that threaten or result in violence. Some cyberterrorists are nation-state actors; others are actors on their own or on behalf of a nongovernment group.

Nation-state actors

Nation states and governments frequently fund threat actors with the goal of stealing sensitive data, gathering confidential information or disrupting another government's critical infrastructure. These activities often include espionage or cyberwarfare and tend to be highly funded, making the threats complex and challenging to detect.

Hacktivists

They use hacking techniques to promote political or social agendas, such as spreading free speech or uncovering human rights violations. Hacktivists believe that they are affecting positive social change and feel justified in targeting individuals, organizations or government agencies to expose secrets or other sensitive information.

Thrill seekers

They attack computer and information systems primarily for fun. Some want to see how much sensitive information or data they can steal; others want to use hacking to better understand how networks and computer systems work. They don't always seek to cause harm but can still cause unintended damage and open the door to future cyberattacks.

Insider threats

Unlike most other actor types, insider threat actors do not always have malicious intent. Some hurt their companies through human error, such as by unwittingly installing malware or losing a company-issued device that a cybercriminal finds and uses to access the network. But malicious insiders do exist..

Interreg Co-funded by the European Union

Italy – Croatia

CRESPORT

Dark Web: myths and realities

The cybersecurity market

Mr. Giuseppe PULEO, Security consultants Unit Manager, IBM Italia spa
Mr. Marco SILVESTRI, Managing Security consultant, IBM Italia Spa

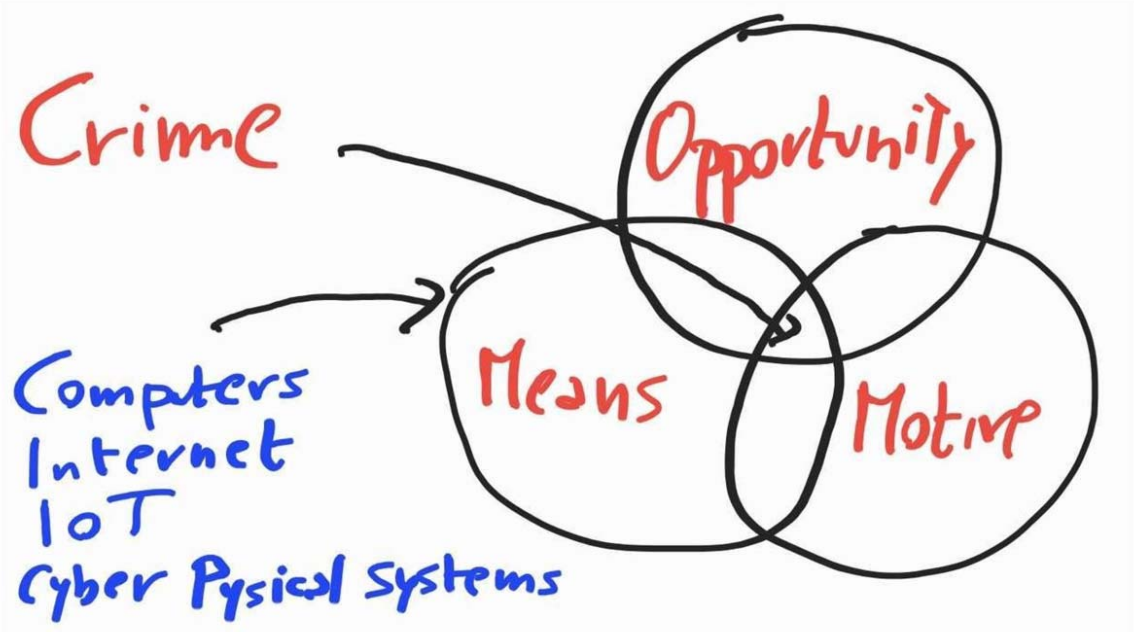
- Understanding the motivations and profiles of potential attackers is essential to defend against cyber threats.
- It is crucial to identify critical assets and processes, as you cannot adequately protect what you do not know
- 100% security is unachievable due to the capabilities of attackers and the complexity of systems. Define an acceptable level of risk and focus on mitigating it up to that level
- Cybercrime may involve many types of costs for an organization, including data compromise, financial losses, loss of productivity, legal compliance, and reputational damage. The global cost of cybercrime is projected to reach $10.5 trillion by 2025.

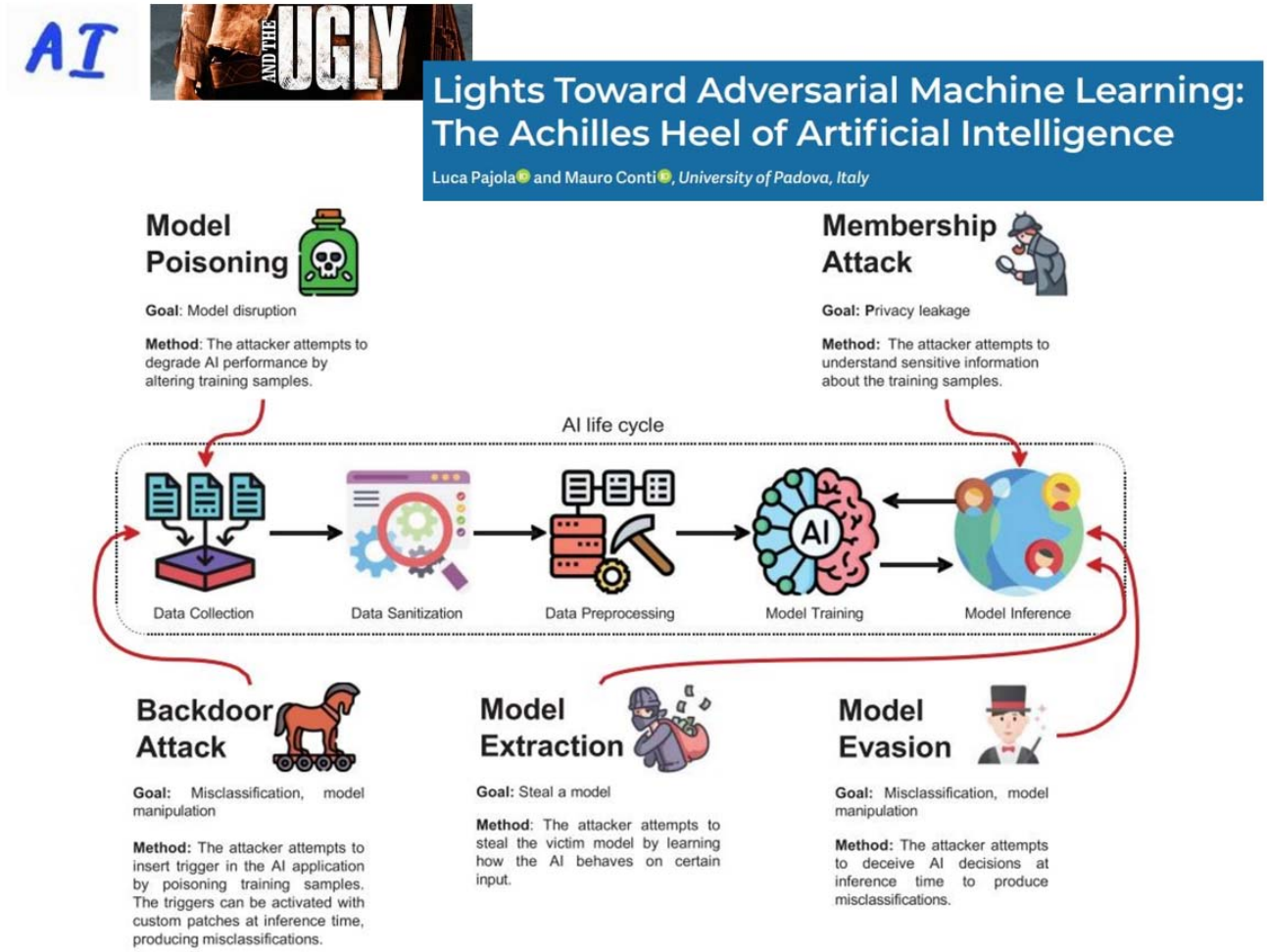
The cybersecurity risk management approach
Mr. Alberto Elia MARTIN, Vice President ISACA Venice Chapter

- Risk management exists to help us to create plans in a deliberate, responsible and ethical manner
- Risk management is about analyzing our options and their future consequences, and presenting that information in an understandable, usable form to improve decision making
- The purpose of risk management is not to chase the unattainable goal of perfectly secure systems and a risk-free business. Rather, it is to make sure that you have thought about what can go wrong, and that this thinking has influenced your organization's decisions
- Don't be fatalistic; you can still protect yourself from many cyberattacks, but if something does go wrong, it isn't always the case that someone is to blame, or that your risk manager missed something

AI & Cybersecurity
Prof. Mauro CONTI, University of Padua

- The protection of information did not originate with the digital age, but rather with humankind. From Julius Caesar's ancient cipher to the decryption of the Enigma during the Second World War by the renowned mathematician Alan Turing, the importance of information security has always been vital. The latter example provided a significant advantage to the Allies, illustrating the enduring importance of information security
- Recently, incidents such as the attack on the Ukrainian power grid and the Colonial Pipeline ransomware case in the United States serve as examples of how critical infrastructure can become dangerously vulnerable targets
- NATO has recognized cyberspace as a domain of war, and Italy has taken a stand to use it for both defensive and offensive purposes

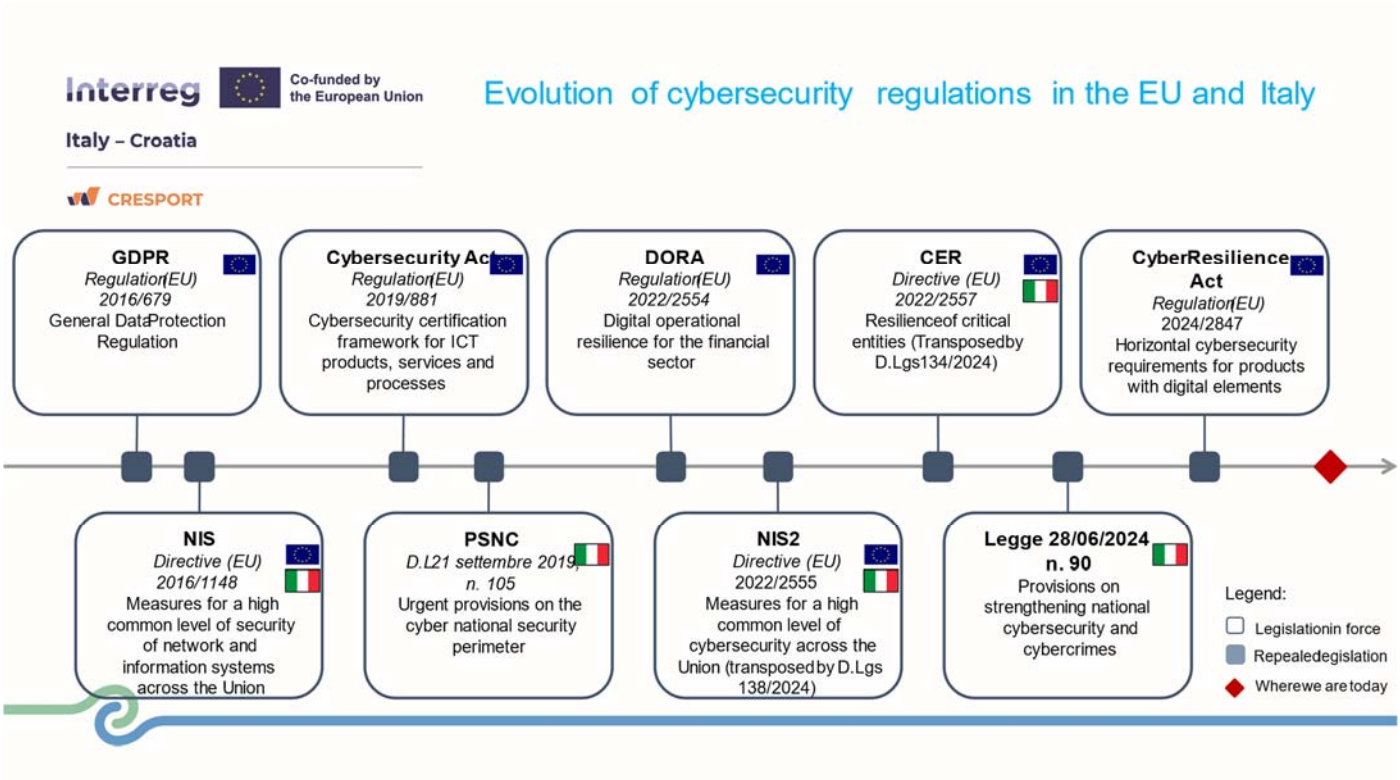



AI
AND THE UGLY
Lights Toward Adversarial Machine Learning: The Achilles Heel of Artificial Intelligence
Luca Pajola and Mauro Conti, University of Padova, Italy
Model Poisoning
Goal: Model disruption
Method: The attacker attempts to degrade AI performance by altering training samples.
Membership Attack
Goal: Privacy leakage
Method: The attacker attempts to understand sensitive information about the training samples.
AI life cycle
Data Collection
Data Sanitization
Data Preprocessing
Model Training
Model Inference
AI
Backdoor Attack
Goal: Misclassification, model manipulation
Method: The attacker attempts to insert trigger in the AI application by poisoning training samples. The triggers can be activated with custom patches at inference time, producing misclassifications.
Model Extraction
Goal: Steal a model
Method: The attacker attempts to steal the victim model by learning how the AI behaves on certain input.
Model Evasion
Goal: Misclassification, model manipulation
Method: The attacker attempts to deceive AI decisions at inference time to produce misclassifications.

Compliance and security, impacts and opportunities

Mr. Luca BECHELLi, Member of Scientific Committee of CLUSIT

- There have been several recent developments in EU cybersecurity regulations, including the NIS2 Directive, CER Directive, and Cyber Resilience Act, which aim to improve the cybersecurity of critical infrastructure and entities
- Focus is currently on the NIS 2 Directive, which imposes various requirements on entities, including risk assessments, incident reporting, and cybersecurity measures, and provides for penalties for non-compliance
- The NIS 2 Directive covers a range of sectors, including energy, transport, banking, healthcare, and digital infrastructure
- NIS 2 penalties for non-compliance address both the organization and the top management



Interreg Co-funded by the European Union
Italy – Croatia
CRESPORT

NIS2 - Entities in scope

1. Sectors of high criticality (Annex I):

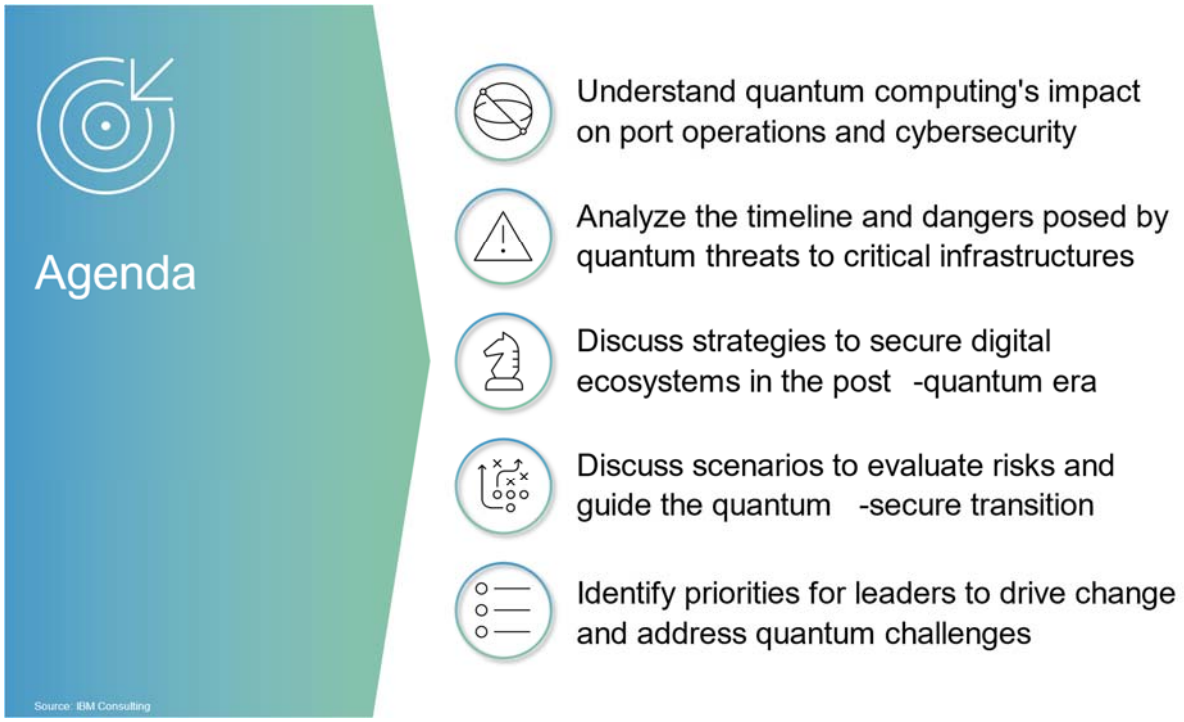
- Energy
- Transport
- *Banking (Dora Regulation applies to this sector)*
- Financial market infrastructures
- Health
- Drinking water
- Waste water
- Digital infrastructure
- ICT service management (business-to-business)
- Public administration
- Space

2. Other critical sectors (Annex II)

- Postal and courier services
- Waste management
- Manufacture, production and distribution of chemicals
- Production, processing and distribution of food
- Digital providers
- Research
- Manufacturing
  - Manufacture of medical devices and in vitro diagnostic medical devices
  - Manufacture of computer, electronic and optical products
  - Manufacture of electrical equipment
  - Manufacture of machinery and equipment n.e.c.
  - Manufacture of motor vehicles, trailers and semi-trailers
  - Manufacture of other transport equipment

Quantum Safe – A strategy for transition
Mr. Francesco PERNA, Associate Partner, IBM Italia Spa

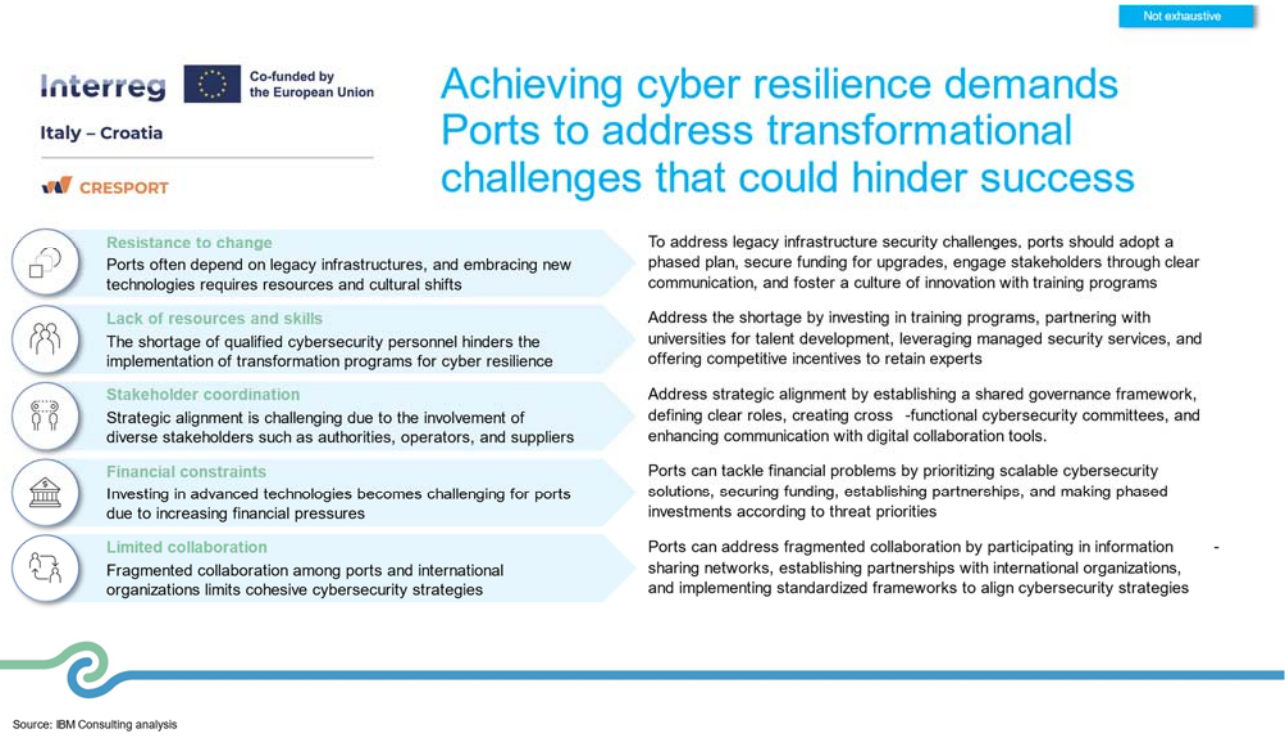
- Quantum computers have applications that can help transform harbor operations. However, advances in quantum computing development will also raise cybersecurity risks
- Quantum threats include the potential for falsification of critical transit data, tampering of critical communications and "harvest now, decrypt later" attacks
- Although quantum computers are still far from mainstream, they pose a threat because of their rapid progress. Port authorities need to start now a quantum-secure transition to deal with transformation complexities



The security of critical infrastructure in the port environment

Mr. Francesco PERNA, Associate Partner , IBM Italia Spa

- Ports are embracing digital technologies to sustain their role in EU economy growth. However, this is increasingly attracting the unwanted attention of cybercriminals
- Cyberattacks can have significant impacts on ports operations, logistics, and the economy
- Ports face existential consequences from cyberattacks due to overconfidence and unpreparedness
- A structured approach is required to secure critical infrastructure at ports and move towards cyber resilience



IoT Security - Threats, risks and controls
Mr. Marco SILVESTRI, Managing Security Consultant, IBM Italia S.p.A

- Industrial Internet of Things (IIoT) technologies enable real-time field data exchange, allowing businesses to make informed decisions quickly and improve operations and services
- However, IIoT systems are vulnerable to various cyber threats, including denial-of-service attacks, malware, and ransomware. These threats can have significant consequences for operations, such as downtime, loss of productivity, and damage to equipment
- According to recent data, 31% of all cybersecurity incidents at transportation companies are IIoT-related
- To mitigate these risks, it is essential to implement robust security measures, including risk assessment, security policies, employee training, and collaboration with vendors and industry groups


Interreg
Co-funded by the European Union
Italy – Croatia
CRESPORT
Agenda
Introduction to IIOT
Cybersecurity Challenges
Strategies for Mitigating IIoT Risks
Anatomy of an IIoT Attack
Future Trends in IIoT Security

Security governance and operational resilience
Mr. Giuseppe PULEO, Security consultants Unit Manager, IBM Italia S.p.A.

- Data breaches can have significant financial impact on organizations. The average total cost of a data breach is USD 4.88M
- Crisi management helps organizations prepare for, respond to and recover from crises. Effective crisis management and business continuity planning are crucial to minimize disruptions and maintain stakeholder trust
- Operational resilience is of paramount importance. It encompasses risk management, incident response, business continuity planning, disaster recovery, and supply chain resiliency.
- Guidance is provided on performing Business Impact Analysis (BIA) and developing a Business Continuity Plan (BCP). This includes conducting regular testing and overcoming common challenges in BCP implementation, such as executive buy-in, resource constraints, and resistance to change.

Interreg Co-funded by the European Union

Italy – Croatia

CRESPORT

Interreg Co-funded by the European Union

Italy – Croatia

CRESPORT

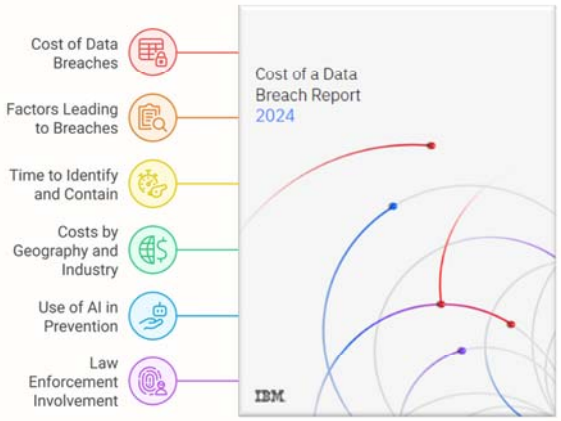
Cost of Data Breach Reports 2024

The annual **IBM Cost of a Data Breach Report**, provides IT, risk management and security leaders with insights collected from 604 organizations impacted by data breaches between March 2023 and February 2024.

This research is provided to IBM clients, researchers in the security industry, policymakers, the media, and the broader community of security professionals and business leaders, to keep you informed of the true cost of a data breach.

The report also explains best practices based on research findings to help you mitigate costs and make the best decisions to prevent a breach.

The report highlights key trends and year-over-year changes.



Interreg Co-funded by the European Union

Italy – Croatia

CRESPORT

Agenda

- Cost of data Breach
- Operational Resilience
- Crisis Management & Business Continuity

3. Follow-up Training Session on 19 February 2025

This training was held in the form of a web session on February 19, 2025, as a follow-up to the January 27 training day in Venice. The training session focused on some of the topics that had attracted the most interest during that occasion.

Topics selection

The topics for the training session covered the following themes:

- Risk management in the port environment
- IEC 62443 and OT Cybersecurity Risk Assessment
- Managing supplies cybersecurity
- Overview of the NIS2 directive

Agenda

Improving the Cyber REsilience and Security of Adriatic PORTs
High level training follow up session 3
19/2/2025, 10:30-12:30

Moderator: Mr. Giuseppe Puleo, Security Consultants Unit Manager –Security & Privacy Services IBM Italia S.p.A.

Session 3: CRESPORT TRAINING FOLLOW UP AND FOCUS ON NIS 2 DIRECTIVE

Timing	Topics	Speakers
H: 10:30 – 12:30	What are the most appropriate guidelines for conducting a cyber risk assessment of a port facility or an entire port?	Mr. Francesco PERNA, Senior Associate Partner, IBM Italia S.p.A.
	OT Cybersecurity Risk Assessments According to ISA/IEC 62443	Mr. Marco SILVESTRI, Managing Security Consultant, IBM Italia S.p.A.
	Managing Supplies Cybersecurity	Mr. Simone Lorenzi, Managing Security Consultant, IBM Italia S.p.A.
	An Overview on the NIS 2 Directive	Mr. Marco SILVESTRI, Managing Security Consultant, IBM Italia S.p.A.
	Q&A	

Presentation Experts and take-home messages

Agile risk management in the port environment
Mr. Francesco PERNA, Associate Partner, IBM Italia Spa

- Ports face a diverse range of threats, including sophisticated cyber-attacks, extreme weather events driven by climate change, operational failures, terrorist threats, and disruptions in the global supply chain. All of these can significantly impact security and economic stability
- Risk management is a crucial approach to handling risks in complex port environments. A well-structured risk management framework minimizes the impact of adverse events, enhances resilience, and ensures continuity of operations
- Key regulatory frameworks such as ISPS, ISM, and EU NIS 2 should serve as a foundation for implementing port risk management processes. This includes a comprehensive understanding of physical risks, cyber risks, operational risks, and supply chain risks

Interreg Co-funded by the European Union
Italy – Croatia
CRESPORT

Risk Management is a structured and strategic approach to handling risk in complex environments such as ports

Ports are vital infrastructures that serve as key hubs for global trade and national security, ensuring the seamless flow of goods while safeguarding economic stability and strategic interests

Ports face a diverse range of threats, including sophisticated cyber attacks, extreme weather events driven by climate change, operational failures, terrorist threats, and disruptions in the global supply chain, all of which can significantly impact security and economic stability

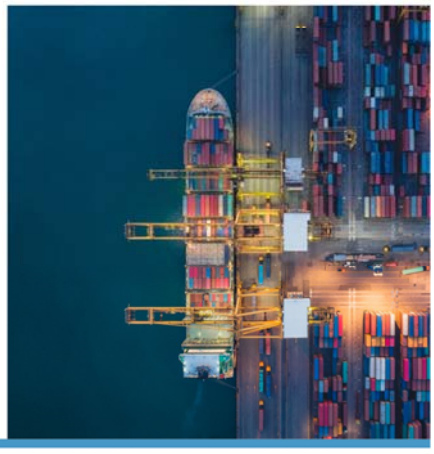
A well-structured risk management framework minimizes the impact of adverse events, enhances resilience, and ensures the seamless continuity of operations, safeguarding both efficiency and security in critical environments

Source: IBM Consulting analysis

Interreg Co-funded by the European Union
Italy – Croatia
CRESPORT

A structured and coordinated approach to risk management in ports is required to face emerging challenges

- Transforms the way ports strategically, operationally, and holistically approach risk, ensuring resilience and continuity
- Establishes a central body for port risk management, enhancing collaboration across operations and security
- Fosters collaboration across port areas, integrating logistics, security, and cybersecurity
- Offers a platform to improve port risk management, optimizing resources and threat response
- Enhances port risk management by optimizing resources and response



Source: IBM Consulting analysis

OT Cybersecurity Risk Assessment according to ISA/IEC 62443
Mr. Marco SILVESTRI, Managing Security Consultant, IBM Italia S.p.A.

- The ISA/IEC 62443 is a family of international standards for cybersecurity in industrial automation and control systems (IACS)
- A methodology is presented for conducting an OT cybersecurity assessment. This includes phases such as asset identification, technical analysis, site organization, and technical reporting
- An IEC 62443 OT cybersecurity assessment aims to evaluate the OT cybersecurity posture of an operational site. It also provides a strategy for improving security according to the IEC 62443-3-3 standard
- An example is provided of an on-site agenda and activities for conducting such an assessment

Interreg Co-funded by the European Union
Italy – Croatia
CRESPORT

IEC 62443-1-1: Terminology, concepts and models

IEC 62443-2-1: Establishing a security program for IACS (Industrial Automation and Controls Systems)

IEC: 62443-2-4: Security program requirements for IACS service providers

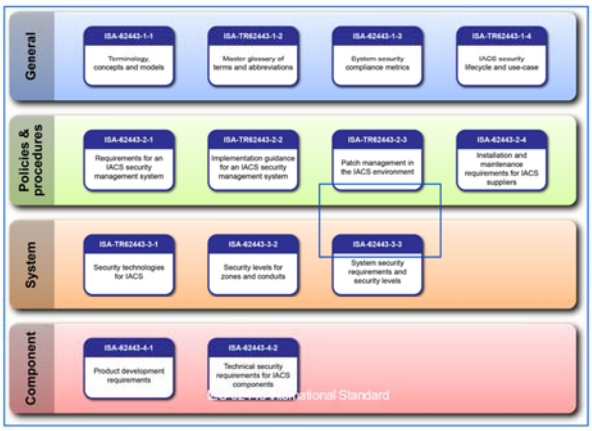
IEC 62443-3-1: Security technologies for IACS

IEC 62443-3-3: System security requirements and Security Levels

IEC 62443-4-1: Security requirements for product development lifecycle

IEC 62443-4-2: Technical security requirements for system components

ISA/IEC 62443 Family Overview

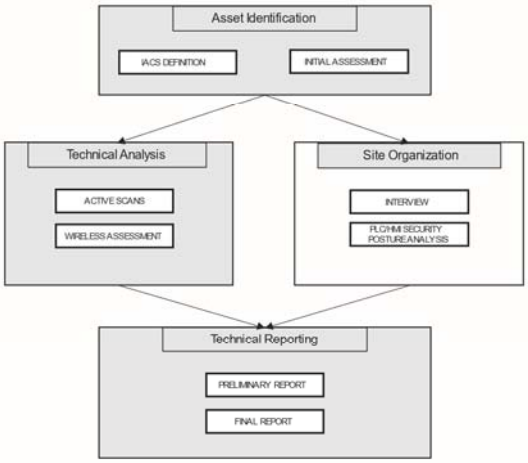


Interreg Co-funded by the European Union
Italy – Croatia
CRESPORT

An OT Cybersecurity Assessment:

- Evaluates the OT cybersecurity posture of the site and gain a quick picture of the status using a risk concept
- Allows the management to better understand the risks enabled by the site cybersecurity weaknesses
- Is the starting point for the definition of a mitigation strategy based on the reported findings and on the suggested roadmap

OT Cybersecurity Assessment



Managing supplies cybersecurity
Mr. Simone LORENZI, Managing Security Consultant, IBM Italia S.p.A.

- Supply chains require effective cyber risk management, particularly in the maritime industry. Organizations must implement robust security controls and measures to protect sensitive information from cyber threats
- Significant risks are associated with third-party suppliers, including data breaches and cyber-attacks. It is crucial to comply with regulations such as NIS2, GDPR, and ISO 27036
- A pragmatic approach to supply chain security includes implementing security controls and requirements during onboarding, monitoring suppliers for material changes, and conducting regular risk assessments

Interreg Co-funded by the European Union

Italy – Croatia

CRESPORT

Interreg Co-funded by the European Union

Italy – Croatia

CRESPORT

The most of data breaches and cyber attacks are originating in the supply chain – with a high cost

60% of incidents involve third -party cyber incidents [1]

62% of supply chain attacks sought to exploit the trust of customers [2]

$4.46M is the average cost of a supply chain data breach [3]

Source:
1 The State of ThirdParty Risk Management, 2023, Forrester
2 https://www.enisa.europa.eu/news/enisa-news/understanding-the-increase-in-supply-chain-security-attacks
3 2022 Cost of a Data Breach, IBM

Interreg Co-funded by the European Union

Italy – Croatia

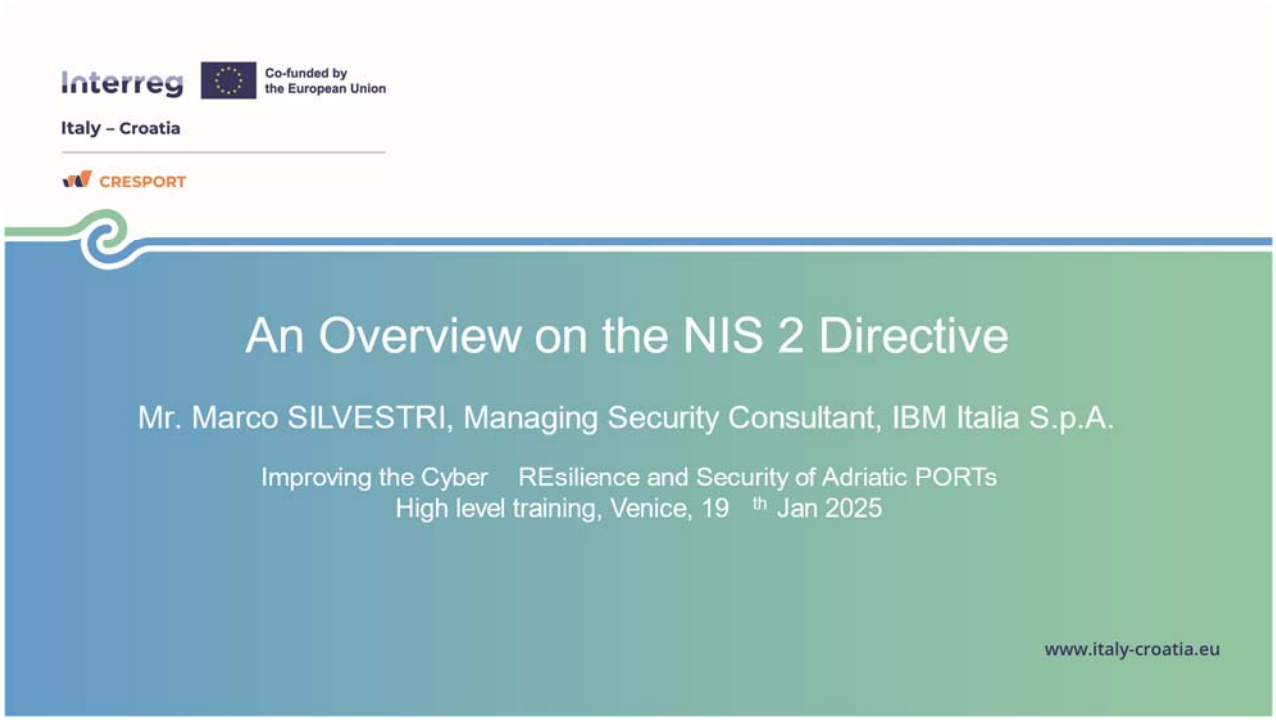
CRESPORT

Agenda

- Reference context
- Main Regulations
- ISO/IEC 27036:Information security for supplier relationships
- Pragmatic Approach to Supply Chain Security

An overview of the NIS 2 Directive
Mr. Marco SILVESTRI, Managing Security Consultant, IBM Italia S.p.A.

- The NIS 2 Directive aims to improve the cybersecurity and resilience of EU critical infrastructure by establishing a common level of cybersecurity. It expands the scope of application of the previous NIS Directive to include medium and large enterprises, as well as public administration organizations
- The NIS 2 Directive introduces new resiliency-related cybersecurity obligations, such as risk analysis, supply chain security, and incident management.
- The directive also establishes a supervisory authority and sanctions regime, with penalties of up to €10,000,000 or 2% of annual global turnover for non-compliance. Penalties will be applied also to the top management



Interreg Co-funded by the European Union

Italy – Croatia

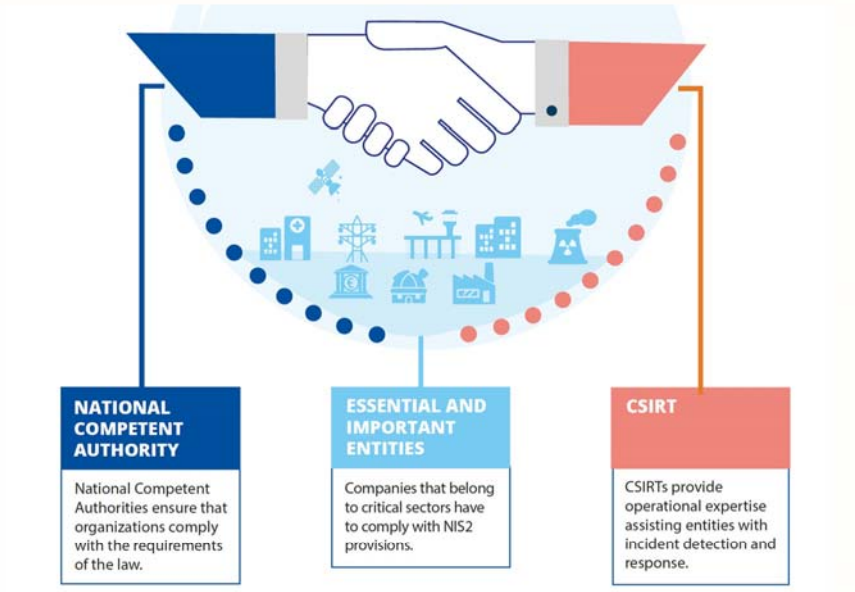
CRESPORT

Interreg Co-funded by the European Union

Italy – Croatia

CRESPORT

NIS 2 Actors



https://www.enisa.europa.eu/topics/awarenessand-cyber-hygiene/network-and-information-systems-directive-2-nis2

Interreg Co-funded by the European Union

Italy – Croatia

CRESPORT

NIS 2 in a Nutshell

NIS2 Network & Information Systems Directive

Replace the NIS Directive

Keep EU citizens protected

Establish a common level of cybersecurity within EU critical infrastructure

Each country transposes the NIS 2 directive in national laws

The board is ultimately responsible

4. Attachments

For the full downloadable package of the presentations delivered during the Training Sessions, please visit the CRESPORT project's official website: https://www.italy-croatia.eu/web/cresport/library