Profili economici e finanziari connessi alla Cybersecurity

Prof. ***Giovanni Satta***
Università degli Studi di Genova
DIEC & CIELI
giovanni.satta@economia.unige.it

Authors
Prof. ***Giovanni Satta***
Dott.ssa ***Bianca Vottero***
Dott. ***Francesco Vitellaro***

Genova, 24/01/2022

UNIVERSITÀ DEGLI STUDI DI GENOVA

LOGISTIC DIGITAL COMMUNITY

Agenda

1. **Cybersecurity & logistica marittimo-portuale**
2. **Investimenti per la cybersecurity**
3. **Finanziamenti per la cybersecurity**

Aspetti introduttivi
Cos'è la cybersecurity

- ✓ Linee guida, approcci di gestione del rischio, azioni, formazione, best practices e tecnologie per proteggere l'organizzazione e le risorse degli utenti (ITU, 2009).
- ✓ Insieme di metodi e tolls per proteggere i sistemi, le reti e i programmi dagli attacchi digitali finalizzati all'accesso, alla trasformazione o alla distruzione di informazioni sensibili, nonché all'estorsione di denaro agli utenti o all'interruzione dei normali processi aziendali.

Elementi costitutivi della cybersecurity

- ❖ Tecnologia: strumenti informatici di sicurezza necessari per proteggere dagli attacchi informatici i dispositivi endpoint (computer, dispositivi intelligenti e router), le reti e il cloud. La tecnologia include: firewall, filtri DNS, protezione dai malware, software antivirus, soluzioni di sicurezza e-mail, ecc..
- ❖ Persone: comprensione/rispetto dei principi di sicurezza dei dati di base (es. password complesse, diffidare degli allegati nelle e-mail, eseguire il backup dei dati, ecc.
- ❖ Processi: framework per prevenire e gestire gli attacchi informatici tentati e quelli andati a buon fine, capace di identificare gli attacchi, proteggere i sistemi, rilevare e rispondere alle minacce e recuperare dagli attacchi riusciti.

Cybersecurity & logistica marittimo-portuale
Elementi di rischio e di criticità

- Ruolo fondamentale della *cyber security* nella logistica marittimo portuale a causa del volumi di dati/informazioni gestiti.
- Alto rischio di compromissione di sistemi informatici e applicativi (sistemi di prenotazione/pagamento, gestione e inoltro documenti, sistemi di gestione/ planning delle operations, *Warehouse Management System, Transportation Management System)* con ricadute negative sulle performance operative ed economico-finanziarie.
- Elevata esposizione a rischi di perdita di dati sensibili: conseguenze commerciali e legali in conformità con la normativa di riferimento.
- Elevato impatto sul livello di trust e di loyalty di clienti e fornitori: il mancato rispetto della consegna JIT può portare alla perdita del cliente e alla riduzione del fatturato
- Problemi di *safety and security* dovuti a potenziali furti, sabotaggi e manomissioni di dati che rendono difficoltoso la gestione e il monitoraggio di sistemi di logistica e trasporto.
- Necessità di monitoraggio 24h/24h e 7/7.

Driver futuri che accrescono il livello di rischio

…crescita di…

- flussi di merci, mezzi, UTI e persone
- bisogni di logistica soddisfatti da 3PL
- numero e tipo di dati gestiti
- smart working
- livello di integrazione nella supply
- automazione e mezzi a guida autonoma

Cybersecurity & logistica marittimo-portuale

I «costi» della «NON *cybersecurity*»

Costo medio violazione dati:
3,56 milioni di dollari

Costo economico dell'attacco informatico

- ✓ Furto di informazioni aziendali
- ✓ Furto di informazioni finanziarie/bancarie
- ✓ Furto di denaro
- ✓ Riparazione/riacquisto di componenti hardware e software a seguito di attacchi
- ✓ Pagamento di riscatti

Conseguenze legali della violazione informatica

- ✓ Multe e sanzioni normative in caso di compromissione di dati personali di clienti o del personale

Danno di reputazione

- ✓ Impatto sul brand equity
- ✓ Riduzione soddisfazione clienti
- ✓ Perdita di clienti (*churn*)
- ✓ Perdita di ricavi (resi, rimborsi, ecc.)
- ✓ Riduzione dei profitti
- ✓ Impatto negativo sulle relazioni con partner, investitori, fornitori e altre terze parti

Aumento dei cash flow negativi

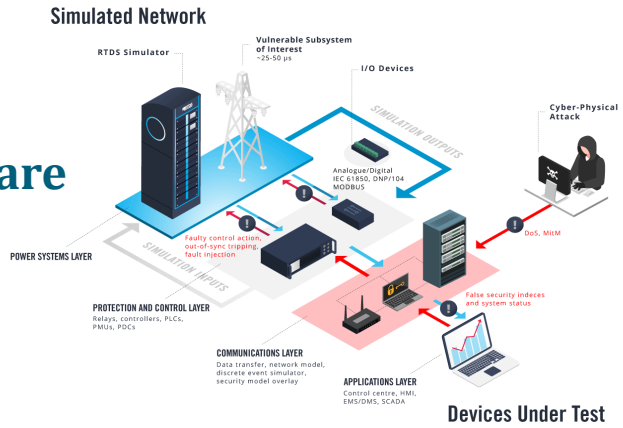
Riduzione dei cash flow positivi

Agenda

1. Cybersecurity & logistica marittimo-portuale
2. **Investimenti per la cybersecurity**
3. Finanziamenti per la cybersecurity

Investimenti in cybersecurity
Principali categorie di investimento/spesa

Hardware



Middleware Software

Servizi

- ✓ Access and authentication
- ✓ Advanced malware prevention
- ✓ Endpoint security
- ✓ Wireless security
- ✓ Data protecion
- ✓ Continuous monitoring
- ✓ Log management
- ✓ Network traffic visibility
- ✓ BYOD security
- ✓ Analytics

Maintenance & repair

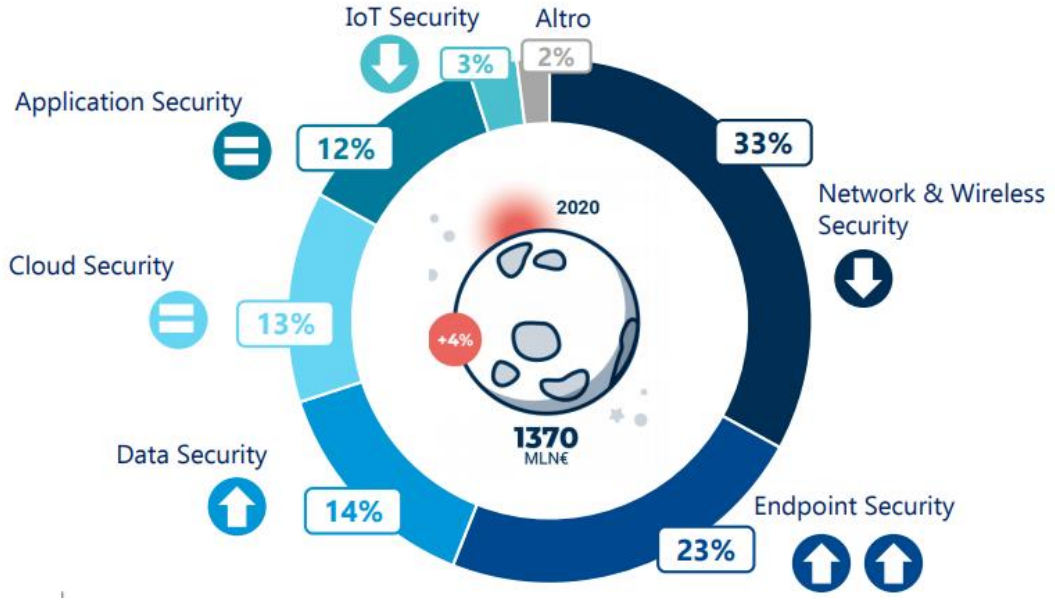
- ➢ **Implicazioni economico-finanziarie**
  - ✓ Capex
  - ✓ Opex
- ➢ **Processi decisionali e scelte d'investimento**
  - ✓ Problematiche di capital budgeting & investment evaluation
  - ✓ Ruolo IT department & CIO.

Personale ICT Formazione

Processi, procedure, monitoraggio

Investimenti in cybersecurity
Tipologie & investimenti realizzati

- A livello mondiale, nel 2020, gli investimenti in cybersecurity hanno raggiunto 153 mld $ (Fortune Business Insights); nel 2021: 166 mld $ (+ 7,8%).
- In Italia, nel 2020: spesa complessiva 1,37 miliardi di euro; crescita del 4% Y.o.Y; 52% per soluzioni di security e 48% per servizi (Osservatorio del Politecnico di Milano, 2021).
- Principali **tipologie di investimenti**:
  - ✓ Network & Wireless Security (protezione infrastruttura da danni e accessi impropri): 33%.
  - ✓ Endpoint Security (protezione di ciascun dispositivo connesso alla rete): 23%.
  - ✓ Data Security (sistemi per la protezione dei dati dell'azienda e dei singoli utenti): 14%.
  - ✓ Sicurezza degli ambienti Cloud: 13%.
  - ✓ Application Security: 12%.
  - ✓ IoT security: 3%.
  - ✓ Cybersecurity awareness e training: 2%.



Campione: 151 grandi imprese

Agenda

1. Cybersecurity & logistica marittimo-portuale
2. Investimenti per la cybersecurity
3. **Finanziamenti per la cybersecurity**

Finanziamenti per la cybersecurity
Digital Europe Programme

➢ **Digital Europe Programme** con budget UE per il periodo 2021-2027 pari a **7,6 mld €**, è il primo programma europeo interamente dedicato alla digitalizzazione.

Network di Digital Innovation Hubs

finanziato con risorse a fondo perduto, per fornire **servizi a PMI e imprese:**

a. *Trasformazione Digitale*, comprese attività di test e attività sperimentali
b. *Scambio buone pratiche tra regioni*, con sinergie tra DIH e PMI di regioni europee diverse
c. *Supporto specifico su intelligenza artificiale, high performance computing e cybersicureity,* ogni DIH potrà specializzarsi su un tema specifico
d. Fornire *sostegno finanziario a parti terze* per lo sviluppo delle competenze digitali avanzate

Definizione di 5 aree tematiche

1. **High performance computing (2,2 mld €)**
2. **Intelligenza Artificiale (2,1 mld €)**
3. **Cybersecurity and Trust (1,6 mld €)** supportando gli Stati Membri nel procurement di sistemi/strumenti di cybersecurity avanzati e infrastrutture di dati implementando sistemi di cybersecurity nel sistema economico, ecc.
4. **Skill Digitali Avanzate (580 mln €)**, con lo sviluppo di sistemi di formazione on the job per studenti, lavoratori e imprenditori per rafforzare le competenze digitali;
5. **Sviluppo e interoperabilità della capacità digitale (1,1 mld €)**

Sinergie tra fondi

✓ **Utilizzo di risorse di programmi diversi in un unico progetto** (Fondi Strutturali della Politica di Coesione - FESR ed FSE+, Horizon Europe, InvestEU e Connecting Europe Facility)
✓ **Finanziamento progetti Seal of Excellence in ambito digitale** con Fondi Strutturali

Finanziamenti per la cybersecurity
Digital Europe Programme

- 28 Call attualmente aperte
- Focus su tecnologie innovative per la cybersecurity come la QCI (Quantum Communication Infrastructure) & QKD (Quantum Key distribution

Grant — Create a European Industrial Ecosystem for Secure QCI technologies and systems

Open for submission

Programme	Digital Europe Programme (DIGITAL)	**Deadline model**	single-stage
ID	DIGITAL-2021-QCI-01-INDUSTRIAL	**Opening date**	17 November 2021
Types of action	Digital SME Support Actions	**Deadline date**	22 February 2022 17:00:00 Brussels time

Grant — Deploying advanced national QCI systems and networks

Open for submission

Programme	Digital Europe Programme (DIGITAL)	**Deadline model**	single-stage
ID	DIGITAL-2021-QCI-01-DEPLOY-NATIONAL	**Opening date**	17 November 2021
Types of action	DIGITAL Simple Grants	**Deadline date**	22 February 2022 17:00:00 Brussels time

Finanziamenti per la cybersecurity
HORIZON EUROPE & Cybersecurity

- Dal 30.06.2021 è aperto il bando **Increased cybersecurity 2021** (HORIZON-CL3-2021-CS-01) del Programma di lavoro 2021-2022 del Cluster Civil Security for Society di Horizon Europe.
- Il bando rientra nella Destination 4 - Increased Cybersecurity che ha l'obiettivo di promuovere una maggiore sicurezza informatica e un ambiente online più sicuro nell'UE e negli Stati membri, assicurando la protezione dei dati e delle reti, nel rispetto della privacy e di altri diritti fondamentali, con azioni volte allo sviluppo di servizi, processi e prodotti sicuri, nonché a solide infrastrutture digitali in grado di resistere/contrastare gli attacchi informatici e minacce ibride.
- Il banco contiene 4 topic RIA (Research & Innovation Action) per un budget complessivo pari a 67,5 milioni di €:
  - ✓ HORIZON-CL3-2021-CS-01-01: Dynamic business continuity and recovery methodologies based on models and prediction for multi-level Cybersecurity
  - ✓ HORIZON-CL3-2021-CS-01-02: Improved security in open-source and openspecification hardware for connected devices
  - ✓ HORIZON-CL3-2021-CS-01-03: AI for cybersecurity reinforcement
  - ✓ HORIZON-CL3-2021-CS-01-04: Scalable privacy-preserving technologies for crossborder federated computation in Europe involving personal data

Finanziamenti per la cybersecurity
HORIZON EUROPE & Cybersecurity

Grant

Improved monitoring of threats, intrusion detection and response in complex and heterogeneous digital systems and infrastructures

Forthcoming

Programme	Horizon Europe (HORIZON)	**Deadline model**	single-stage
ID	HORIZON-CL3-2022-CS-01-01	**Opening date**	30 June 2022
Types of action	HORIZON Innovation Actions	**Deadline date**	16 November 2022 17:00:00 Brussels time

- ✓ Tipo di azione: Innovation Action (IA)
- ✓ Contributo previsto dell'UE: circa 21,00 milioni €
- ✓ Technology Readiness Level: le attività dovranno raggiungere TRL 7 entro la fine del progetto.
- ✓ Descrizione: le proposte dovranno sviluppare e convalidare prototipi dimostrativi di strumenti e tecnologie per monitorare e analizzare gli incidenti di cybersecurity in un ambiente operativo in linea con la direttiva NIS e il regolamento generale sulla protezione dei dati. I risultati contribuiranno a migliorare i metodi di test di penetrazione e la loro automazione utilizzando l'apprendimento automatico e altre tecnologie di intelligenza artificiale.

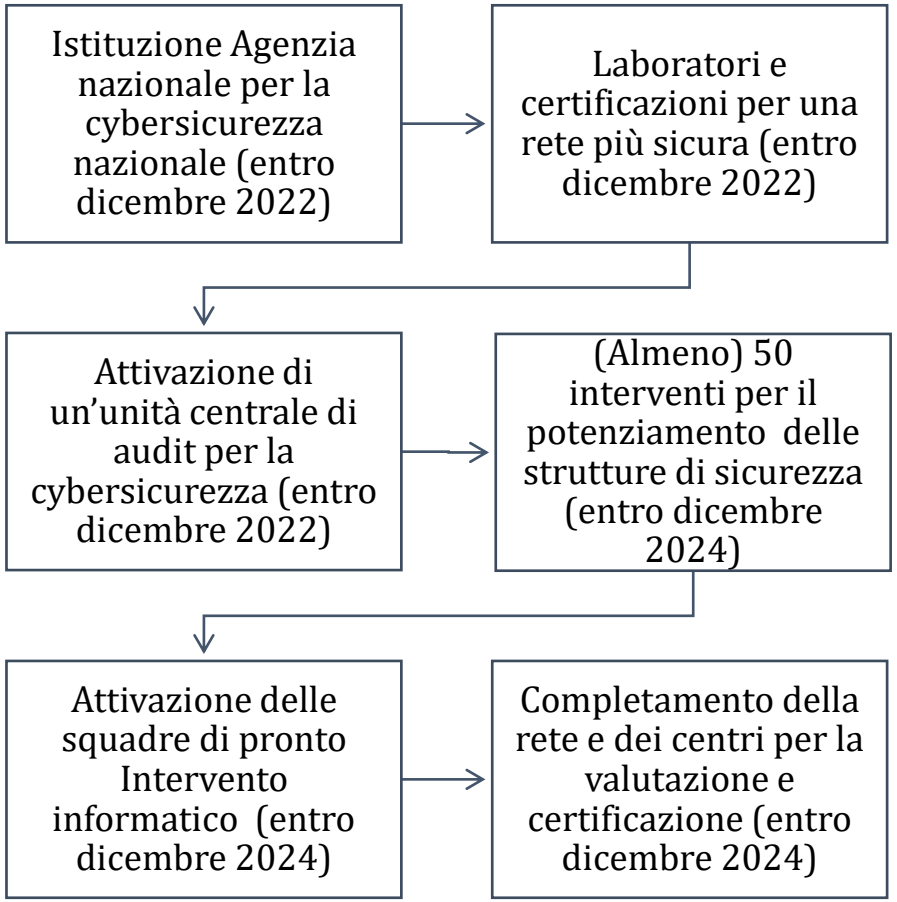
Finanziamenti per la cybersecurity

PNRR & Cybersecurity

623 milioni € sono destinati a rafforzare le difese di cybersecurity nelle Pubbliche amministrazioni.

1. Rafforzare le capacità di prima linea per gestire gli alert e le situazioni di attacco.
2. Rafforzare le capacità di ispezione e audit del Paese di hardware e software per certificare l'affidabilità e prevenire le minacce.
3. Potenziare le forze dell'ordine e le unità informatiche all'interno delle Forze di Polizia preposte alle indagini su attività criminali.
4. Rafforzare le risorse informatiche e umane responsabili della sicurezza nazionale e della risposta alle minacce informatiche.

Le tappe



Finanziamenti per la cybersecurity
Forme di finanziamento per le imprese

Finanziamenti a fondo perduto e finanziamenti agevolati

- ✓ **Legge Sabatini**: Riapertura con fondo perduto per rinnovare macchinari e attrezzature.
- ✓ **CYBER 4.0**: Contributi a fondo perduto per progetti di R&S in ambito cybersecurity.

Sgravi fiscali e contributi

- ✓ **Piano Industria 4.0** e **Piano Transizione 4.0**: Credito d'imposta per beni materiali e immateriali.

Garanzia di credito

Strumenti di intervento nel capitale di rischio

Grazie per l'attenzione

Prof. Giovanni Satta

Università degli Studi di Genova;
CIELI & DIEC
giovanni.satta@economia.unige.it

Genova, 24/01/2022

UNIVERSITÀ DEGLI STUDI DI GENOVA

LOGISTIC DIGITAL COMMUNITY