WORKSHOP GARR 2023

NET MAKERS

Uno Strumento per l'Auto Valutazione del Cyber Risk

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

Danilo Montesi - danilo.montesi@unibo.it

Università di Bologna

Sommario

- Introduzione e Motivazioni
- Il modello del rischio nel contesto informatico
- Il Cyber Risk Self Assessment Tool
- Risultati
- Conclusioni e Sviluppi Futuri

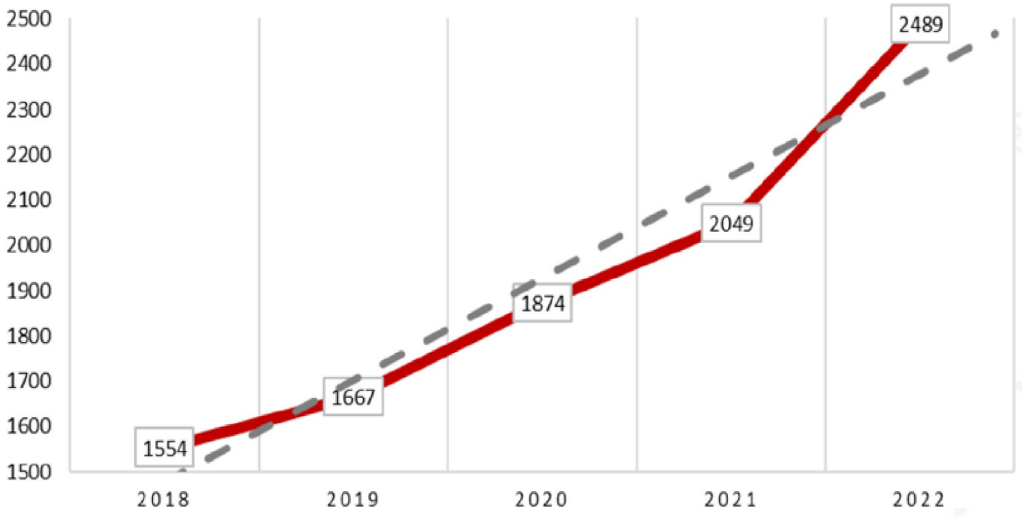
Introduzione

- La continua **espansione delle tecnologie** come strumenti di lavoro (e.g., dispositivi mobili, servizi cloud) ha portato ad una **maggiore vulnerabilità** dell'intero spazio cibernetico
- Sono sempre più evidenti le possibili **conseguenze** di un evento informatico per le imprese e le società, sia **in termini di business continuity che di privacy**
- Molte aziende considerano la **cybersecurity** come un **rischio d'impresa**

Contesto Italiano

Andamento dei cyber attacchi nel periodo 2018 - 2022

[*Clusit Rapporto 2023*]



Settori più colpiti in Italia (valori %)

[*Il Sole 24 Ore, 7 Marzo 2023*]

Motivazioni

- La realizzazione di un modello per la valutazione del rischio informatico necessita di una base di dati:
  - Registro dei **profili** che identificando la **classe di rischio** di appartenenza
  - Registro di tutti gli **incidenti informatici** ai fini della realizzazione di una **serie storica**

- I profili e gli incidenti devono essere messi in correlazione con il dataset degli eventi per modulare variabili e pesi di un modello predittivo di rischio cibernetico

Rischio: Definizione Generale

- Il **rischio** *R* è dato dalla **probabilità** *P* (o frequenza) del verificarsi di un determinato evento per l'**impatto** *I* (o danno) che genera l'evento

$$R = P \times I$$

Rischio: Contestualizzazione Cyber

$$R = P \times I$$

- È complesso determinare la **probabilità a causa di**:
  - Continua evoluzione delle tecnologie: nuove vulnerabilità e nuove tipologie d'attacco
  - Mancanza di serie storiche
- È complesso stimare l'**impatto**:
  - Difficile quantificare i danni a beni immateriali come know-how, dati personali/medici, dati finanziari e alla reputazione

Cyber Risk Modello

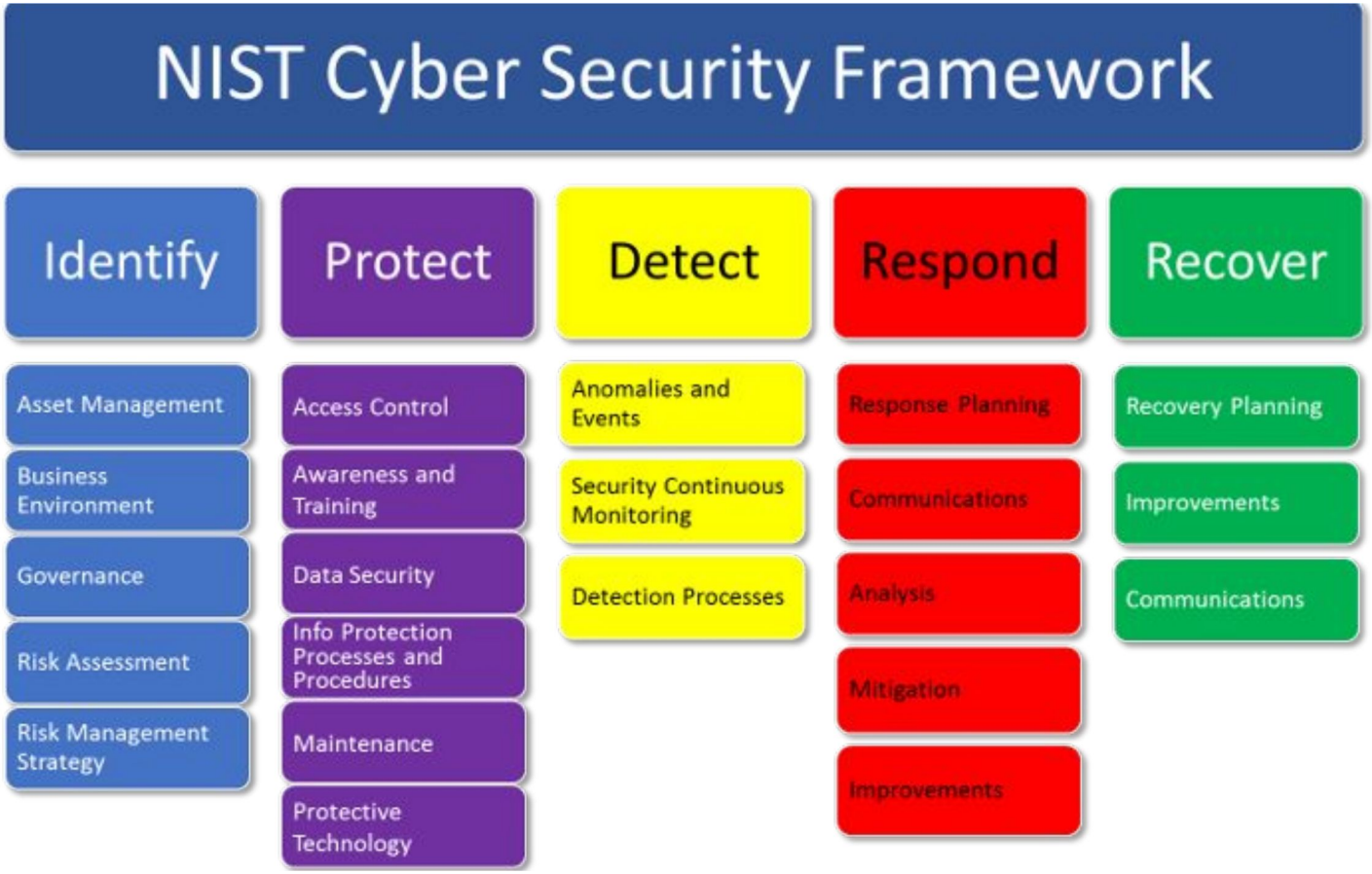
- La probabilità *P* è sostituita dall'indice di sicurezza *S* e dall'esposizione *E*

$$R_C = S \times E \times I$$

  - **Indice di Sicurezza (S)**: basato sulle 22 attività previste dal "Framework for Improving Critical Infrastructure Cybersecurity" redatto dal National Institute of Standards and Technology*
  - **Esposizione (E)**: riguarda l'identificazione dei fattori interni ed esterni che interessano l'esposizione al rischio

*Il NIST sta lavorando alla nuova versione *Cybersecurity Framework 2.0* atteso per il 2024.

Indice di Sicurezza



- Indice di sicurezza associa ad ogni area un livello di
  - maturità
  - priorità in base al contesto in cui si opera

Esposizione

- Riguarda l'identificazione dei fattori interni ed esterni che interessano l'esposizione al rischio
  - I **fattori interni** sono quelli legati ai **dati detenuti**, per cui è **la tipologia e la quantità** a determinare questo fattore
  - I **fattori esterni** sono alcune **caratteristiche dell'organizzazione** (e.g., settore, stato, dimensione) direttamente collegate con le **tipologie di attacco**

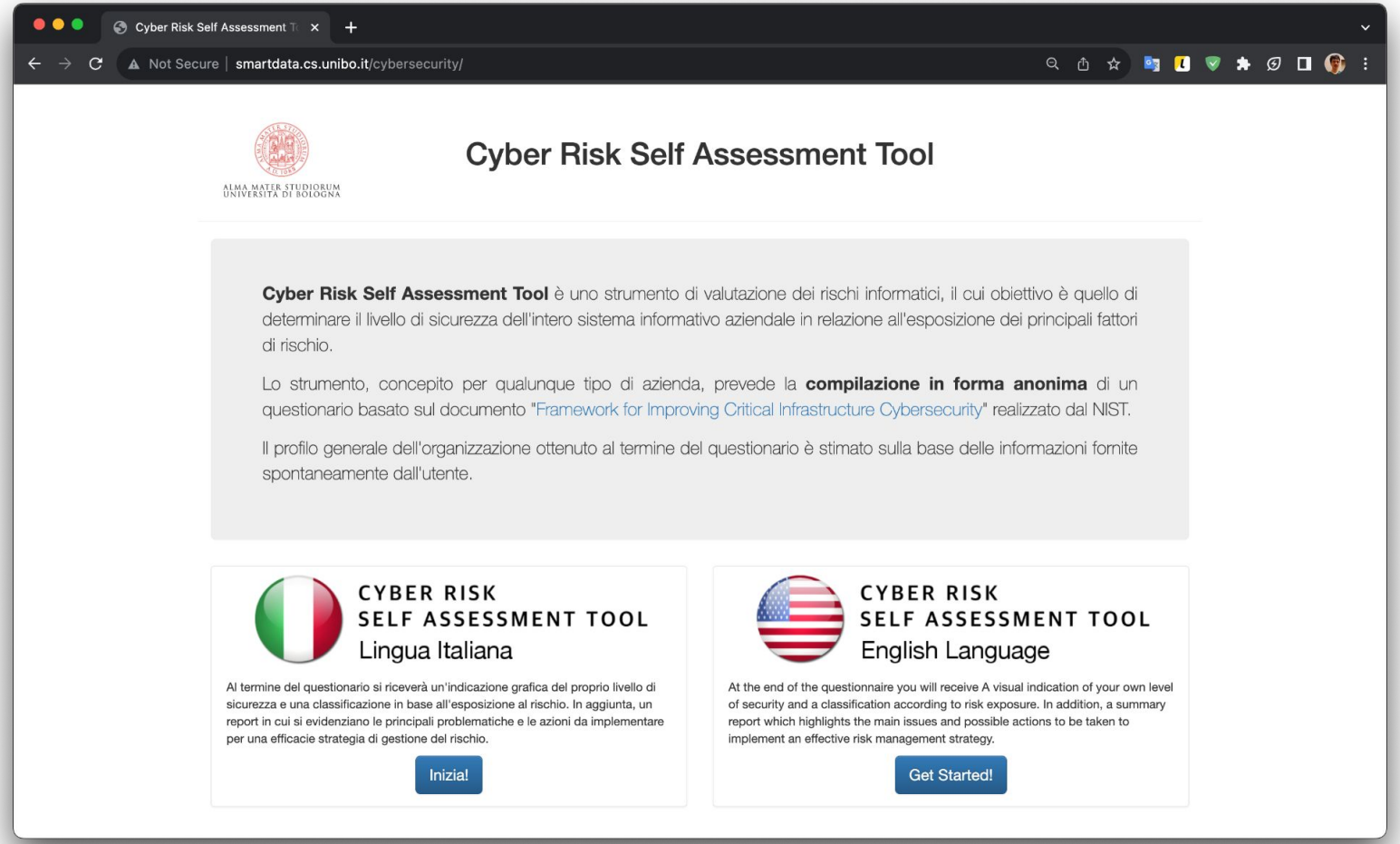
Strumento di Prima Diagnosi (1)

- Obiettivi del questionario:
  - riassumere graficamente il proprio **livello di sicurezza**, fornendo una **classificazione** in base all'**esposizione al rischio**
  - fornire un report in cui si evidenziano le **principali problematiche**, suggerendo le **azioni da implementare** per una efficace strategia di gestione del rischio informatico

Strumento di Prima Diagnosi (2)

- Il questionario ha una duplice valenza:
  - di effettuare un **self-assessment** da parte delle aziende e delle organizzazioni, dando una prima valutazione di rischio cibernetico
  - di **catalogare** (in forma anonima) come le suddette entità sono organizzate nelle varie aree di gestione del rischio, raccogliendo i dati a fini statistici

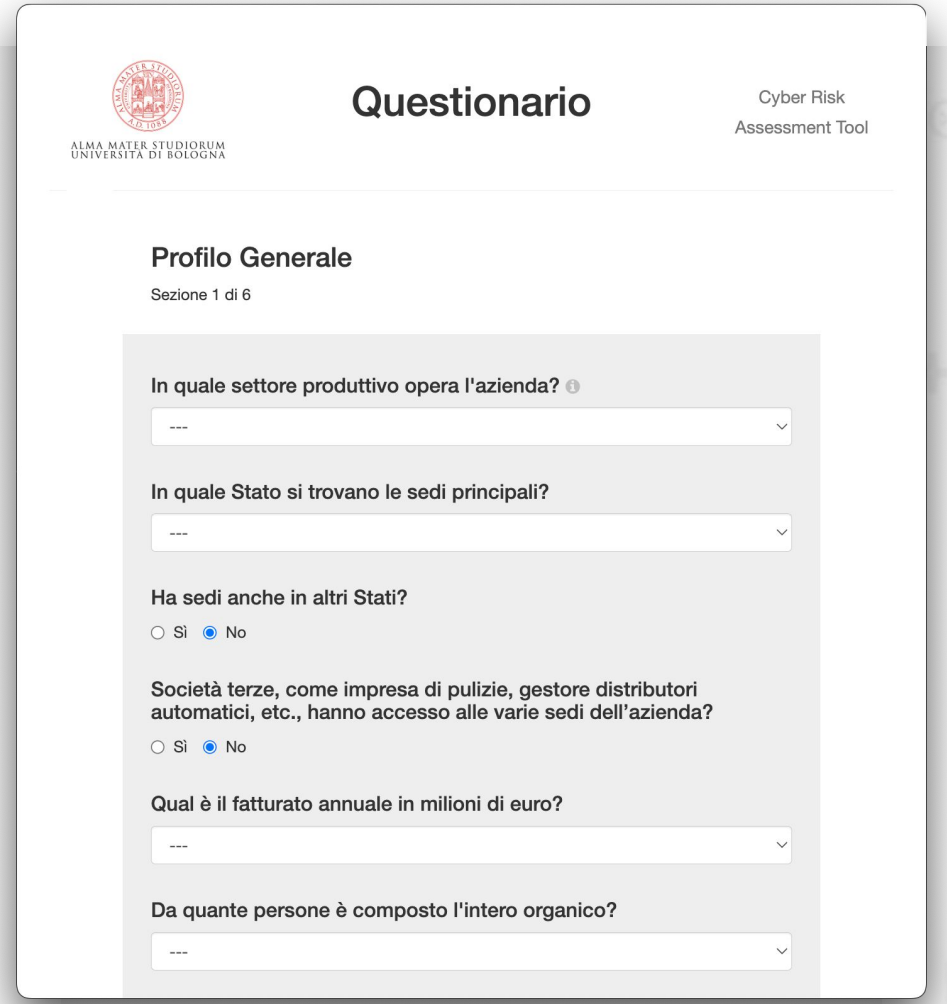
Cyber Risk Self Assessment Tool



http://smartdata.cs.unibo.it/cybersecurity

Questionario

- Allineato a strumenti simili:
  - IBM Data Breach Risk Calculator [*non più disponibile*]
  - AON Cyber Risk Diagnostic Tool [*non più disponibile*]
  - Marsh Cyber Risk Self-Assessment Tool [*non più disponibile*]
  - Cyber Security Assessment Tool [*a pagamento*]
- Basato sulle aree del framework proposto dal NIST



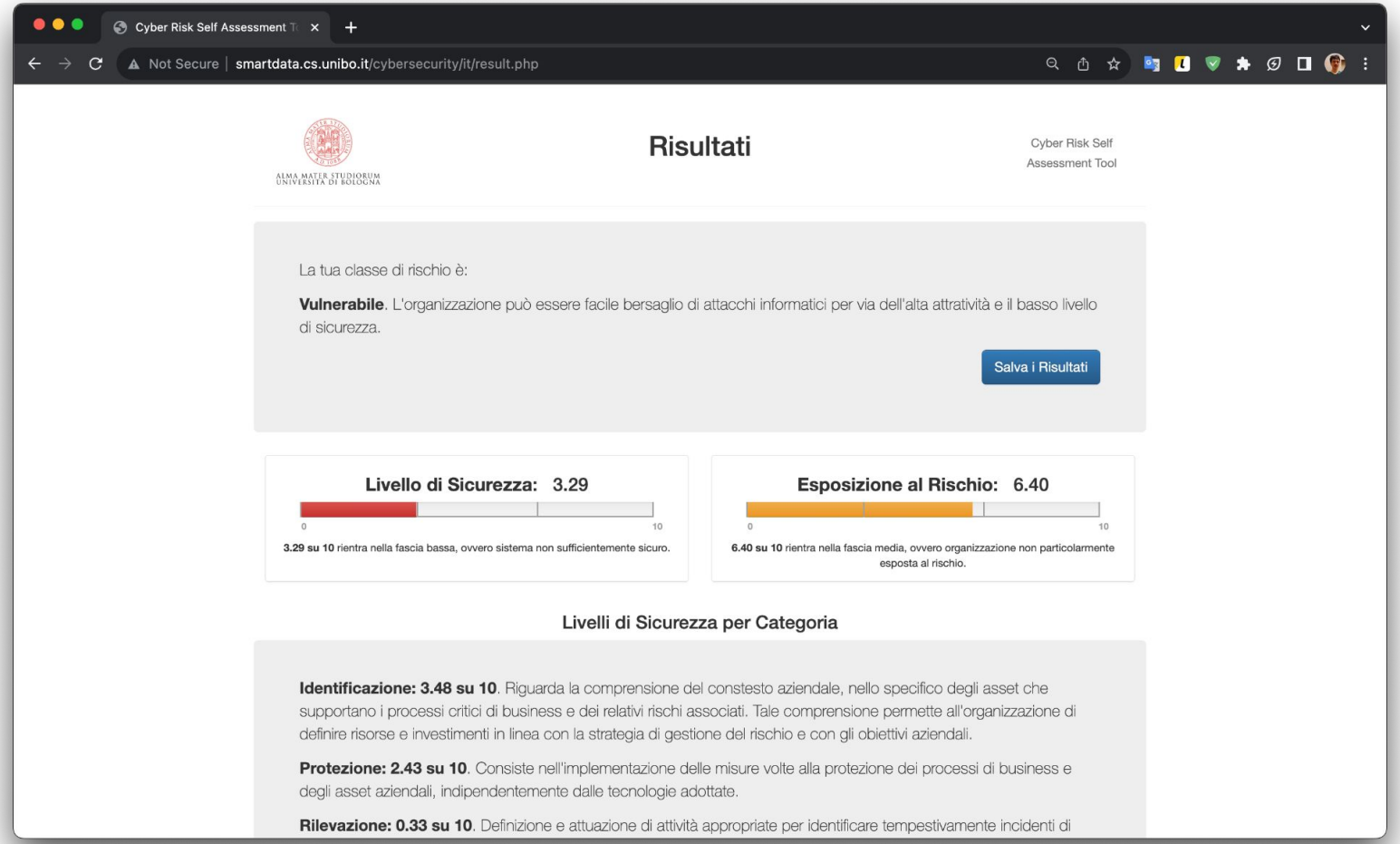
Risultati: Classi di Rischio

- Le quattro classi di rischio identificate dal questionario per aziende e organizzazioni sono:
  1. **Resistente**: (*sicurezza alta e esposizione bassa*) il soggetto non si espone al rischio ed ha un sistema sufficientemente maturo
  2. **Sensibile**: (*sicurezza alta e esposizione alta*) a rischio attacco anche se si seguono correttamente le procedure
  3. **Inesperto**: (*sicurezza bassa e esposizione bassa*) occorre alzare il livello di sicurezza per evitare incidenti
  4. **Vulnerabile**: (*sicurezza bassa e esposizione alta*) caso pessimo in cui l'organizzazione può essere facile bersaglio di attacchi informatici per via dell'alta attrattività

Risultati: Livello di Sicurezza

- Le quattro aree per il livello di sicurezza identificate dal questionario aziende e organizzazioni sono:
  1. **Identificazione**: comprensione del contesto aziendale e degli asset che supportano i processi critici di business
  2. **Protezione**: implementazione delle misure volte alla protezione dei processi di business e degli asset aziendali
  3. **Rilevazione**: definizione e attuazione di attività appropriate per identificare tempestivamente incidenti di sicurezza informatica
  4. **Resilienza**: intervento e gestione dei piani di ripristino dei processi e dei servizi durante e/o a seguito di un incidente informatico

Cyber Risk Self Assessment



[Report con i risultati]

Conclusioni

- Il Cyber Risk Assessment Tool può essere utilizzato come **strumento di prima valutazione** del cyber-rischio
  - Se impiegato da imprese permette di evidenziare le **principali problematiche** ed individuare le azioni utili per una efficace **strategia di gestione del rischio**
  - Se impiegato da compagnie assicurative rappresenterebbe uno strumento più accurato per la **definizione del premio assicurativo**

Sviluppi Futuri

- **Conservazione sicura dei profili** (anonimi) di rischio
- **Integrazione** di
  - Cybersecurity Framework 2.0 (NIST)
  - Framework Nazionale per la Cybersecurity e la Data Protection (CINI Cybersecurity National Lab)
- **Allineamento alla normativa recente** relativa al trattamento dei dati e ai mercati digitali
  - General Data Protection Regulation (GDPR)
  - Digital Services Act (DSA)
  - Digital Markets Act (DMA)
- **Sviluppare un modello predittivo del rischio cibernetico**, combinando i **profili** di rischio (indici di sicurezza + esposizione) con i dati degli **incidenti informatici**

Grazie per l'attenzione

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

Danilo Montesi - danilo.montesi@unibo.it

Credits: Flavio Bertini e Matteo Tiscornia