BANCA D'ITALIA
EUROSISTEMA

III Conferenza Nazionale

Cybersecurity nelle Infrastrutture critiche: tipologie di rischio e risposte di sistema

La gestione del rischio nelle Infrastrutture critiche tra norme e compliance

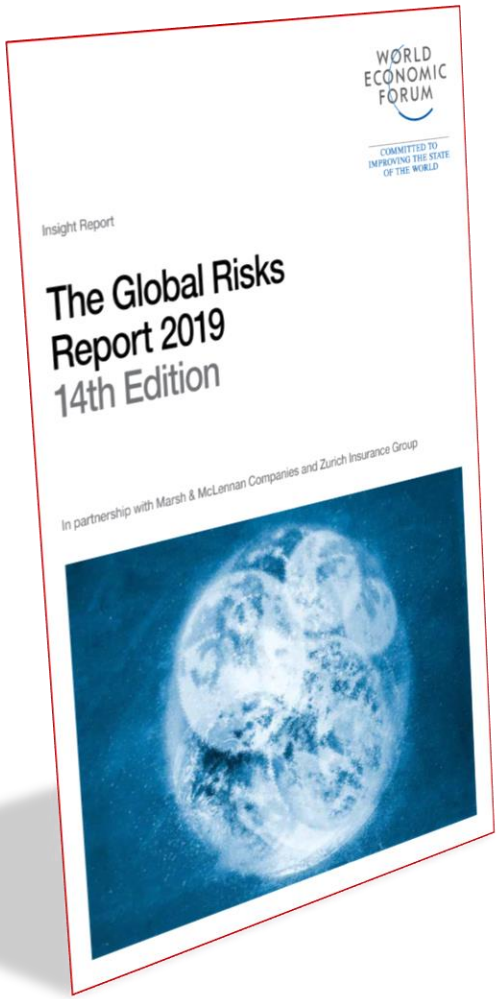
Claudio Impenna (claudio.impenna@bancaditalia.it)

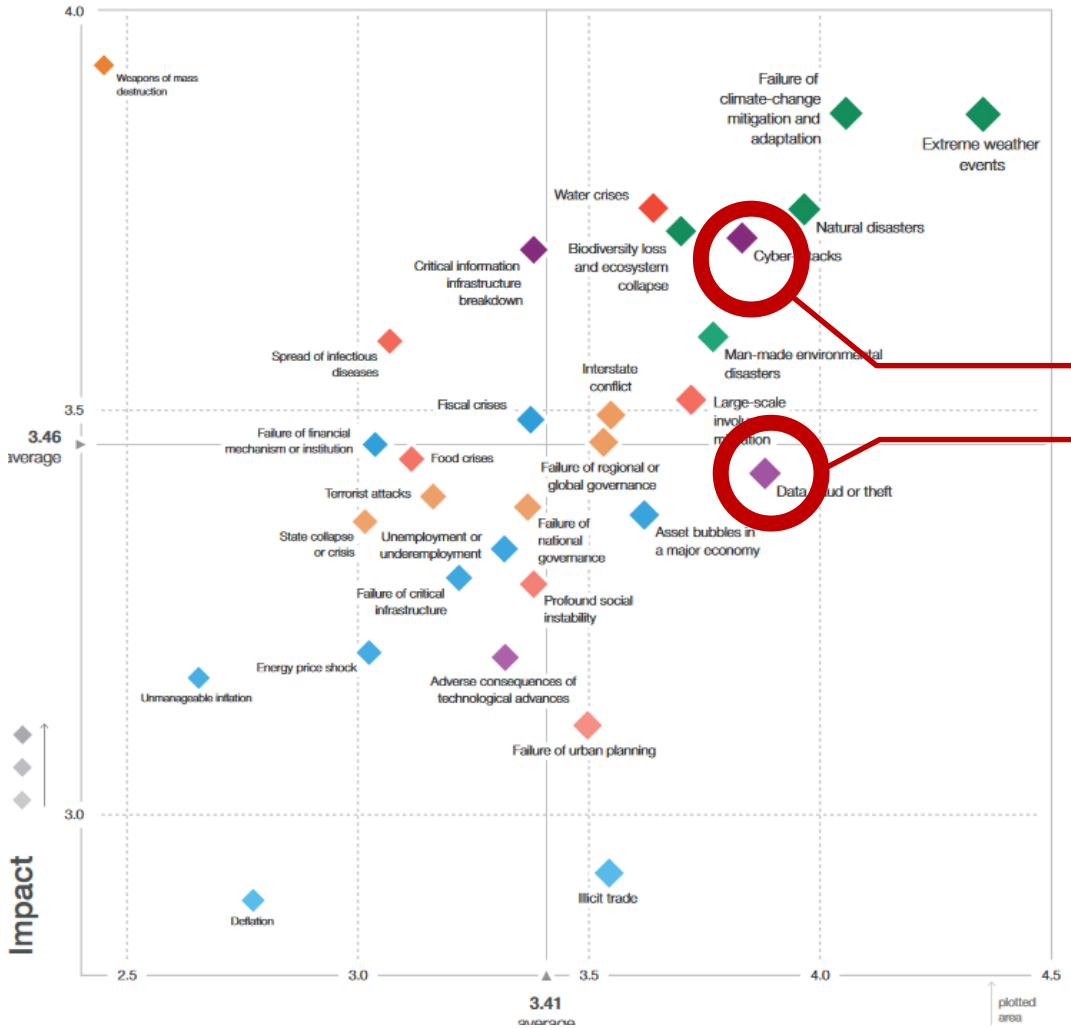
Dipartimento Mercati e sistemi di pagamento
Capo del Servizio Supervisione mercati e sistema dei pagamenti

Università di Tor Vergata, Roma 20 gennaio 2019

Rischio cyber nel settore finanziario e rilevanza sistemica

Perchè la sicurezza dello spazio cibernetico e la protezione delle infrastrutture critiche è una priorità



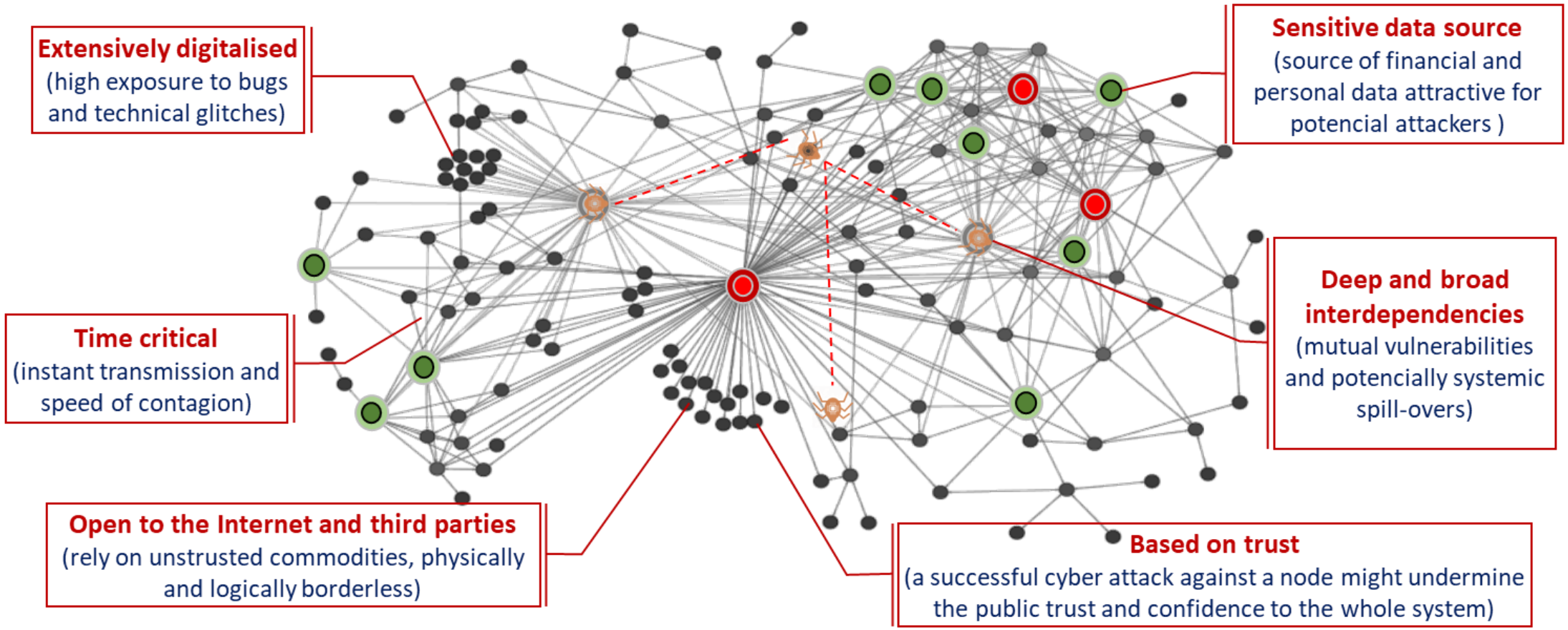


Gli attacchi cibernetici e il furto di dati sono indicati tra i principali rischi globali dopo gli eventi legati agli straordinari cambiamenti climatici e ai disastri naturali

Fonte: WEF, The Global Risks Report 2019

Rischio cyber nel settore finanziario e rilevanza sistemica

- Perchè il settore finanziario è esposto ai rischi cyber?
  - target attrattivo per una moltitudine di potenziali attori della minaccia
  - caratteristiche che ne aumentano l'esposizione, con possibili ricadute sistemiche



Fonte: ECB, Eurosystem Oversight Cyber Resilience Strategy – Map of the FMIs in Europe (2018)

Sfide per le Autorità e l'approccio alla Cyber security

- Necessità di integrare gli strumenti tradizionali di gestione del rischio operativo e della Business Continuity con nuove regole e strumenti

- Focalizzazione degli interventi su 4 aree di policy:
  - Regolamentazione e Supervisione
  - Cooperazione, coordinamento e scambio informativo (cross-authority, cross-industry e pubblico-private)
  - Cultura del rischio e Cyber security Awareness
  - Capacità di protezione degli asset infomativi da scenari di rischio emergenti

- Armonizzazione delle iniziative a livello nazionale, europeo ed internazionale

- Gradualità e applicabilità degli interventi a diversi livelli:
  - Singola entità
  - Categoria di soggetti/Comparto (es. Operatori finanziari sistemici, Operatori di Servizi Essenziali, Assicurazioni, …)
  - Settore
  - Intersettoriale

Sfide per le Autorità e l'approccio alla Cyber security

- Le Banche Centrali rivolgono particolare attenzione alla Cyber security in relazione ai diversi compiti svolti e al mandato di assicuare la stabilità finanziaria, l'efficienza e l'affidabilità del sistema dei pagamenti e di preservare la fiducia del pubblico nella moneta

FORNITORE DI SERVIZI IT

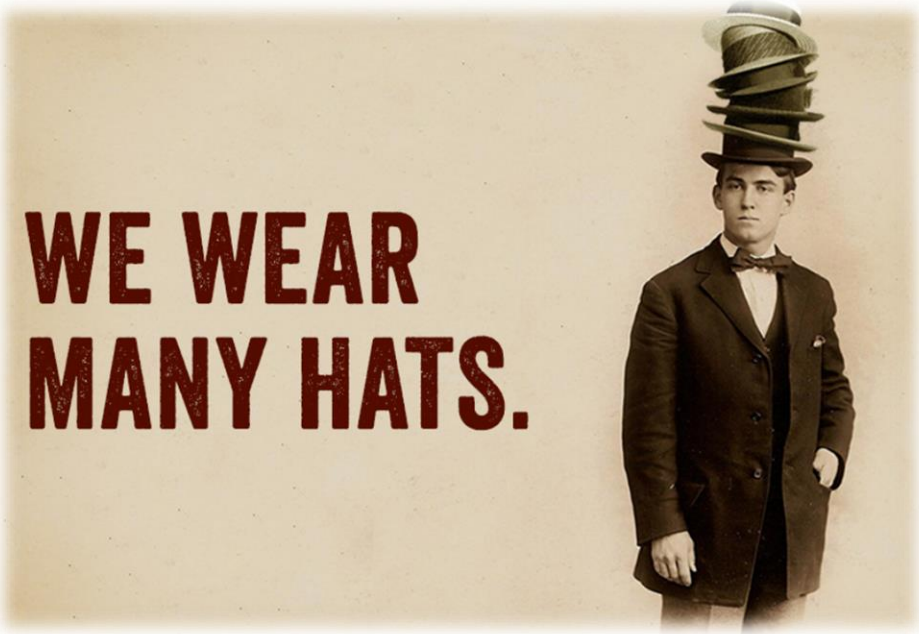
(Infrastruttura Critica Informatizzata ai sensi DM 9 gen. 2008 del Min. Interno)

CENTRO DI ANALISI

(Ricerca e analisi economica, advisory per Governo e Istituzioni)

BANCA

(Gestore di infrastrutture finanziarie)



AUTORITA'

(Regolamentazione e supervisione in campo creditizio e finanziario)

CATALYST

(per favorire la cooperazione e sviluppo di soluzioni di sistema)

Iniziative per rafforzare la Cyber Resilience del settore finanziario

- A livello internazionale, a partire dal 2016, il G7 *(Finance Track)* ha pubblicato un insieme di principi di alto livello *(Fundament Elements)* e non vincolanti *(soft law)* per rafforzare la Cyber Resilience del settore finanziario

G7 Fundamental Elements of Cyber Security for the financial sector, Oct. 2016

G7 Fundamental Elements for effective assessment of cybersecurity in the financial sector, Oct. 2017

G7 Fundamental Elements on Threat-Led Penetration Testing (FE-TLPT, Oct. 2018)

G7 Fundamental Elements on third party cyber risk management (FE-TPCRM, Oct. 2018)

- A giugno 2019 si è svolta una simulazione G7 basata su uno scenario di **attacco cibernetico su larga scala cui hanno partecipato 24 autorità finanziarie** con l'obiettivo di testare il livello di preparazione e i meccanismi di coordinamento tra le autorità in caso di grave attacco cyber ai danni del Sistema finanziario internazionale

Iniziative per rafforzare la Cyber Resilience del settore finanziario

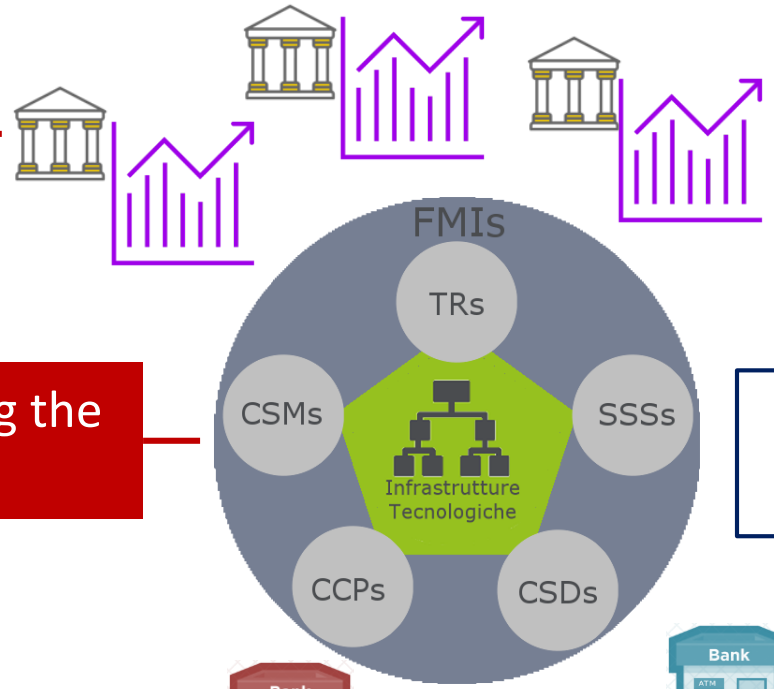
- Coerentemente con i principi G7, a livello G20/FSB, è stata avviata una serie di iniziative per perseguire strategie condivise e sviluppare strumenti armonizzati a livello internazionale:

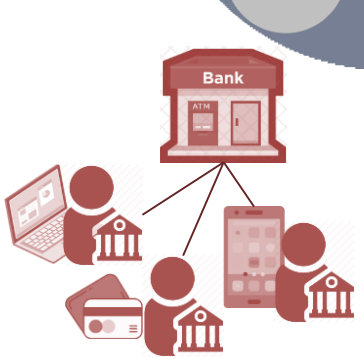
Mercati:
- sedi di negoziazione

Infrastrutture di mercato:
- sistemi di pagamento
- depositali Centrali Titoli
- controparti centrali

Service Provider:
- outsourcer
- fornitori di servizi IT

Protecting the Core





Securing the Periphery

Utenti:
- Cittadini
- Imprese
- PA

Intermediari finanziari:
- Istituti di credito
- Altri PSPs

Risposta delle autorità per a Cyber Resilience del settore finanziario

- Allo scopo di sostenere l'applicazione armonizzata della CPMI-IOSCO Cyber Guidance in Europa, l'Eurosistema si è dotato di una Strategia di Cyber Resilience per le Infrastrutture finanziarie

CPMI-IOSCO Guidance on Cyber Resilience for Financial Market Infrastructures (2016)

Iniziative per rafforzare la Cyber Resilience del settore finanziario

- Altre rilevanti iniziative legislative dell'UE:
  - NIS Directive (Direttiva 2016/1148 sulla sicurezza delle reti e dei sistemi informativi) recepita in Italia con D. Lgs. 65/2018 con cui il MEF, in collaborazione con Banca d'Italia e CONSOB, è designata quale autorità competente per i settori Bancario e delle Infrastrutture Finanziarie
  - PSD-2 (Direttiva 2015/2366/UE convertita con D.Lgs.2018/2017) e normativa secondaria *(Guidelines and Regulatory Technical Standards)* dell'EBA
- Da ultimo, l'ECOFIN ha avviato riflessioni sulle minacce ibride e sulla possibile inclusione delle infrastrutture finanziarie nel quadro normativo delle infrastrutture critiche Europee (Direttiva 2008/114) anche in relazione alle previsioni contenute nella *EU Strategic Agenda for 2019-2024 e nel Cyber Security Act*
  - tale inclusione, condivisibile per la rilevanza cross-sector e cross-border dei servizi e delle infrastrutture finanziarie, presenta un trade-off tra le norme nazionali di sicurezza e protezione del paese in cui un'infrastruttura è insediata (esigenze di sicurezza nazionale), l'esigenza di un coordinamento intersettoriale e transfrontaliero in caso di incidente e gli obiettivi del mercato unico (integrazione, apertura, competitività)

Iniziative per rafforzare la Cyber Resilience del settore finanziario

- In ambito nazionale, il rafforzamento della resilienza cibernetica del settore finanziario è un obiettivo strategico della Banca d'Italia perseguito con due piani d'azione:

  1. Accrescere la sicurezza e la continuità di servizio del settore finanziario italiano attraverso l'attuazione – anche nell'ambito del nucleo per la risposta a emergenze informatiche per il settore finanziario italiano (CERTFin) – di una strategia di cyber resilience per le infrastrutture di mercato italiane (rilevanza esterna)

  2. Rafforzare la cyber security della Banca in relazione a nuovi scenari di rischio (rilevanza interna)

- Con riferimento al punto 1, la Banca d'Italia e la Consob hanno concordato una strategia comune per rafforzare la sicurezza cibernetica del settore finanziario italiano attraverso specifiche misure rivolte alle infrastrutture finanziarie: sistemi di pagamento, controparti centrali, depositari centrali e sedi di negoziazione dei titoli (*Comunicato stampa 16 gen. 2020*)

- Tale strategia prevede tra l'altro il ricorso a strumenti di valutazione del rischio adottati in ambito Eurosistema e in particolare l'adozione e lo svolgimento di test avanzati di tipo *Red Teaming (Threat Intelligence-Based Ethical Red Teaming, TIBER-IT)*

Iniziative per rafforzare la Cyber Resilience del settore finanziario

- Da marzo 2018 è attivo il tavolo di coordinamento partecipato da Banca d'Italia, CONSOB e MEF per l'attuazione della Direttiva NIS (D. Lgs. 65/2018) al settore bancario e a quello delle infrastrutture finanziarie

- È in corso un confronto con le autorità competenti per l'attuazione della L. 133/2019 in materia di perimetro di sicurezza nazionale cibernetica sia per i profili di raccordo con il D. Lgs. 65/2018 e con la regolamentazione di settore, sia per le potenziali ricadute sul settore finanziario nel suo complesso e sull'Istituto.

- In relazione al rafforzamento della cooperazione pubblico-privato la Banca d'Italia, insieme con l'Associazione Bancaria Italiana, ha promosso la costituzione del CERTFin, operativo da gennaio 2017, considerato un modello di riferimento nell'ambito delle cosiddette *Public-Private Collective Actions on Cyber security*

Iniziative per rafforzare la Cyber Resilience del settore finanziario

Il Computer Emergency Response Team Finanziario Italiano (CERTFin)

Iniziativa cooperativa pubblico-privato volta a migliorare la gestione del rischio cibernetico da parte degli operatori bancari e finanziari e a rafforzare la cyber resilience del sistema finanziario italiano

- Fungere da punto di **contatto unico** per il settore finanziario e verso gli altri settori strategici
- Facilitare lo **scambio tempestivo di informazioni** su potenziali minacce cyber
- Facilitare le **risposte agli incidenti cyber** di larga scala
- Supportare il **processo di gestione delle crisi cyber** attraverso il raccordo con il **l'Unità di coordinamento delle crisi operative della piazza finanziaria italiana (Codise)**
- Cooperare con altre strutture omologhe (**CERTs/CSIRTs)** e istituzioni nazionali ed internazionali
- Promuovere iniziative di **training & awareness**

Fonte: www.certfin.it

Conclusioni e punti di attenzione

- La cyber security e la protezione delle infrastrutture critiche è una priorità di governi e istituzioni perché gli attacchi cibernetici e il furto di dati sono tra i principali rischi globali

- La Banca d'Italia è profondamente impegnata nel rafforzamento della Cyber Resilience del settore finanziario attraverso:
  I. il sostegno alle iniziative legislative, l'aggiornamento e l'attuazione della regolamentazione e delle metodologie di supervisione
  II. la promozione della cooperazione tra autorità e con l'Industria finanziaria
  III. l'innalzamento della consapevolezza sul rischio cibernetico nelle attività finanziarie, nel settore dei pagamenti e in quello assicurativo (in collaborazione con IVASS e in relazione ai programmi di Educazione finanziaria)
  IV. la protezione dei propri asset informativi a supporto dei servizi offerti al Paese e all'Eurosistema

- Sebbene le iniziative sin qui realizzate e quelle in fase di sviluppo hanno contribuito e contribuiranno a rafforzare la resilienza cibernetica del settore finanziario e del Paese, permangono comunque **gap e punti di attenzione**

Conclusioni e punti di attenzione

- Trade-off tra le esigenze di sicurezza nazionale, integrazione del sistema finanziario e sviluppo del mercato unico
- Promuovere l'armonizzazione tra le diverse fonti normative che insistono sulla stessa materia per:
  - Assicurare competitività e parità di trattamento attraverso la gradualità e la proporzionalità nell'applicazione di regole e strumenti (level playing field)
  - Contenere gli oneri di compliance evitando, ove possibile, duplicazioni e sovrapposizioni (es. incident reporting dello stesso evento secondo criteri e schemi differenti: GDPR, EMIR, CSDR, MIFID2, NIS-D, PSD-2, L.133/2019, Cir. 285, Codise, …)
- Gestire il cambiamento in ottica di miglioramento continuo in relazione alla rapida trasformazione digitale e all'evoluzione del quadro della minaccia
- Investire su fattore umano
  - trasformare le persone da anello più debole della catena a prima e più efficace linea di difesa (awareness)
  - fronteggiare l'esigenza di risorse qualificate per lo sviluppo del Paese e il contenimento dei tempi di realizzazione di iniziative e progetti (es. skill e competenze per lo svolgimento di Threat-led Penetration Tests)