

Banche e Sicurezza, 14-15 maggio 2024

IL RISCHIO CYBER PER IL SISTEMA FINANZIARIO: LE RISPOSTE DELLE AUTORITA' E IL RUOLO DELL'INNOVAZIONE

Claudio Impenna

Capo Servizio Supervisione mercati e sistemi di pagamento

Evoluzione delle minacce e rilevanza sistemica del rischio cyber

Minacce più diffuse

- Attacchi *ransomware*
- Campagne DDoS
- *Phishing* e distribuzione di *malware*



Spinte da differenti motivazioni

- Spionaggio cyber
- Guerra ibrida, attivismo
- Frodi, interessi economici



Amplificate da...

- Tensioni geopolitiche
- Tecnologie emergenti (e.g. AI and QC)

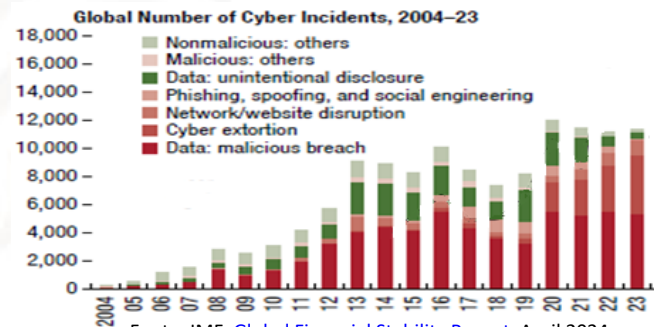
Italia	2022	2023	Δ%
Eventi cyber	1094	1411	+29,0 %
Incidenti cyber	126	303	+140,5 %

- Settore finanziario tra i più colpiti
- Italia tra i paesi più interessati da campagne **DDoS** e attacchi **Ransomware (3° in Europa e 6° al mondo)**

Fonte: ACN, [Relazione annuale 2023](#)

Intermediari finanziari italiani	2021	2022	2023
Notifica major cyber incidents	12	13	30

Fonte: Banca d'Italia, [Rapporto Stabilità Finanziaria 1-2024](#)



Fonte: IMF, [Global Financial Stability Report](#), April 2024

Come fronteggiare i nuovi rischi: le risposte delle Autorità



EUROPEAN CENTRAL BANK

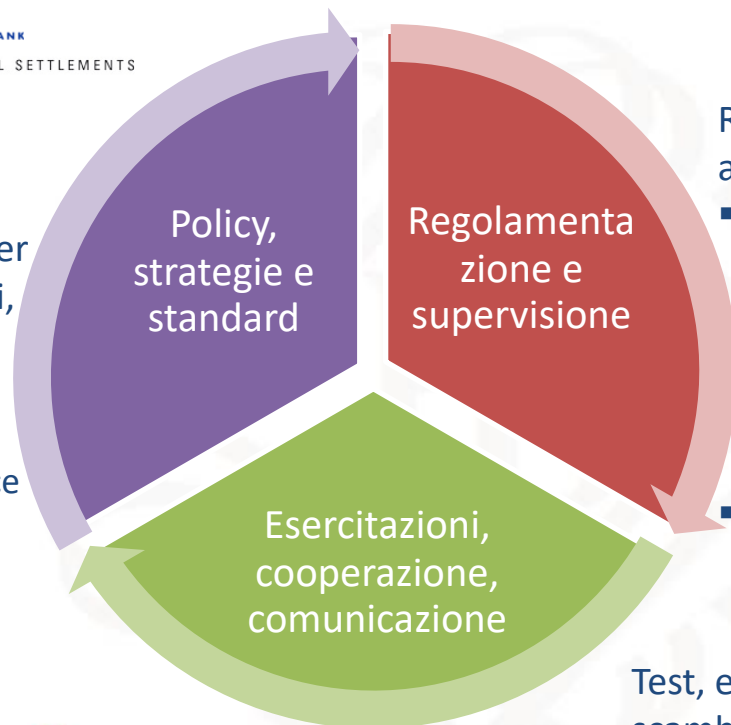


BANK FOR INTERNATIONAL SETTLEMENTS



Indirizzi e standard internazionali di alto livello per autorità e operatori finanziari, per es:

- G7 Fundamental Elements
- Eurosystem Cyber Resilience Strategy



Regole armonizzate ad hoc, con *scope* più ampio:

- DORA, NIS-D, CER, CRA, AI-Act. *Fil rouge*:
 - ICT risk management
 - ICT incident reporting
 - Rischio di terze parti
 - Testing (TLPT)
 - Info sharing
- Vigilanza e Sorveglianza sui sistemi di pagamento

Test, esercitazioni, cooperazione per scambio informativo e analisi, campagne comunicazione



Nuove tecnologie: Artificial Intelligence, Quantum Computing

	Opportunità	Rischi
QC	<ul style="list-style-type: none">▪ gestione del rischi▪ calcolo del merito di credito▪ allocazione di capitale▪ trading algoritmico	<ul style="list-style-type: none">▪ Crittografia e cybersicurezza▪ Asimmetrie tecnologiche▪ Concentrazione dei providers → dipendenza▪ Rischi indiretti ('importati')▪ Competenze
AI	<ul style="list-style-type: none">▪ Raccolta e trattamento di grandi volumi di dati granulari in tempo reale:<ul style="list-style-type: none">➢ outliers detection➢ forte capacità predittiva (profilazione del cliente, personalizzazione dei servizi, prevenzione delle frodi, AML, asset inventory, ...)▪ Cybersecurity:<ul style="list-style-type: none">➢ miglioramento delle capacità di prevenzione preparazione e risposta	<ul style="list-style-type: none">▪ Privacy, cybersicurezza, proprietà intellettuale▪ Aumento del digital divide▪ Disinformazione▪ Interpretabilità, 'allucinazioni'▪ Stabilità finanziaria → effetti del trading algoritmico▪ Competenze▪ Concentrazione dei providers → dipendenza

Quantum Computing

- Comprensione del fenomeno
- Sviluppo delle competenze
- Sviluppo di policy, linee guida e standard armonizzati
 - promozione roadmap di migrazione globale per la resilienza quantistica del sistema finanziario

Artificial Intelligence

- Sviluppo delle competenze
- Sviluppo di policy, linee guida e strumenti armonizzati per:
 - data governance
 - corporate governance



Temi prioritari per la Presidenza italiana del G7