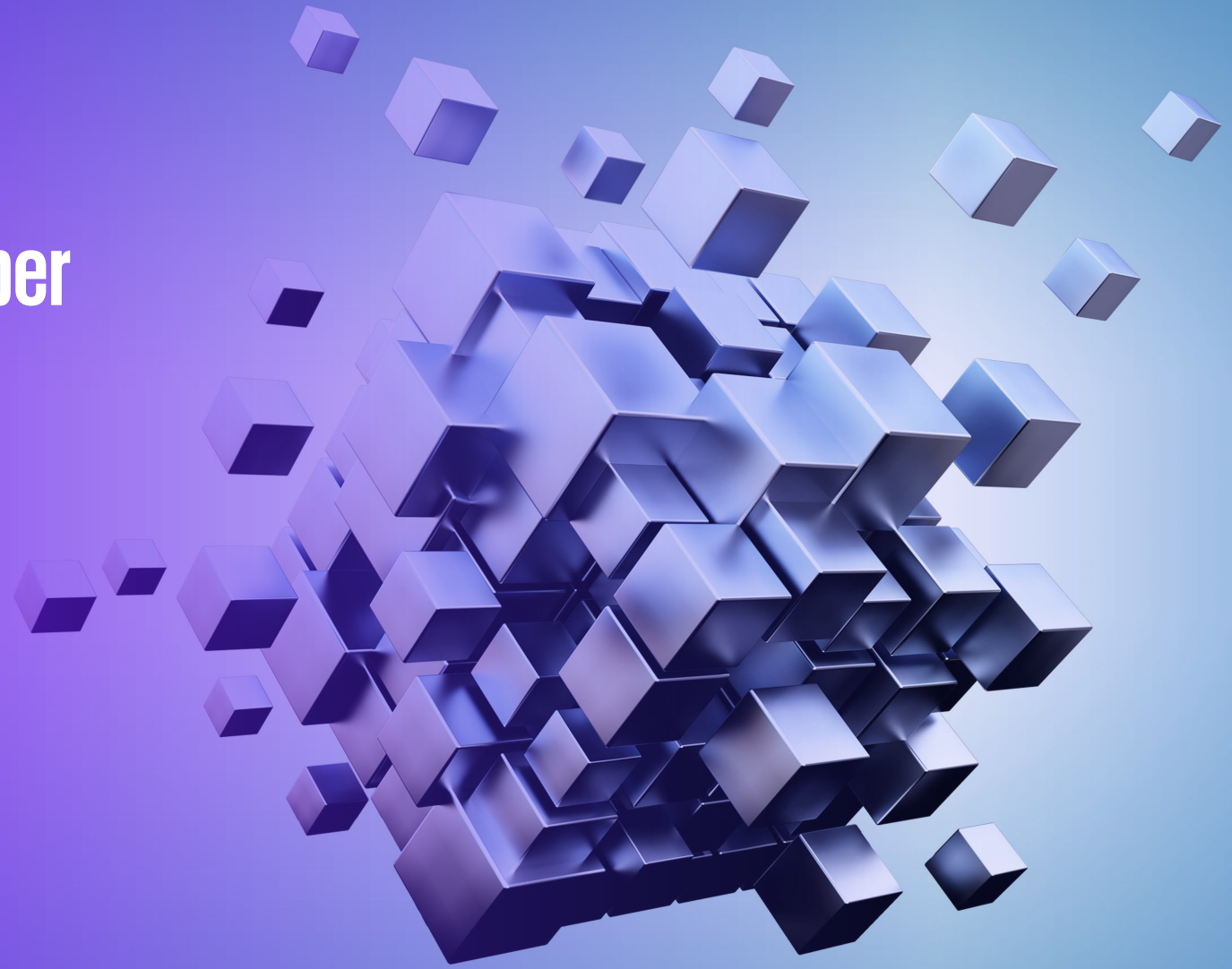
Sviluppare strategie innovative per fronteggiare le minacce cyber: il valore della resilienza e delle collaborazione e il ruolo dell'intelligenza artificiale



Banche e Sicurezza 2025 | Milano, 27 maggio

Luca Boselli, Partner KPMG, Head of Cyber & Tech Risk

01

I rischi della Cyber Security e lo scenario geopolitico

Top Geopolitical Risks 2025 – Le dimensioni della frammentazione

01
Trasformazioni radicali negli equilibri di potere, ricchezza e commercio

02
Contesto normativo e fiscale complesso e frammentato

03
Panorama tecnologico in rapida evoluzione e fortemente politicizzato

04
Molteplici minacce alla Supply Chain

05
Pressioni demografiche, tecnologiche e culturali sul capitale umano

La sfida è allineare la gestione del rischio con gli obiettivi strategici

Fonte: KPMG 'Top Geopolitical Risks 2025'

Top Geopolitical Risks 2025 – Impatti lungo i settori

	Trasformazioni radicali negli equilibri di potere, ricchezza e commercio	Contesto normativo e fiscale complesso e frammentato	Panorama tecnologico in rapida evoluzione e fortemente politicizzato	Molteplici minacce alla Supply Chain	Pressioni demografiche, tecnologiche e culturali sul capitale umano
Consumer & Retail					
Energy, Natural Resources & Chemicals					
Financial Services					
Industrial Manufacturing & Automotive					
Infrastructure & Transport					
Life Sciences					
Technology, Media & Telecom					

I rischi geopolitici impattano le nostre filiere strategiche

Fonte: KPMG 'Top Geopolitical Risks 2025'

Impatto Limitato | Impatto Moderato | Impatto Alto

I rischi della Cyber Security nello scenario geopolitico

Implicazioni ed impatti

- **State-sponsored attacks**: minacce persistenti avanzate (APT) che mirano al furto di proprietà intellettuale e al sabotaggio delle linee di produzione
- **Catena di fornitura digitale frammentata**: dipendenze da fornitori colpiti da tariffe, sanzioni o leggi sulla sovranità digitale possono creare delle 'falle' nei sistemi di sicurezza
- **Impatto operativo ed economico**: interruzioni della produzione con conseguente riduzione dei ricavi, danni reputazionali e penalità contrattuali dipendenti dalla lunghezza del fermo produttivo e dalla gravità delle violazioni
- **Minaccia alle infrastrutture critiche**: reti elettriche, idriche, di trasporto, finanziarie e di telecomunicazioni sono sempre più bersaglio di attacchi Cyber come arma geopolitica
- **Pressione normativa e di governance**: regolamenti frammentati (NIS2, GDPR, controlli sulle esportazioni) e crescenti richieste da parte dei consigli di amministrazione e dei regolatori richiedono l'aggiornamento 'real time' delle metriche di sicurezza.

Geopolitical cyber-risk trends

- State competition over sensitive technologies (AI, semiconductors)
- Tariffs and export controls
- Attacks on critical infrastructures
- Commoditization of cyber-attack tools
- Sanctions and financial transaction controls
- AI automation (attack & defence)
- Cyber-war evolution
- Digital sovereignty initiatives
- Digital espionage

Priorità e sfide della Cyber Security nel settore finanziario

In un contesto di **conflitti ibridi** e crescente **instabilità geopolitica**, le banche sono obiettivi primari per attacchi informatici avanzati. Le dinamiche globali rendono la **cybersicurezza bancaria una priorità strategica** e un pilastro della resilienza nazionale. Anticipare l'impatto dei **rischi geopolitici** consente di rafforzare tempestivamente le difese, valutare l'esposizione ai fornitori in aree ad alto rischio e potenziare l'intelligence informatica e la cooperazione interistituzionale.

Geopolitical Threat Intelligence

Per contrastare le crescenti minacce informatiche provenienti da attori sponsorizzati dagli Stati, in particolare quelli che utilizzano tattiche avanzate come gli APT e gli exploit zero-day, le banche stanno potenziando le loro strategie di cybersicurezza attraverso:

- **lo sviluppo dell'intelligence sulle minacce geopolitiche**
- **il rafforzamento della collaborazione con le autorità nazionali**

Geopolitical Cyber Risk in the Supply Chain (Due Diligence)

Considerata l'instabilità politica globale, le organizzazioni stanno adottando misure proattive di intelligence sulle minacce geopolitiche, come ad esempio:

- **due diligence sui fornitori;**
- **revisione dei contratti con clausole di uscita;**
- **diversificazione delle dipendenze tecnologiche.**

Affidarsi a fornitori provenienti da stati geopoliticamente sensibili (es. Cina o Russia) può aumentare l'esposizione a rischi come sanzioni o interruzioni dei servizi.

Cyber Warfare ready & Multi-Stakeholder War Game Simulation

Per rafforzare la resilienza contro la guerra cibernetica e le minacce sistemiche rivolte al settore finanziario, le banche stanno adottando:

- **strategie di continuità operativa e gestione delle crisi** che integrano la risposta agli incidenti con la comunicazione strategica;
- **simulazioni di guerra cibernetica multi-attore** — che coinvolgono autorità nazionali e media — per prepararsi ad attacchi DDoS, ransomware e campagne di defacement progettate per destabilizzare il sistema bancario.

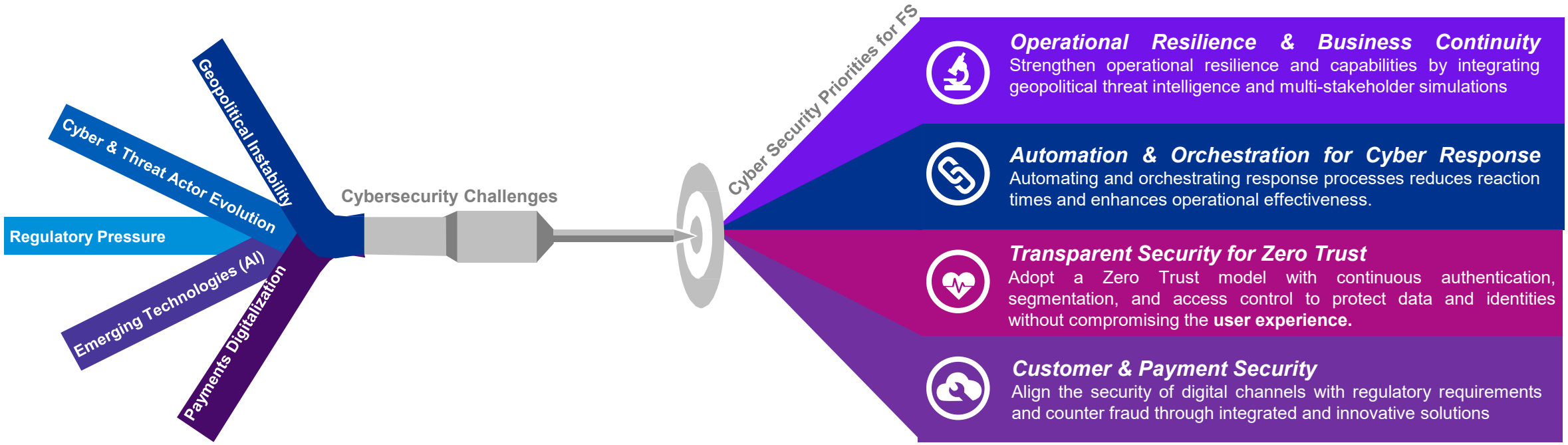
.

02

Priorità e sfide per la gestione della compliance

Cyber Security Trend & Priorities in Financial Sector

Geopolitical Instability	Cyber & Threat Actor Evolution	Regulatory Pressure	Emerging Technologies (AI)	Payments Digitalization
International tensions, **hybrid conflicts**, and sanctions increase banks' exposure to systemic risks and state-sponsored attacks	The rise in **DDoS attacks, ransomware, targeted phishing**, and banking trojans demands a timely and coordinated response.	The **EBA and DORA reports** highlight the centrality of ICT risk, incident reporting, and **third-party management**	**Technical innovation** (including growing usage of artificial intelligence (**AI**)) may have contributed to a continuously **growing risk of fraud** but at the same time it can provide a **booster to cybersecurity measures.**	The expansion of **digital channels**, new customer and third party **on-boarding experience**, the introduction of regulations such as **PSD3/PSR** require advanced protection.



Operational Resilience & Business Continuity
Strengthen operational resilience and capabilities by integrating geopolitical threat intelligence and multi-stakeholder simulations

Automation & Orchestration for Cyber Response
Automating and orchestrating response processes reduces reaction times and enhances operational effectiveness.

Transparent Security for Zero Trust
Adopt a Zero Trust model with continuous authentication, segmentation, and access control to protect data and identities without compromising the **user experience.**

Customer & Payment Security
Align the security of digital channels with regulatory requirements and counter fraud through integrated and innovative solutions

Cyber Security Trend & Priorities in Financial Sector

Operational Resilience & Business Continuity

The adoption of more dynamic and proactive strategies and the strengthening of response and **recovery capabilities**, also through the vulnerability analysis and prioritization, scheduling of advanced tests, as well as a greater engineering of an actionable **Threat Intelligence**, mainly regarding **supply chain risks.**

Automation & Orchestration for Cyber Response

Automation in cybersecurity allows the use of technologies to automatically perform repetitive and low-level tasks, reducing the manual workload for operational teams.
Meanwhile, **Orchestration** ensures the coordination and integration of various security tools and processes to create coherent and optimized workflows.
This results in a **reduced response time for detecting and managing cyber attacks** and **greater efficiency in operational activities.**

Transparent Security for Zero Trust

Transparent Security integrates with the Zero Trust model, ensuring minimal operational impact through continuous authentication, monitoring, segmentation, and access control measures without compromising the **user experience.**

Customer & Payment Security

The security of **digital onboarding processes**, web-exposed interfaces, and the integration between channels (Internet and Mobile) must be aligned with corporate strategies.

The Payment Services Directive 3 (**PSD3**) and the Payment Service Regulation (**PSR**) constitute the European Commission's response to enhance the security and protection of Payment Service User (PSU) against **fraud.**

Cyber Resilience Through Innovation: Cyber Agentic AI for the purpose of Automated Threat/Fraud Detection & Response

The power of the People: evolution of organizational models and strengthening of the workforce in terms of both capacity and upskilling

DORA Topics

Main DORA Topics with Partial Coverage

1 Incident Management

DORA requires to classify ICT-related incidents and cyber threats based on criteria such as the number of affected clients, transaction impact, incident duration, and data losses. However, challenges persist, including improper classification, **immature incident processes** not **aligned with threat intelligence**, and **insufficient communication strategies and governance.**

2 DORA testing

Overall testing and TLPT required by DORA are not entirely mastered. This includes developing an overarching testing concept based on **application-specific threats**, ensuring annual **testing of critical ICT assets**, and establishing a **concept for conducting and documenting TLPT.**

3 TPRM

Third Party Risk Management presents significant **challenges for** financial services companies during **implementation**. To make the best use of this data for risk management and to **reduce ongoing management efforts**, companies should evaluate whether **tool-based solutions** can help streamline their future upkeep processes.

Source: KPMG EMA Benchmarking

Cybersecurity considerations for 2025

01

The ever-evolving role of the CISO

CISOs and their teams are increasingly integrating cybersecurity into the broader organization, leading to more fluid interactions and a better understanding of security functions across all levels.

02

The power of the people

Organizations are transforming their business models due to digital disruptions, facing challenges with workload that worsen the cyber skills gap. While AI and automation offer solutions, there is a risk of talent attrition as teams struggle to adapt.

03

Embed trust as AI proliferates

AI is here to stay and has a place in virtually every organizational function, but there are a number of key cyber and privacy challenges that have the potential to effect the adoption and deployment of AI.

04

Harness AI for Cyber: Racing ahead vs. racing safe

The hype around AI adoption is driven by factors like inadequate training and fear of falling behind, with the main challenge being to balance the benefits of AI integration in cyber and privacy functions against the associated risks.

05

Platform consolidation: Embrace the potential but recognize the risks

Many global organizations are seeking to simplify and reduce technology costs by consolidating tools onto fewer platforms, which requires careful navigation of associated risks.

06

The digital identity imperative

Global initiatives for digital identity face ongoing challenges in interoperability and authentication due to deepfakes, shaped by regulations, risk appetite, and public opinion on data processing.

07

Smart security for smart ecosystems

The global rise of smart devices is reshaping security perspectives, leading regulators to implement new standards to ensure basic security compliance.

08

Resilience by design: Cybersecurity for businesses and society

Organizations must foster a robust culture of resilient security from the CISO down to ensure alignment among all stakeholders.

Source: KPMG Cybersecurity considerations for 2025

Cybersecurity: The #1 threat to business over the last decade

At a time when technology is intertwined with every facet of our professional and personal lives, cybersecurity emerges not just as a business concern but as a broad issue that impacts all aspects of society. According to KPMG 2024 CEO Outlook report, CEOs view cybersecurity as the top threat over the last decade.

The same KPMG research shows that **64 percent of global CEOs are committing to AI investments regardless of economic conditions.** However, a significant **majority (78%) is worried about AI's 'black box' nature,** the lack of transparency and potential operational challenges and ethical dilemmas.

Recognizing these risks, **70% of CEOs are increasing their cybersecurity investments to protect their operations and intellectual property from AI-related threats.** Bottom line, CISOs must prioritize AI-specific safeguards to ensure responsible AI development and deployment, mitigating risks and fostering trust in this transformative technology.

Learn more

KPMG Global Tech Report 2024

Lack of common data practices

Although many organizations are investing in data accessibility,

only

24% prioritize a data-centric culture and ensuring data interoperability.

Is AI delivering on its promise?

While nearly 3/4 of organizations are realizing business value from their AI investments,

only

1-in-3 has been able to achieve these gains at scale.

FOMO surrounding AI in cybersecurity

The hype surrounding AI in cybersecurity has led to a growing sense of fear of missing out (FOMO) among organizations, particularly at the senior management and board levels.

82% are investing tech investments such as virtual and augmented reality, which are enabled by AI, in order to keep pace with their competitors.

kpmg.com/socialmedia