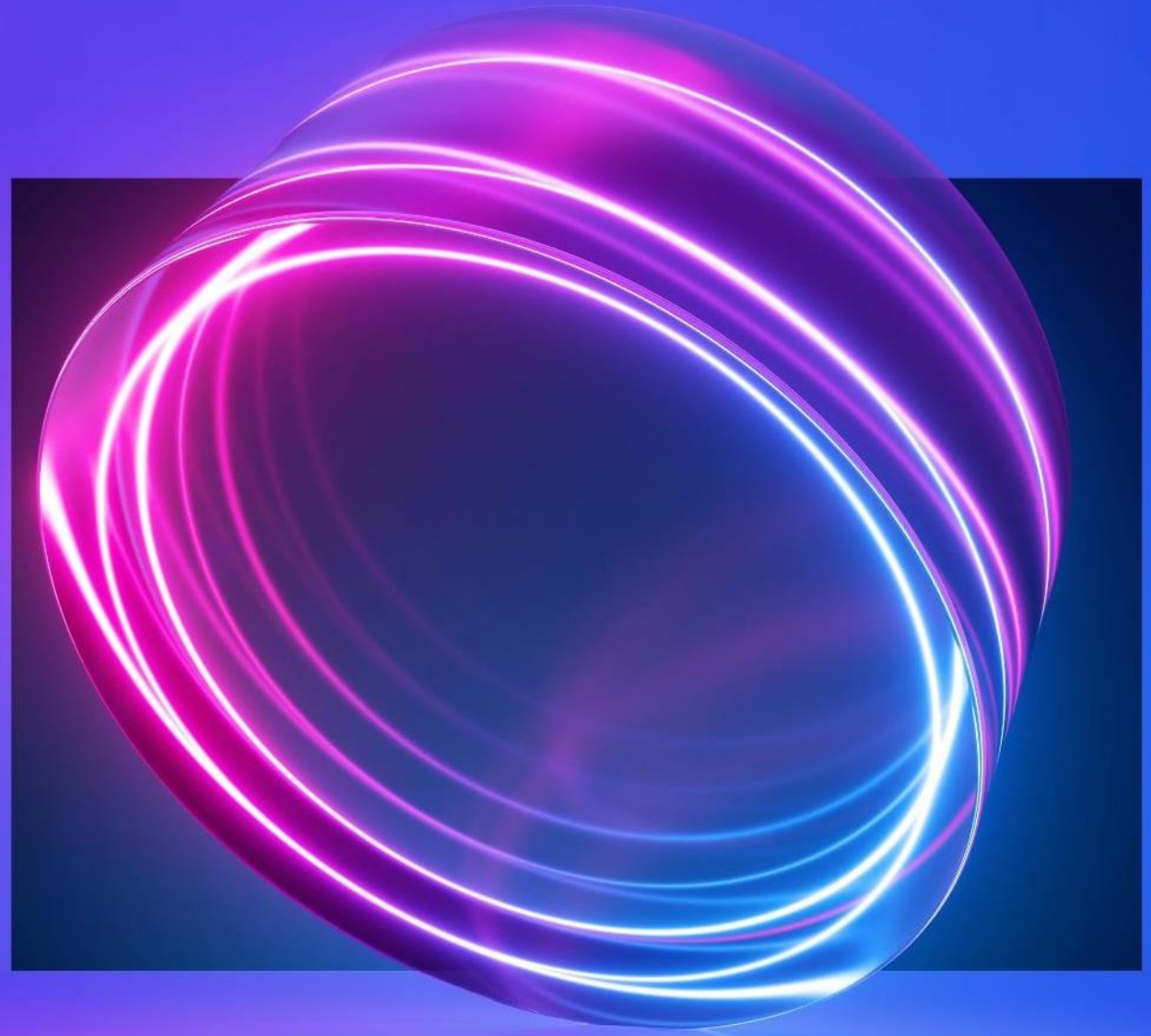
Le minacce informatiche come rischio sistemico per il sistema finanziario europeo

L’importanza di strategie comuni per riconoscerle e fronteggiarle e il ruolo dell’intelligenza artificiale

Banche e Sicurezza 2024 | Milano, 14 maggio



Luca Boselli

Partner, KPMG

Head of Cyber Security Services

01

AI Governance & Security

Trusted AI is critical

We understand trustworthy and ethical AI is a complex business, regulatory, and technical challenge, and we are committed to helping clients put it into practice. We help develop, and deploy end-to-end Trusted AI programs across the AI/ML lifecycle

Fairness
Ensure models reduce or eliminate bias against individuals, communities or groups

Transparency
Include responsible disclosure to provide stakeholders a clear understanding as to what is happening within the AI solution and across the AI lifecycle

Explainability
Ensure AI solutions are understandable as to how and why recommendations are made or conclusions drawn

Accountability
Human oversight and responsibility embedded across the AI lifecycle to manage risk and ensure compliance with regulations and applicable laws

Security
Safeguard against unauthorized access, bad actors, misinformation, corruption, or attacks

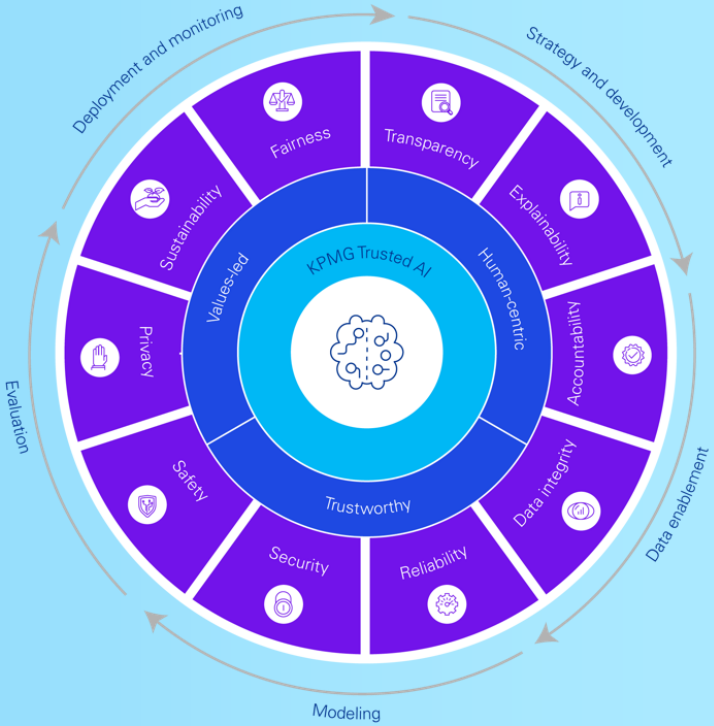
Privacy
Ensure compliance with data privacy regulations and consumer data usage

Sustainability
Optimize AI solutions to limit negative environmental impact where possible

Data integrity
Ensure data quality, governance, and enrichment steps embed trust

Reliability
Ensure AI systems perform at the desired level of precision and consistency

Safety
Safeguard AI solutions against harm to humans and/or property



Why is AI so important for the future of cyber security?

Challenges of faced by security teams

Organizations struggle to detect, analyze, and respond to the evolving cyber threat landscape

As cyber threats become increasingly sophisticated and pervasive, existing tools struggle to effectively detect and defend against adversaries. Manual processes further limit the efficiency and scalability of cyber operations while introducing the potential for human error.

Lack of visibility

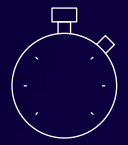
Blind spots resulting from the extreme changing velocity of the threat landscape and limitations in detection make it necessary to capture and respond to a broader array of threat intelligence

Poor fidelity

Manual investigation may not encompass the full scope of an evolving threat landscape, whereas machine learning can observe new patterns and account for historical context in real-time

Insufficient contextualization

Alerts are the product of often complex correlation logic, layering of rules within rules, and enrichment of high-velocity IOCs, which are impractical for a human to account for at scale



Sluggish response time

Analysts face the challenge of investigating an overwhelming volume of alerts, some of which may be inaccurately prioritized and be false positives

Ecosystem of AI for Cyber is broadening

AI is not a net new technology for securing business infrastructure. It's a new way of working with data. Businesses should carefully prioritize where AI is best applied, and understand the pros and cons. There are some core areas where it is more applicable and already being used either by security teams or their supply chain

Analysts consider some of the top trends and innovations in leveraging AI for cybersecurity

AI engineering

discipline that applies engineering best practices to AI development, deployment and operation

AI-augmented security operations

combination of human and machine intelligence that enhances the efficiency and effectiveness of security operations centers

AI security

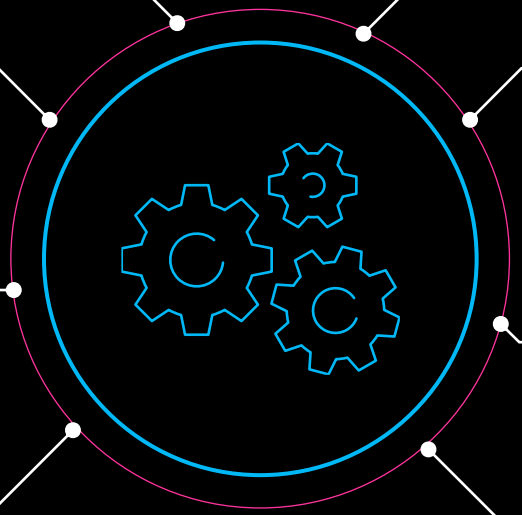
set of capabilities that protect AI systems from malicious attacks and ensure the ethical and trustworthy use of AI

AI-enabled threat detection and response

use of AI techniques to improve the detection and response to cyber threats across various domains, such as network, endpoint, cloud and identity

Applying AI/ML to Privacy and Security

When properly designed and deployed, AI is very powerful in anomaly/hidden outliers detection, pattern recognition and nonlinear system analysis. AI/ML can be applied to enhance both privacy & security of businesses, use cases include:



Data Classification & Labeling

- Semantic data classifier and artificial neural network performing automated tagging of tabular data using supervised learning for label allocation

Identity Matching

- Probabilistic & deterministic matching model, computes user identity based on similarity of PII or exact match in existing records

Age Gating

- Facial age progression, document verification based age prediction model & geo-blocking based on jurisdictional age of majority

Access Restriction

- Abnormal behaviour identification using anomaly detection, classifier models and pattern recognition using computer-vision

Incident Detection & Response

- Anomalous operations detection, automated pattern evaluation for activity classification and prioritized response action automation, rapid recovery

Threat Mitigation and business continuity

- UEBA, erratic or irregular behavioural analytics for insider threat modeling, response and prioritized response action, as well as third party security

Access Controls

- AI authentication fusing biometric traits with soft attributes and authorization based on behavioural pattern analysis

Analysis Augmentation

- Real time systems monitoring leveraging automated security risk triage, data enrichment & pattern recognition, virtual cyber security assistants

02

Cybersecurity considerations

Cybersecurity: From inhibitor to transformation enabler

Organizations are prioritizing security in response to privacy and trust concerns in digital transformation.

Commercial imperative

Organizations that perform strongly on security will drive competitive advantage.

63%

expect improved cybersecurity and privacy will boast loyalty.

That's why

51%

of cybersecurity teams are focusing on how to automate, streamline and embed security into the core of the business.

Cyber and privacy

Concerns were ranked as primary factors that could slow down transformation progress.

71%

say they must be more proactive at integrating trust, security, privacy and resilience into technology rollouts.

40%

say that enhanced security has become a key goal in their XaaS projects.

Winning outcomes with security by design

Those taking action will see increased success in their transformation programs

62%

manage risk in the early stages of projects with security and control by design to increase the success rates of transformation programs.

In some countries it's far higher:

88% India, **83%** China

74% Brazil

Source: KPMG global tech report 2023.

Eight key cybersecurity considerations for 2024

01

Meet customer expectations, improve trust

With cyber threats and data privacy concerns growing, CISOs should work closely with stakeholders across the organization to maintain trust by ensuring operations are resilient in the event of an incident.

02

Embed cyber and privacy, for good

The act of embedding security across the organization should be viewed as an exercise in driving operational excellence.

03

Navigate blurring global boundaries

A central consideration that organizations should examine is how to most effectively navigate the increasingly complex global business landscape to ensure resilience and business continuity.

04

Modernize supply chain security

Despite the challenges and competing priorities, ensuring the supplier and partner ecosystem is secure should not be a bottleneck; it should be a business enabler.

05

Unlock the potential of AI – carefully

Security and privacy leaders should be supporting the business objectives reliant on AI and determine how to harness this game-changing technology effectively and responsibly.

06

Supercharge security with automation

As operating models digitize, security teams should automate and upgrade their processes to keep pace.

07

Make identity individual, not institutional

Driven by expanding business models, it's vital that organizations now view identity not in isolation but from a broad perspective.

08

Align cybersecurity with organizational resilience

Organizations should be seeking to find a way to create a culture of resilient security throughout the enterprise and ensure all stakeholders are on the same page.

Meet customer expectations, improve trust

Consumers, employees, suppliers — every corporate stakeholder — expect businesses to pursue growth and profits. But increasingly, organizations are expected to operate socially responsibly, as well. Organizations should heed this call and strengthen the connection between security and privacy and environmental, social and governance (ESG) factors. This bond is increasingly recognized across the business ecosystem, particularly by ESG rating services, as they search for greater transparency in measuring and comparing organizations.

Key actions clients should consider for 2024

- Connect with your organization's ESG team to determine whether they consider cyber a key aspect of their mandate. If not, work to build awareness of how and why it's important to all three areas of ESG.
- Be practical. Effective cybersecurity is not as much about getting business partners to do things differently as it is about reframing the conversation across the enterprise to inspire other areas of the organization to infuse security into what they already do.
- Sharpen your global regulatory intelligence around cyber in general and ESG and privacy in particular with the aim of ensuring timely compliance and reporting; keep track of and remain familiar with ever-increasing regulations and their effects on your cyber efforts.

"Increasing trust should be high on the cyber agenda in relation to how video and audio files are used in the creation of deepfakes, the impact of which can be grave for privacy and perhaps even democracy.

Mika Laaksonen
Partner, Global Cyber Security
ESG Leader
KPMG in Finland

Cyber considerations

01 02 03 04 05 06 07 08

Embed cybersecurity and privacy, for good

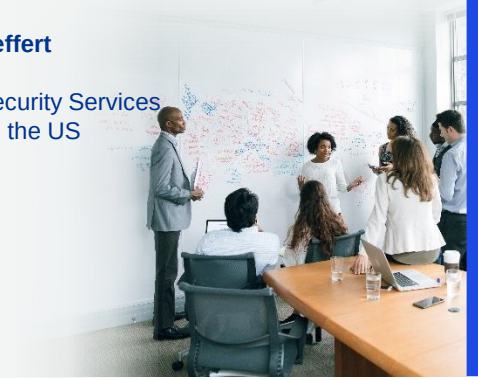
Security, from the CISO down through their entire team, is a very different role today. Cyber is becoming more embedded in core business processes. That reality is being reflected in a move away from a centralization of cybersecurity in the CISO role to a federated model, in which the CISO is the conductor of the orchestra, establishing the frameworks, assessing risk, and providing implementation support. Security is integral to every function across the organization, from front office to back, and many leaders now acknowledge the value of integrating a security mindset into their very different business cultures and processes.

Key actions clients should consider for 2024

- Bring a new perspective to the board on what could disrupt the business and what should be done to manage those risks without impacting operations and customer experience.
- Security teams should determine how and where to embed certain security tasks within the business vs. outsourced to a third-party service provider and monitor those tasks to ensure they are carried out properly.
- Run the cyber team like a business, which means you must give up a degree of control over what other parts of the organization are doing from a security perspective.

Ten or 15 years ago, the 80/20 rule for security professionals was 80 percent technical skills and 20 percent soft skills. If CISOs want to ensure they are not perceived as support staff, they must get comfortable with the new 80/20 rule under which imperatives such as communication, building trust, problem-solving and conflict management are as vital as ensuring an efficient security operations center.

Brian Geffert
Principle
Cyber Security Services
KPMG in the US



Cyber considerations

01 **02** 03 04 05 06 07 08

Supercharge security with automation

Businesses are increasingly moving systems to the cloud, the volume of data that needs protection is skyrocketing, and more people are working remotely and accessing corporate networks with their own devices. As a result, the cyberattack surface is expanding, creating more alerts, false positives and triage events for CISOs to manage. There's a lot of noise in security operation centers (SOCs), and there aren't enough panes of glass or humans to deal with the volume. How can CISOs keep detecting threat after threat and feel they're not missing something? They need to collect, correlate and escalate the signals that require a response — and it must be done rapidly. The only way to do that is through automation.

Key actions clients should consider for 2024

- Define your initial vision and strategy for automation. Consider your short- and long-term security objectives, ensure how those goals align with the organization's business priorities, and determine the type of protections those shared objectives require.
- Identify what data the organization has centrally accessible and define an automated continuous controls monitoring plan to drive efficiencies across all three lines of defense.
- Determine what tools to build versus acquire and understand how supply chain partners are automating to strengthen trust between the organizations and leverage that learning where appropriate.

"There is huge proliferation of security vulnerabilities from multiple scanner sources. It is imperative to co-relate and identify issues that are real threats. This enables CISOs and governance teams to get a risk view of the organization and sheds light on where we need more human resources with specialized skills. Automation affords security teams the luxury of knowing what to prioritize."

Pratiksha Doshi
Partner
Cyber Security Services
KPMG in India

Cyber considerations

01 02 03 04 05 **06** 07 08

Make identity individual, not institutional

Every organization with which consumers interact assigns them a unique digital identity, and just as usernames and passwords vary, authentication methods do as well. From a cybersecurity perspective, the identity model is evolving. Most identity and access management (IAM) models were originally devised to manage digital identities and user access for single organizations. Many are now being reconceptualized to encompass a level of resilience suitable for federated, private, public or multi-cloud computing environments. This will eliminate the need for individuals to ensure the exhaustive, time-consuming and intrusive process of identity-proofing every time they interact with a new institution, either as a customer or employee.

Key actions clients should consider for 2024

- Keep your approach to identity flexible to comply with the evolving regulatory environment and ensure your architecture can integrate emerging technologies into the security process much faster than the two-, three- or four-year journeys we see today.
- Explore more agile and interoperable identity systems to facilitate a federated identity ecosystem.
- Consider your role, now and in the future, as an identity/credential issuer, relying party, digital wallet provider or all three in this evolving identity ecosystem.

“As assurance levels associated with those identities increase, we are beginning to see a trend toward a federated identity model — fewer distinct digital IDs that can be securely leveraged across different domains.”

Marko Vogel
Partner
Cyber Security Services
KPMG in Germany

Cyber considerations

01 02 03 04 05 06 07 08

kpmg.com/socialmedia