



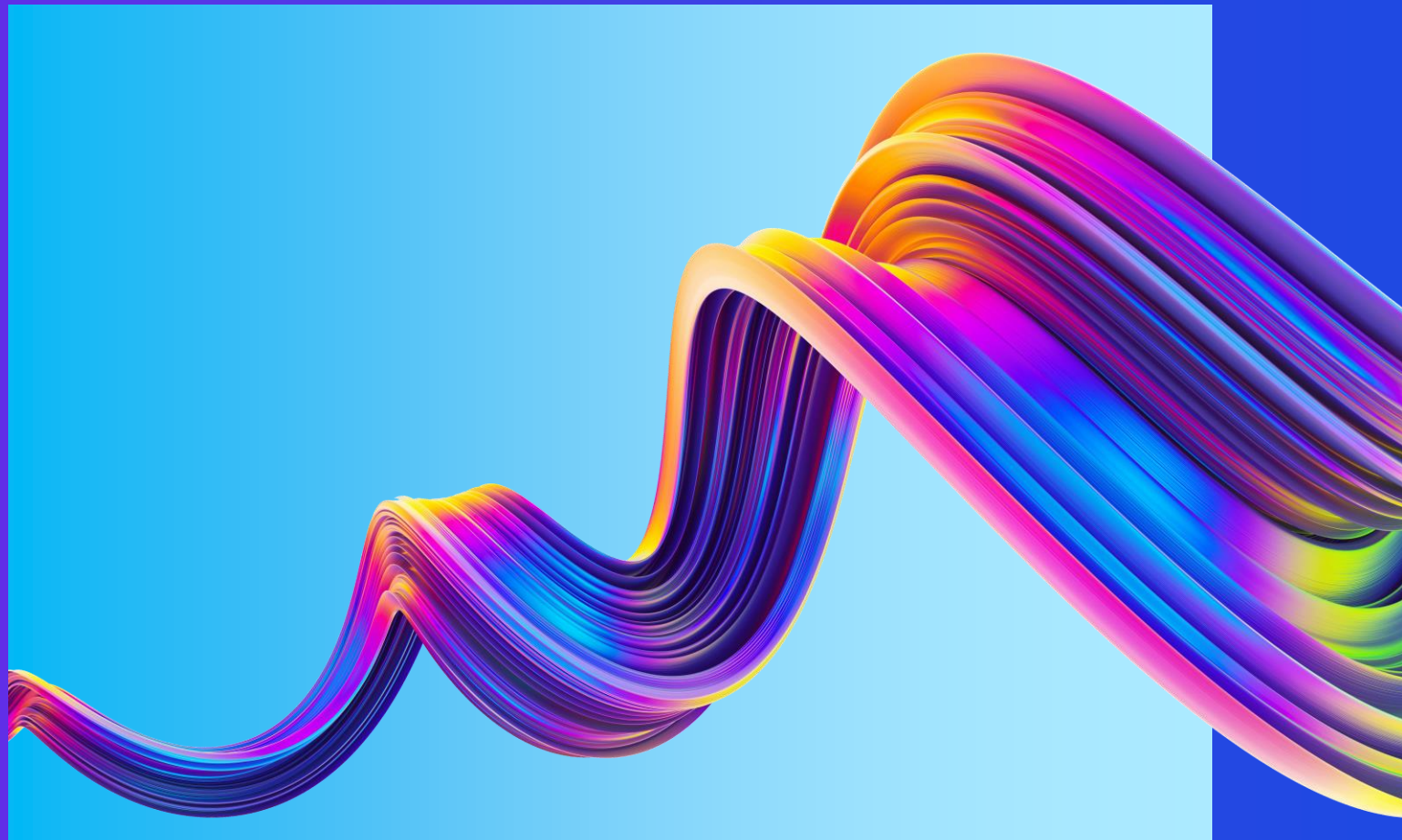
Banche e Sicurezza 2023

Evoluzione degli attacchi e
investimenti per la sicurezza del
settore finanziario e dei cittadini

Luca Boselli

Partner, KPMG

Head of Cyber Security Services



01

Nuove minacce e sistemi di regole





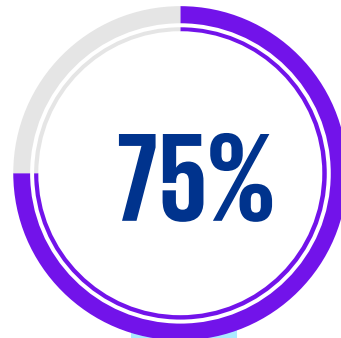
AI is being

embedded into every business process but...

Nobody knows



whether their AI is secure.

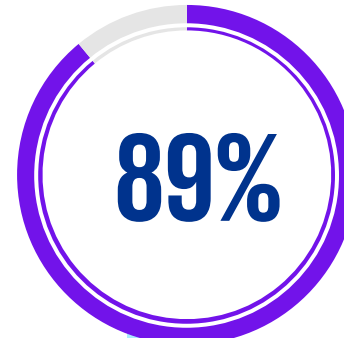


75%



of companies that will shift from piloting to operationalizing AI by 2024

Source: Gartner Top 10 trends in data and analytics for 2020

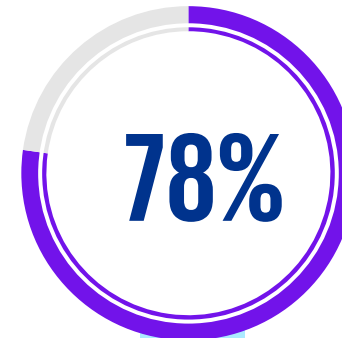


89%



of surveyed companies don't have tools in place to secure their ML systems

Source: VentureBeat, The Future of AI Deployments Reaching Production is Bright in 2021



78%

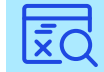


agree that AI and ML bring unique cybersecurity challenges.

Source: KPMG Cyber trust insights 2022



3 in 4



say AI and ML raise fundamental ethics questions.

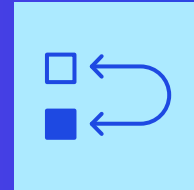
Adversarial AI are cyber threats specific to AI and Machine learning models

There are no mature approaches to assess, secure, or respond to these threats today

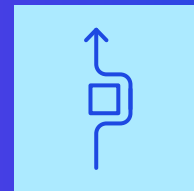
Poisoning Attack



Inference Attack



Model Evasion



Data extraction



The regulators are coming!

Nations, industries, and regulators worldwide are starting to take action around the implementation of responsible and trustworthy AI, not least the G20, which set out its AI Principles, which include freedom, dignity and autonomy, privacy and data protection, non-discrimination and equality, diversity, fairness, social justice, and internationally recognized labor rights.



The EU is paving the way with its EU AI Act, which will require organizations to:



Determine the level of risk embedded in their AI Systems



Conduct conformity assessments on high-risk AI systems



Implement post-market monitoring systems on high-risk AI systems

Non-compliance brings major penalties:

Up to €30M Euros (\$30.3m USD) or 6% of total worldwide turnover, whichever is higher

Other regulations, frameworks and standards include (non-exhaustive list):			
Name	Region/Country	Type	Link
Australia's AI Ethics Principles	Australia	Published Framework	AI Ethics Principles
Draft AI Law and AI Bill No. 21/20	Brazil	Proposed Law	AI Bill N 21/202 Draft AI Law
Canada Bill C-27, Artificial Intelligence and Data Act, 2022	Canada	Proposed Law	Bill C-27
China - Internet Information Service Algorithmic Recommendation Management Provisions	China	Published Framework	China AI
EU AI Act	European Union	Proposed Law	The Act The Artificial Intelligence Act
Singapore A.I. Verify Framework	Singapore	Published Framework	A.I. Verify
UAE - Ethical AI Toolkit	UAE	Published Guidelines	AI Ethics Principles & Guidelines
National AI Initiative Act	US	Passed Law	National AI Initiative Act
US - NIST – AI Risk Management Framework	US	Published Framework	AI Risk Mgt. Framework
Blueprint for an AI Bill of Rights	US	Proposed Bill	US AI Bill of Rights

Quantum Computing Adoption

Quantum computing adoption has increased rapidly over the last 5 years, with organizations looking at various use cases and capabilities in the space. The key highlights of the quantum computing revolution are highlighted below –



Quantum adoption grows

29%

of enterprises are already on the journey towards quantum adoption, with another 40% planning to adopt quantum computing



Top Quantum Use Cases

71%

State machine learning and data analytics problems are the top use cases for early adopters of quantum computing, particularly in the US where enterprises are further along in their quantum adoption.



Building Quantum Capability

61%

The Most Advanced Quantum Adopters Take the Lead by Developing Quantum Workforce, Working with Outside Vendors and Building Applications



Complexity of IT Integration

49%

State that the complexity of integrating quantum computing with existing IT infrastructure was the most cited hurdle to quantum adoption



Security Concerns as a Barrier to Adoption

49%

All the security concerns that come with cloud-based enterprise IT solutions apply to quantum computing as well, and in fact are magnified by quantum.



Lack of Advanced Capabilities to Build On

35+%

Among early quantum adopters, those that are generally late to adopt new technologies are much more likely to cite a lack of advanced capabilities to build on as a barrier to quantum adoption.



Quantum Cloud Based Services

Majority of cloud service providers now provide quantum computing as a service such as Azure Quantum Services, AWS Braket, Google Quantum, IBM Q One and Condor



Increase in funding in quantum computing startups

30+

Over the past 6 years, total deals increased over 200% — from 7 in 2013 to 24 in 2018 and 30+ in 2021



Increase in R&D on Quantum Computing

85%

of the organizations working/planning to work with quantum expect to increase investments in the technology in the next year

Source: <https://zapata.wpenginepowered.com/wp-content/uploads/2022/04/Survey-Report--FINAL.pdf>

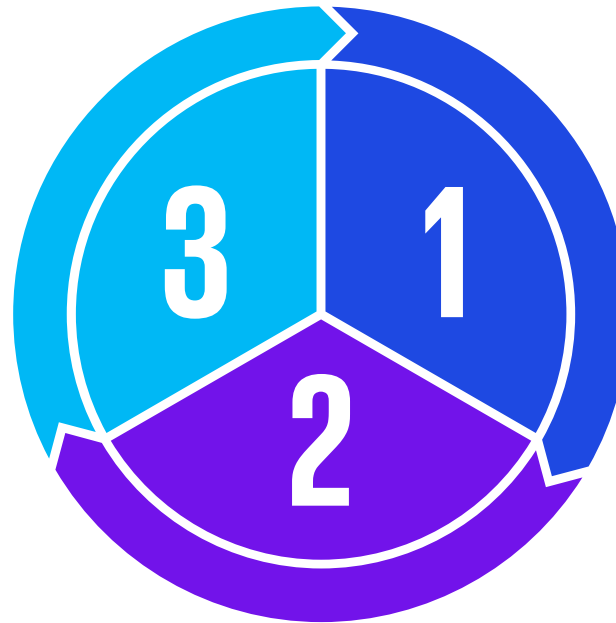
<https://known-production.s3.amazonaws.com/uploads/attachment/file/2891/What%20Is%2BQuantum%2BComputing.pdf>

The Quantum Threat: Y2Q (Year to Quantum)

With the rapid evolution of quantum computing, the quantum threat is the fact that most of the algorithms that were considered secure earlier are now vulnerable to be crypto analyzed

Store-Now-Decrypt-Later

- Use-case of an adversary collecting data encrypted today with cryptography that will be vulnerable upon Y2Q.
- This will enable the adversary to cryptanalyze the stored data to cause exposures and loss for any targets whose data remains valid (e.g., personal information, persistent credentials).



Parallel Computation

- A new paradigm of computation. New quantum algorithms like Shor and Grover algorithm; breaks up large brute forcing tasks into smaller tasks and then solves in parallel

Cryptography Affected

- Affects the current public key technology for signature and key exchange including the RSA algorithm used for signatures and encryption, the Elliptic Curve key exchange and signature algorithm, and the Diffie-Hellman key exchange algorithm.

Global Directions influencing Quantum Security



The following regulations were the ones identified as part of the global initiatives towards quantum security. Across regions, Americas, Europe and Asia have different initiatives towards quantum security.

Americas	EMA	ASPAC
<p>Quantum Computing Cybersecurity Preparedness Act</p> <ul style="list-style-type: none">• Applicable to all Federal Organizations• Establish an inventory of cryptographic systems• Annual reporting to Congress <hr/> <p>Quantum-Safe Canada</p> <ul style="list-style-type: none">• Quantum-Safe Canada will receive \$675,000 for their project Laying the Foundations for a Quantum-Safe Canada, which raises awareness and preparedness of the quantum threat. This funding is made available under the Cyber Security Cooperation Program.	<p>European Union Agency for Cybersecurity (ENISA) : Post-Quantum Cryptography: Current state and quantum mitigation</p> <p>Quantum Flagship was launched in 2018 as a research initiative of the European Union.</p> <hr/> <p>Quantum Security initiative, part of the World Economic Forum – a community of senior executives and experts.</p> <p>OPENQKD will raise awareness of the maturity of QKD and its seamless integration into existing security and networks for a wide range of use-cases.</p> <hr/> <p>UK National Quantum Strategy (Mar 23) – set out a ten year vision and plan for quantum in the UK, committing £2.5bn to research, innovation, skills and more.</p>	<p>In the recent 2023 Consumer Electronics Show (CES) in Las Vegas was a claim by Chinese scientists who say they've developed an algorithm that can decrypt 2048-bit RSA using a combination of classical and quantum computers with at least 372 qubits.</p> <hr/> <p>The Beijing-Shanghai Backbone Network (BSBN), the world's first long-distance quantum-secured communication route, was put into service on Aug. 30.</p> <hr/> <p>India set up its National Quantum Mission with 6000 cr INR investment to develop satellite-based secure quantum communications between ground stations over a range of 2000 km within India, long-distance secure quantum communications with other countries, inter-city quantum key distribution over 2000 km.</p>

02





L'evoluzione della spinta normativa



ECB Annual Report on supervisory activities 2022

“IT and cyber risk continued to be a key risk driver for the banking sector in 2022”

ECB Banking Supervision conducted a number of off-site and on-site supervisory activities around IT and cyber risk in 2022 with the following **takeaways**:

-  Banks still showed room for improvement in terms of **implementing basic cybersecurity measures**, with around half of the severe findings being identified during IT risk on-site inspections conducted in 2022 and concentrated in the area of IT security and cybersecurity risk.
-  After some years of a steady increase, the **reliance on end-of-life systems stabilised**, albeit at a very high level
-  **Data quality management** remained the least refined risk control area and some of the key controls were not yet fully implemented in several banks.
-  **The number of critical projects with an impact on the IT landscape increased very considerably**, pointing to the clear relevance of having appropriate management procedures in place for IT developments and IT projects.

Digital Operational Resilience Act (DORA)

Il Digital Operational Resilience Act (DORA) copre 6 aree di intervento principali:



DORA: focus su regolamentazione secondaria

A partire dal mese di **Gennaio 2024**, le **Autorità Europee di Vigilanza (AEV) – EBA, ESMA, EIOPA** – avvieranno l'**emissione normativa di standard tecnici di secondo livello (RTS, ITS, Guidelines)**, a cui gli enti e le organizzazioni dovranno adeguarsi entro il **2025**: tali Autorità si pongono a livello europeo come **Lead Overseers**, ovvero Autorità di Sorveglianza che mirano a garantire un **approccio della sorveglianza armonizzato**, tramite attività di investigation, emissione di raccomandazioni e richieste di informazioni sulle azioni intraprese dagli enti a seguito dell'emissione delle stesse.



ESMA

5 standard tecnici sull'ICT Risk

Management:

- RTS on **ICT RMF** (Risk Management Framework).
- RTS on simplified **ICT RMF**.
- RTS on **TLPT** (Threat-Led Penetration Testing).
- RTS on **ICT services policy**.
- RTS on sub-contracting elements.



EBA

6 standard tecnici sull'Incident

Reporting:

- RTS on IR **classification criteria**.
- RTS on reporting of **major IR**.
- ITS on incident reporting **details**.
- GL on estimation of costs/losses from major **ICT incidents**.
- Feasibility report on **IR EU Hub**.
- ESRB **recommendation A+B**.



EIOPA

5 standard tecnici sull'Oversight:

- ITS on **register template**.
- GL on **ESAs-Cas** oversight cooperation.
- RTS on oversight **conduct**.
- Call for Advice on **criticality criteria**.
- Call for Advice on **oversight fees**.

The regulatory outlook

As societal concerns over digital trust grow, so too does the interest of lawmakers and regulators, with greater demands for transparency and oversight. According to the **KPMG Cyber trust insights 2022 survey**:

36%

of respondents worry about their ability to meet **existing or new regulation of cybersecurity** when activities are **outsourced** to digital service providers.

34%

worry about **corporate-reporting disclosures** related to cybersecurity.

31%

worry about the growing demands around **critical infrastructure**, which is the subject of increasing regulation in the UK, the EU and the US.

To add to the burden, international organizations must cope with an increasingly complex, diverse and sometimes contradictory tapestry of extra-territorial regulation. "One challenge for CISOs is that stakeholders in different regions construe different meaning from the same regulations," says Ulrich Baisch, CIO, Bechtle, one of Europe's largest IT providers. "You need to have a clear concept of what you can and can't do."

KPMG perspective: Regulatory drivers

Globally, growth of cybersecurity and privacy regulation is accelerating. **More than 137 countries now have some form of data-protection regime**, often claiming extra-territorial jurisdiction over services offered into the country or the data of citizens of that country. More mature privacy regimes are moving into a **second generation of regulation** while confronting new privacy challenges driven by technology adoption. For example, discussions about the **regulation of AI** are now being formalized in draft legislation.

In addition, countries are implementing **increasingly strict critical infrastructure cybersecurity regulations** as concerns grow around attacks on industrial control systems. These regulations are moving from self-assessment to more **directive control frameworks, including mandatory incident reporting and external audit**.

Regulators are also being more prescriptive in their control frameworks, while also seeking to **reinforce the independence of the CISO** and their role in setting internal control standards. More holistic resilience requirements, focusing on business recovery in extreme but plausible scenarios, are also emerging in sectors such as finance.

Corporate requirements for transparency over cyber risks are under debate, along with growing requirements for the disclosure of ransomware incidents. **Companies should invest to automate compliance monitoring and reporting; maintain a regulatory watch; and consider privacy and security regulatory trends when developing new services and products.**



kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

2023 KPMG Advisory S.p.A. is a public limited company under Italian law and part of the KPMG network of independent entities affiliated with KPMG International Limited, a company incorporated under English law. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.