

# Future-proofing your Bank's Resilience

## Effective Cyber Risk Management in the Age of AI & Quantum Computing

تحسين مرونة مصرفك لمواجهة تحديات المستقبل  
الإدارة الفعالة للمخاطر السيبرانية في عصر الذكاء الاصطناعي والحوسبة الكمومية

© webID Risk Consulting / Switzerland  
Usama Abdelhamid

# Objective Statement



“Provide an overview understanding of

- **AI and Quantum Computing** and
- **related risks.**

عرض فهم عام للمخاطر الرقمية الناشئة التي تواجهها البنوك في عصر الذكاء الاصطناعي والحوسبة الكمية.



Explore how these technologies are

- **transforming banking operations,** and
- **highlight real-world risks and failures.**

استكشاف كيف تعمل هذه التقنيات على تحويل العمليات المصرفية، وتبسيط الضوء على المخاطر والإخفاقات في العالم الحقيقي.



Learn **strategies** for banks to stay ahead: **strengthen cybersecurity**, achieve **operational resilience**, and **prepare for future challenges**, including the critical need for **quantum agility.**"

مناقشة استراتيجيات البنوك لتعزيز الأمن السيبراني، وتحقيق الصمود التشغيلي، والاستعداد للتحديات المستقبلية، بما في ذلك الحاجة الماسة إلى الاستعداد للحوسبة الكمية

# Before we start ...

The “Pale Blue Dot” image of 1990, reminds us to:

- be **humble**, for we are very small in a vast cosmos,
- be **curious**, curiosity is our bridge to understanding and learning
- stay **grounded**, and see things in their true scale and meaning

You are here 

# Presentation structure

1

Security Threats  
Landscape

2

Quantum Risk &  
Impact

3

AI Risks &  
Opportunities

4

Conclusions  
& Takeaways

# 1 Cyber Security Threat Surge

## تصاعد التهديدات الأمنية السيبرانية

### Ransomware

Global attacks doubled YoY;  
+9% in financial sector incidents.



### DDoS

Global +20% increase YoY;  
Banking sector +97% increase in 2024.



### Social Engineering

42% of orgs hit;  
~45% of bank staff click malicious links in tests.  
*Hacking humans is still alarmingly effective.*



### Phishing

1M+ attacks Q1 2025 (record high);  
23 % target finance.



### Zero-Day Exploits

75 exploited in 2024 (down from 98 in 2023);  
>30 already in 2025 and unfolding.  
Note: Many zero-days remain undisclosed or undetected.



### Malware

40% of breaches involve malware (+30% YoY);  
Finance IoT malware +252%.  
*Malware mayhem intensifies.*

### Zero-Click Attacks (the silent threat)

Exploits with no user interaction - no clicks, no links  
Example: Pegasus spyware  
Targeting diplomats C-suite, VIP clients, client advisors  
Many attacks remain undisclosed or undetected.



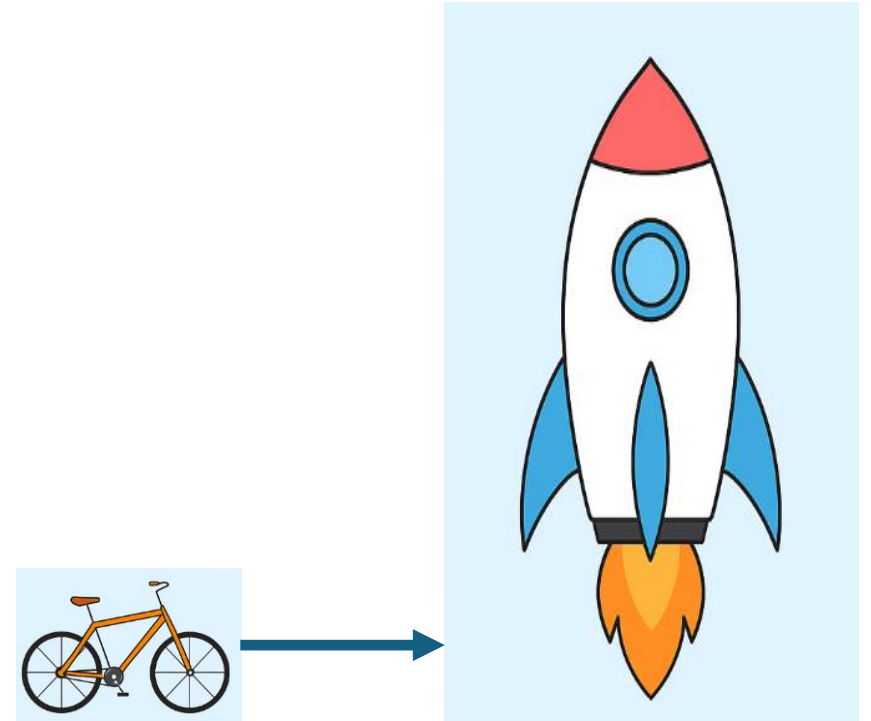
## 2 Quantum Computing – The Game Changer

Moving from classical computing to Quantum Computing is like moving from a **bike to a rocket**, but that speed comes with serious risks.

إن الانتقال من الحوسبة الكلاسيكية إلى الحوسبة الكمية يشبه الانتقال من دراجة إلى صاروخ، ولكن هذه السرعة تأتي مع مخاطر جسيمة.

### What is Quantum Computer (QC)?

- QC uses **qubits** (not bits) to handle complex calculations that classical computers can't even dream of.
- QC leverages the **principles of quantum physics** to process information.



# Quantum Computing Key Principles: Superposition

**Superposition** mean a qubit can exist in multiple states simultaneously.

2 Classical Bits

|    |
|----|
| 00 |
| 01 |
| 10 |
| 11 |

Only one state at a time

2 Qubits (Superposition)

|    |
|----|
| 00 |
| 01 |
| 10 |
| 11 |

All states simultaneously

This means **exponential growth**:

If you have **n** qubits, they can represent  **$2^n$**  different states simultaneously.

Example:

**10 qubits** → can represent **1,024** states at once,

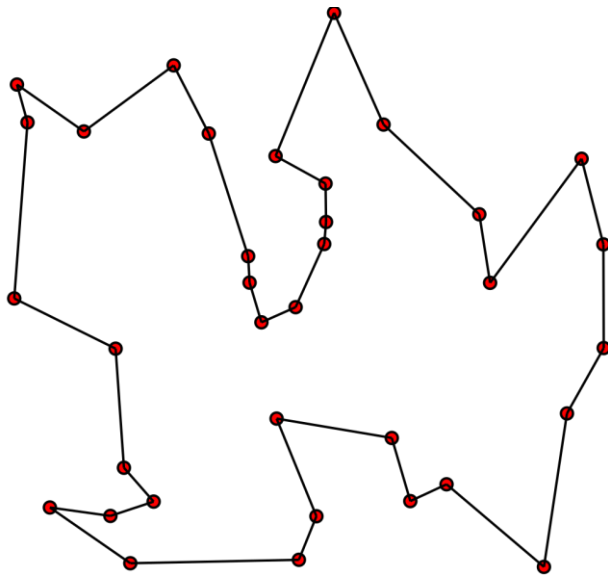
**20 qubits** → can represent **over a million** states at once,

**50 qubits** → can represent over **1 quadrillion** states (this is where classical supercomputers struggle!)

# Real-world Problem Example

## The **Traveling Salesman Problem (TSP)**

shortest possible route that visits a set of cities exactly once and return to origin city

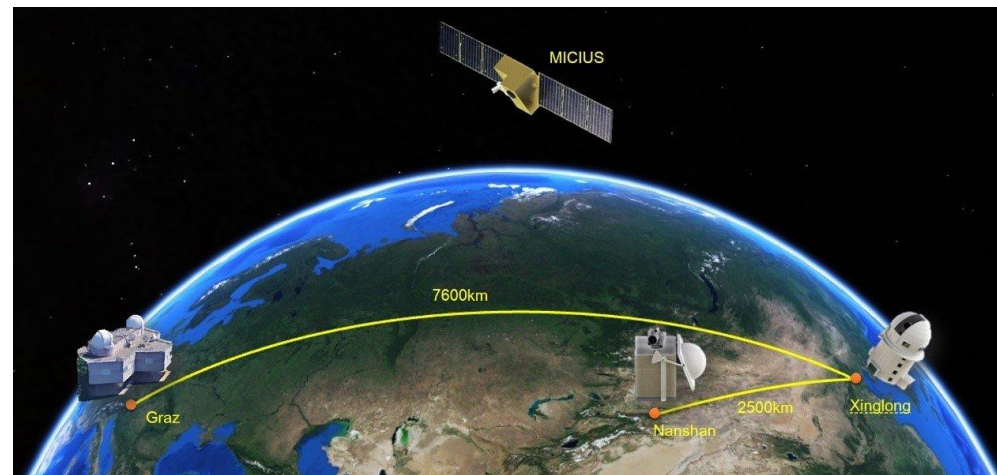


Possible routes of 15 cities = 87,178,291,200 routes

# Quantum Computing Key Principles: Entanglement

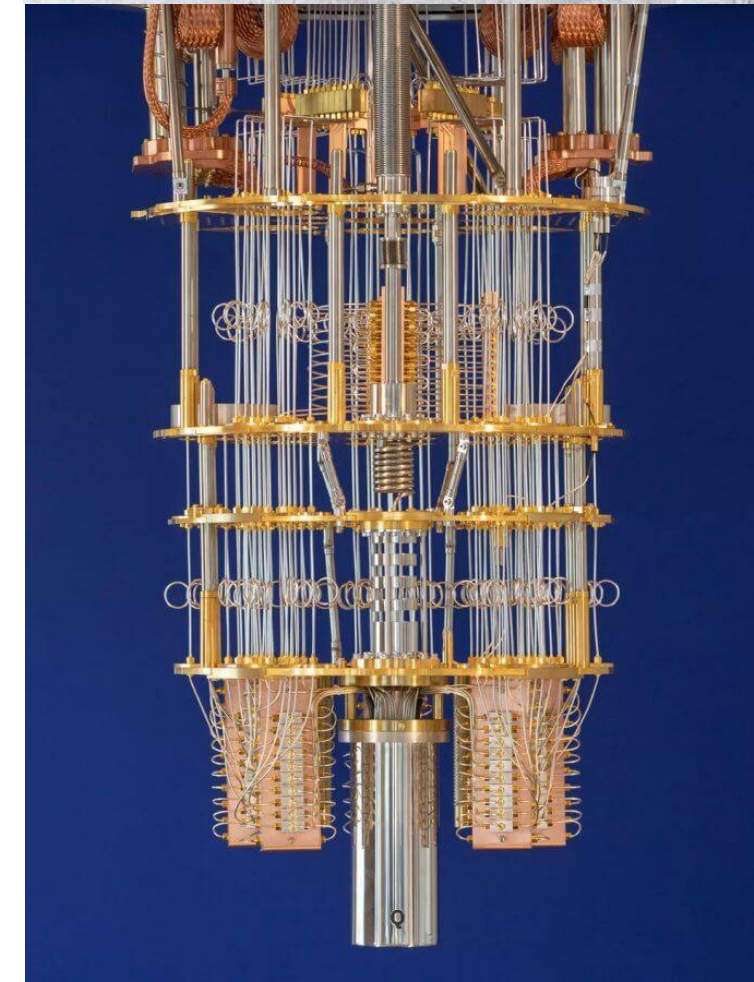
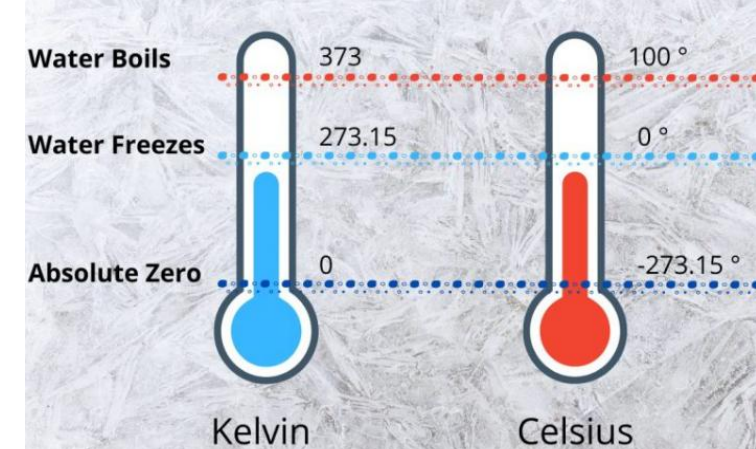
- **Entanglement:**

- Definition: Qubits can become entangled, **meaning their states are linked regardless of distance.**
- Profound implication: This allows for **parallel processing** of vast information. Open-up completely new computational possibilities.
- Real-world example: **China's Quantum Satellite "Micius"**: In 2017, China successfully demonstrated Quantum Key Distribution (QKD) using entangled photons sent between a satellite (Micius) and ground stations over a distance of 7'600 km (China & Austria).



# Quantum Computing: Challenges

- Require complex refrigeration systems to maintain **qubit stability**.
- **Vulnerable** to any interferences, e.g. electromagnetic signals like radio waves or Wi-Fi or any change in temperature
- When a qubit loses its delicate quantum state, it becomes **decoherence** and leads to error in calculations
- **QC remain error prone due to isolation imperfection.**



# The Quantum Threat

Quantum Computing promises speed, but what if I told you it could also break almost all current encryption methods overnight? Imagine waking up to a world where all your bank's encrypted data is vulnerable.

تعدنا الحوسبة الكمية بالسرعة، ولكن ماذا لو أخبرتك أنها يمكن أن تكسر أيضًا جميع طرق التشفير الحالية تقريبًا بين عشية وضحاها؟ تخيل أن تستيقظ على عالم تكون فيه جميع بياناتك المصرفية المشفرة غير محمية.

- **Threat to Cryptography:** Quantum computers will crack widely used encryption like RSA and ECC, putting bank data and transactions at risk.
- **Quantum Cyberattacks:** A 2020 Homeland Security report warned that nation-states are already storing encrypted data for future decryption. ***Harvest Now, Decrypt Later (HNDL) when the Q-Day arrives***

# What is the Q-Day?

- **A future date when quantum computers become powerful enough to break today's cryptographic systems** such as RSA and ECC
- **How powerful:** *Examples*
  - To break a 2048-bit RSA, QC must reach at least 4'000 logical qubits
  - To break a 3072-bit RSA, QC must reach at least 6'000 logical qubits
- **Expected Timeline to reach Q-Day ??**

# A single quantum attack

“We estimate that a single quantum attack on one of the five largest financial institutions in the U.S. would cause a cascading financial failure costing anywhere from \$730 Billion to \$1.95 Trillion.” Forbes

Source: [Getting The Big Banks To Confront The Quantum Challenge](#) Forbes

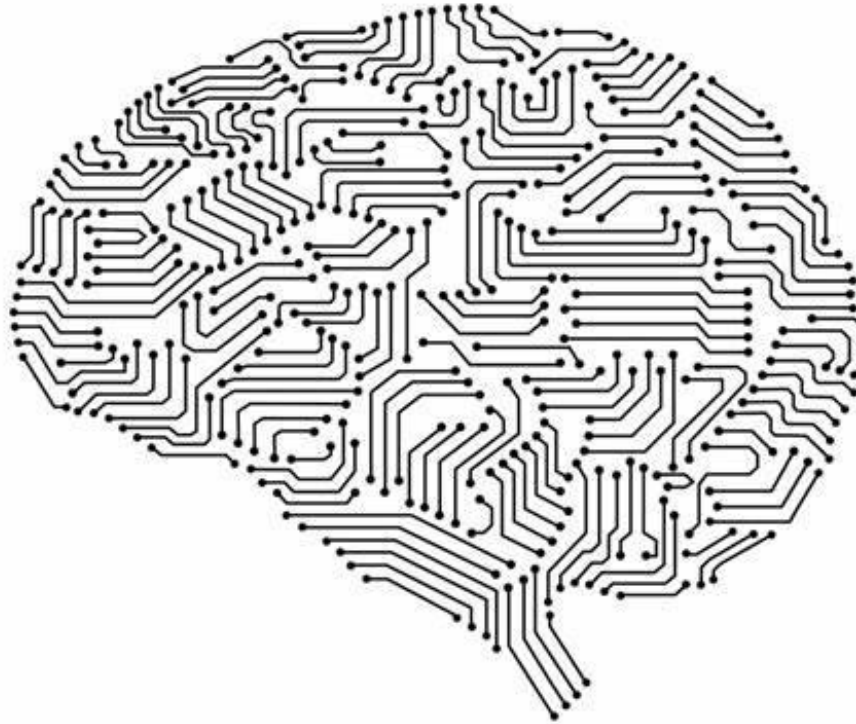
# Why Banks Must Become Quantum-Ready?

1. **Loss of confidentiality and data integrity:** exposure of sensitive client data and financial transactions
2. **Loss of trust:** in institutions, governments and banks
3. **Potential Financial Catastrophes:** as a result of quantum attack
4. **Regulatory Pressure for quantum resilience:** e.g. European Central Bank
5. **Competitive Advantage:** Early adoption of **quantum-ready solutions** can position banks as leaders in the industry - banks can differentiate themselves as secure and trustworthy institutions
6. **Future-Proofing Operations:** Investing now in Quantum-Ready “**Q-Agility**”, you can manage risks before they materialize and safeguard your assets and your clients

# Steps Toward Quantum Readiness

- **Assess Your Current Cryptographic Systems:** audit existing encryption, identify and prioritize critical assets that require enhanced quantum-resistant.
  - **Transition to Quantum-Resistant Algorithms:** Adopt post-quantum algorithms recommended by NIST.
  - **Collaborate and partner with Technology Providers and Consultants:** To ensure quantum-resistant solutions are integrated into core infrastructure.
  - **Build Quantum-Safe Governance Framework:** Develop governance policies that **oversee the migration** to quantum-safe protocols, ensuring compliance with emerging regulations and standards.
  - **Monitor Emerging Quantum Technologies:** Stay updated on advancements in quantum computing and post-quantum encryption.
  - **Educate and Train Teams:** Provide training for cybersecurity, IT, and compliance teams to **understand quantum threats** and their role in safeguarding the bank's operations against these future risks.
- 
- The National Institute of Standards and Technology (NIST) has officially standardized five quantum-resistant algorithms.
  - These algorithms are now recommended for immediate adoption to future-proof systems against quantum attacks.

# 3 Gen AI Opportunities Risks



# AI has been with us since the 1950s



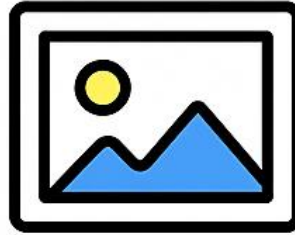
Grandfather of AI: John McCarthy 1956

# Types of AI



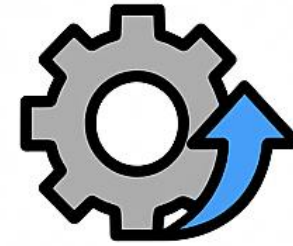
## Traditional AI

Follows rules  
to perform  
specific tasks



## Generative AI

Creates new  
content based  
on data



## Agentic AI

Acts autonomously  
to achieve goals

# AI Agents: Visions of the New Workforce



- Marc Zuckerberg of Meta  
*“I think we're going to live in a world where there are going to be hundreds of millions or billions of different AI agents eventually, probably more AI agents than there are people in the world.”*



- Jensen Huang of Nvidia  
*“The IT department of every company is going to be the HR department of AI Agents in the future”*



- Gartner:  
*“AI agents are the top strategic tech trend for 2025”*

**AI agents aren't just tools — they're becoming coworkers.**

# AI savings real-world banking examples

| Institution                                                           | Estimated Savings / Gains                                                 | AI Impact Area                                                            |
|-----------------------------------------------------------------------|---------------------------------------------------------------------------|---------------------------------------------------------------------------|
| <b>Bank of America (Erica)</b>                                        | 100M+ customer requests/year; 1.5B+ total interactions                    | Virtual assistant for customer service and financial guidance             |
| <b>JPMorgan Chase</b><br><i>18 bn invested last two years on tech</i> | ~30% reduction in servicing costs; 10% support headcount cut              | Generative AI for service automation, client interaction                  |
| <b>JPMorgan Chase</b>                                                 | 360'000 hours/year                                                        | Document analysis automation using COiN (Contract Intelligence) platform. |
| <b>HSBC</b>                                                           | Expects up to \$1.5 B/year savings from back-office ops now powered by AI | Agentic AI agents for compliance (e.g. AML, Fraud detection) & operations |
| <b>Commonwealth Bank (Australia)</b>                                  | 40% drop-in call center wait time; 50% reduction in scam losses           | Customer support & fraud prevention AI                                    |
| <b>Deloitte (industry est.)</b>                                       | \$0.5–\$1.1M per software engineer in annual savings by 2028              | Developer efficiency via GenAI copilots<br>- see graph next slide         |

"AI and advanced analytics could unlock up to \$1 trillion in annual value for banking, including customer service, fraud detection, development, and operations“ [McKinsey Building the AI Bank of the Future Report](#)

# How AI Changes the Risk Landscape

- **AI amplifies traditional IT risk.**
- **AI introduces new risks unique to AI**
- **AI risks emerge in decision-making systems**
- **Expands systemic and geopolitical risk exposure**

AI risks are **not just more of the same** — they **extend old vulnerabilities** while in parallel **creating new ones**, making AI a *dual amplifier and disruptor* in the risk landscape.

# The Dark Side – Real-Life AI Failures



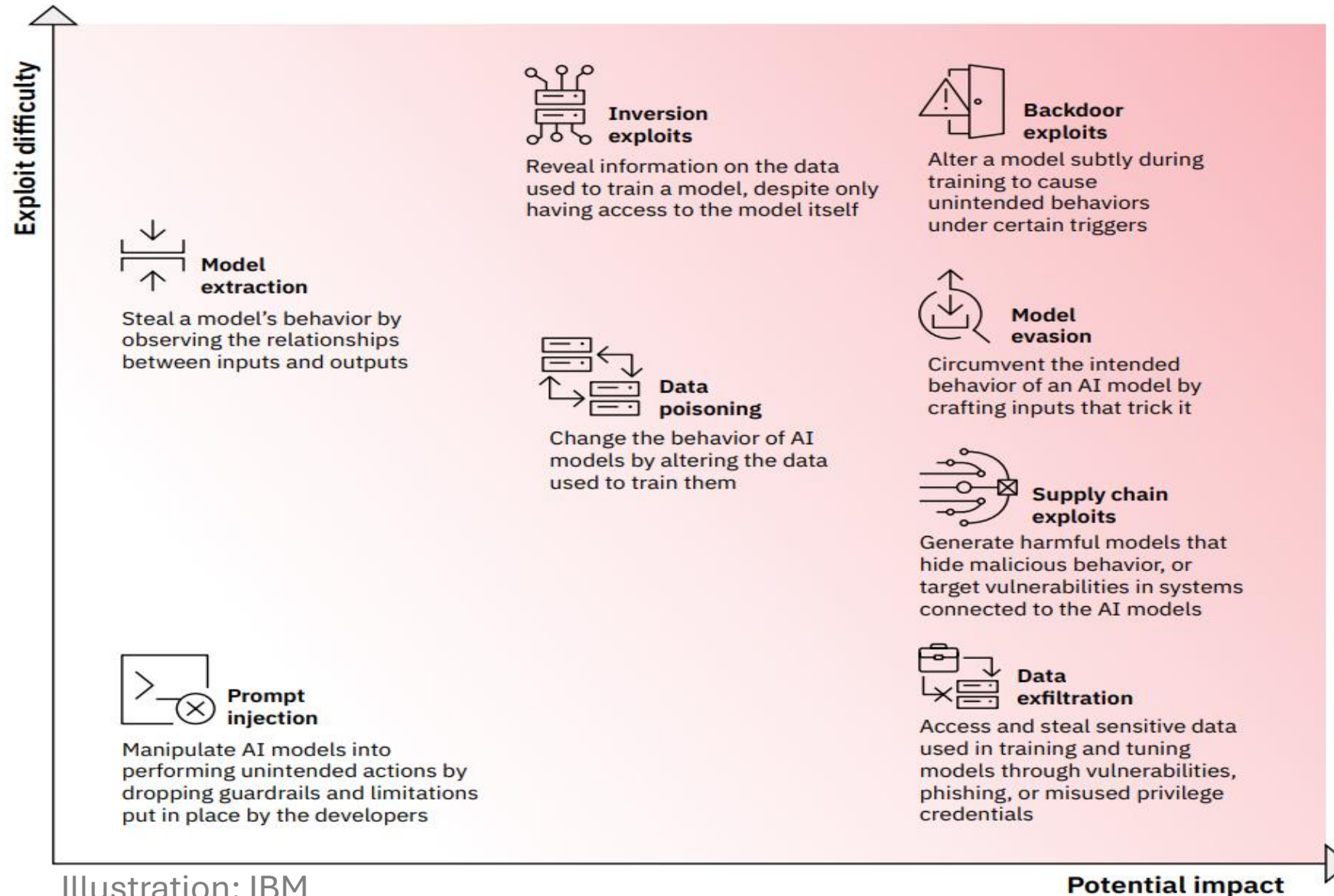
While AI offers remarkable capabilities, it also **expands the attack surface** and exposures to banks and raises concerns about data privacy, data accuracy, ethics and cyber security.—let's look at some real stories.

على الرغم من أن الذكاء الاصطناعي يوفر قدرات مذهلة، إلا أنه يوسع أيضاً من نطاق الهجمات والتعرضات التي تتعرض لها البنوك ويثير المخاوف بشأن خصوصية البيانات ودقة البيانات والأخلاقيات والأمن السيبراني. - لنلقي نظرة على بعض القصص الحقيقية.

- **AI Fraud Deepfake Case in Hong Kong February 2024: A \$25.6 million** AI-driven deepfake video simulation fraud exposed how AI can be weaponized by cyber attackers. [CNN](#)
- **AI Fraud Voice Cloning Case in UAE 2020:** Cybercriminals employed AI and cloned the voice of a company director in the U.A.E. to steal as much as **\$35 million** Source: [Forbes](#)
- **Bias in Algorithms:** Apple's credit card, developed with Goldman Sachs was found to be giving lower credit limits to women than men, even when they had similar financial profiles.

**AI is only as good as its governance and its security**

# Emergent threats to AI *offline reading*



**These threats involve manipulating AI model during development and operational life-cycles** aiming the model takes unintended actions – and represent critical challenges to the safe deployment and maintenance of AI models, and mitigating them requires robust security protocols, regular audits, and real-time monitoring throughout AI Dev and Op lifecycles..

# Statement on AI Risk

Mitigating the **risk of extinction** from AI should be a global priority alongside other societal-scale risks such as pandemics and nuclear war.

يجب أن يكون تجنب خطر الانقراض الناجم عن الذكاء الاصطناعي أولوية عالمية إلى جانب المخاطر الأخرى على المستوى المجتمعي مثل الأوبئة والحرب النووية.

May 2023, 350 Signatories of executives, researchers and engineers working in AI, including Bill Gates.

Source: <https://www.safe.ai/work/statement-on-ai-risk>

# AI Enhances Cyber Security

AI doesn't just make banking faster—it makes it safer. Imagine AI bots hunting cyber threats 24/7, learning and evolving every time they hinder an attack.

الذكاء الاصطناعي لا يجعل الخدمات المصرفية أسرع فحسب - بل يجعلها أكثر أماناً. تخيل أن روبوتات الذكاء الاصطناعي تطارد التهديدات الإلكترونية على مدار الساعة طوال أيام الأسبوع، وتتعلم وتتطور في كل مرة تعيق فيها هجوماً.

- **Automated threat detection:** AI models scan massive volumes of logs and network traffic to identify anomalies and potential cyber intrusions (e.g. malware, phishing).
- **Behavioral Analytics:** AI tracks and learns user behavior, flagging and alerting on suspicious activity and preventing insider breaches. (Citybank)
- **Fraud Detection:** Machine learning algorithms analyze real-time transactions to detect unusual patterns, making it easier to spot fraud as it happens and protect both the bank and its customers.
- **Incident response automation:** AI can automatically isolate compromised systems or accounts when a security threat is detected, preventing spread of the attack.

**AI is not replacing security teams; it is amplifying their reach and speed,** turning defense into a *proactive, real-time capability*. AI can act as a risk manager.

## 4 Conclusions & Takeaways

# Conclusion – Strategic Takeaways

1. **Start Q-Agility Today:** don't wait until it's too late – waiting is a risk
2. **Establish an AI Governance Board with Clear Mandate:**
3. **Define & Socialize AI Strategy**
4. **Update & embed your bank's GRC capabilities in all your AI initiatives**
5. **Monitor and Eliminate Shadow AI**
6. **Champion a Culture of Responsible AI by Default**
7. **Decide Strategically on AI deployment approach**
8. **Remember “Strategy is a choice”** – and doing nothing is a choice too.
9. **A proactive strategy to AI and Quantum risks** will differentiate the **leaders from the laggards** in the next decade
10. **Call to Action:** Your bank's future will be shaped by the decisions you make today.



# Thank you

---

## Q&A

Usama Abdelhamid

**webID Risk Consulting**

[www.webID.ch](http://www.webID.ch)

October 2025