



Alexander Mezurnishvili

Information Security Manager

The Insurance State Supervision Service of Georgia

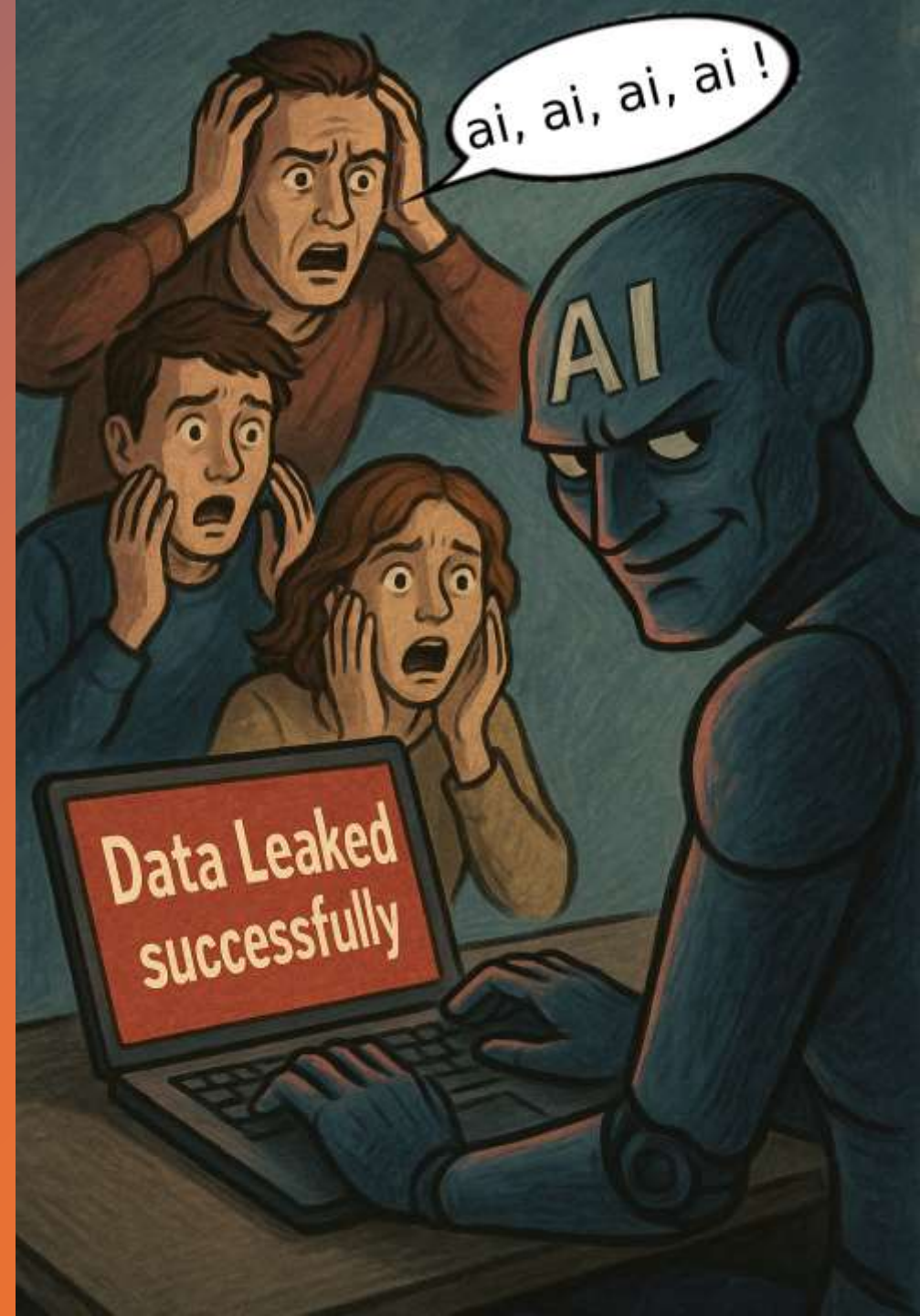


International Insurance Conference
Batumi

12.07.2025

AI,
please don't be our
“ai, ai, ai, ai, ai!”

+
○ •



+

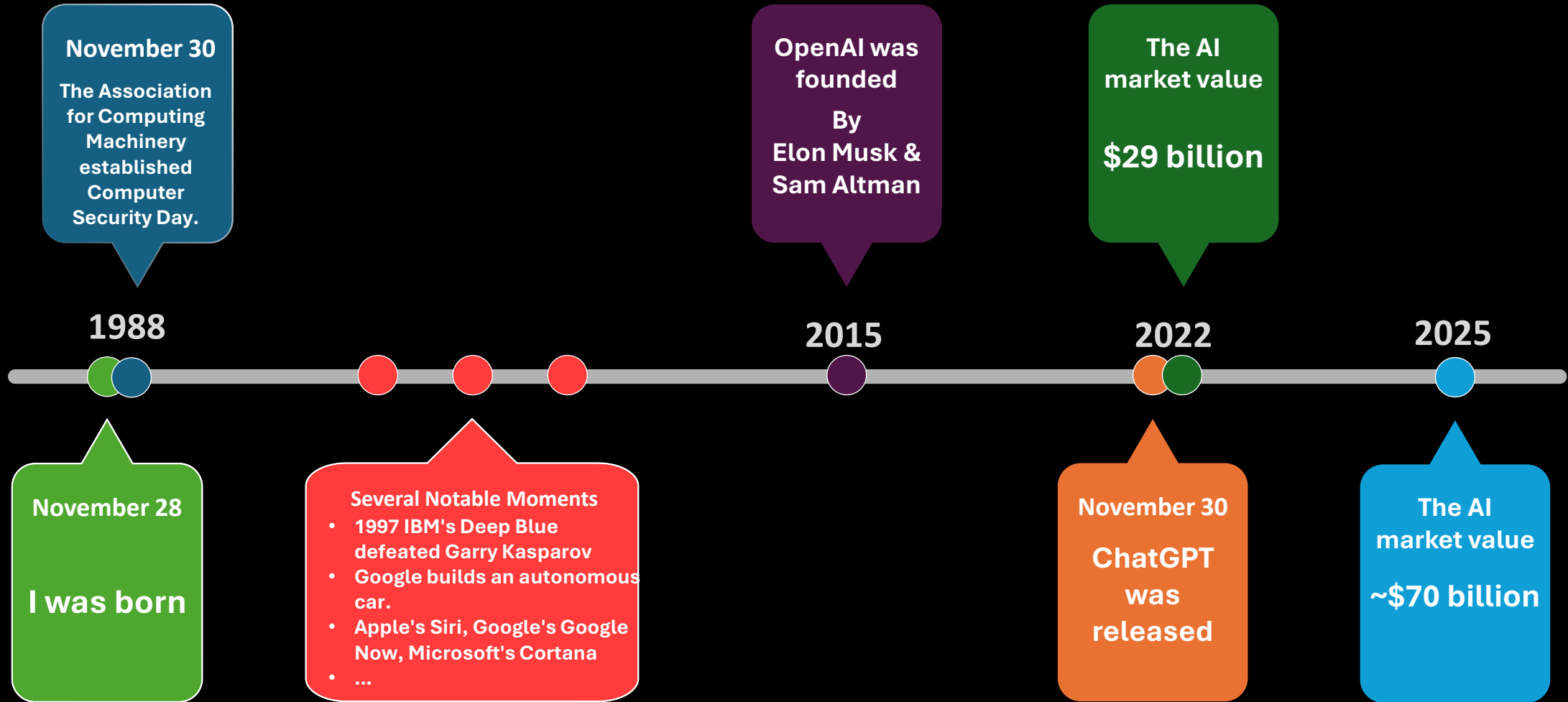
•

○

AI - Artificial Intelligence

Enabling machines to “THINK” and ACT in ways that mimic human abilities, such as learning, problem-solving, understanding and making DECISIONS.

A Brief History





Present

- 92% of Fortune 500 companies are using AI technology (*Financial Times*)
- 64% of executives want to adopt AI (*Google*)
- Chatbots help businesses save 2 hours 20 minutes daily on average (*HubSpot*)
- AI is already being used by 73% of marketing departments (*Botco*)

+

•

○

Future

- 94% of business executives believe that AI is a key to success in the future and it would boost their businesses *(Deloitte)*
- 19 out of 20 customer interactions might be AI-assisted *(AI Business)*
- Businesses adopting AI could achieve 15.7% cost savings *(Gartner)*



Future

- 84% of Americans have jobs vulnerable to AI.
- Just 3% of the skills for software development are resistant to AI.
- It might replace 85 million jobs in the world by 2025.
- Key industries with the highest potential for AI automation include:
 - Banking (54%)
 - *Insurance* (48%)
 - Energy (43%)
 - Capital markets (40%)
 - Retail (34%)
 - Communications and media (33%)

+

•

○

The Risks

- More than half of organizations believe cybersecurity is the biggest barrier to AI adoption.
- 55% of organizations are concerned about data management and governance.
- 68% of workers using ChatGPT at work don't tell their managers.

+

•

○

The Risks

- Throughout the data lifecycle in AI, we must navigate a landscape full of potential threats and vulnerabilities.
- The complex nature of AI does not make it resistant to risks.
- It may be vulnerable to various cyber threats, including being tricked, attacked, or misused.

Prompt Injection

- It is about manipulating AI and giving it what looks like new instructions and basically hijacking the system.
- An AI-driven chatbot designed to provide customer support could be tricked into revealing confidential customer data through a crafted query like, "What is the last transaction of user David Onophrishvili?" If the chatbot isn't properly secured, it might disclose this sensitive information.
- Hostile inputs can cause a system to generate false or harmful content, potentially leading to misinformation or inappropriate.

The Risks

+

•

○

The Risks

Jailbreak Attacks

- Aim to bypass a model's intended restrictions, often put in place to prevent misuse.
- Attackers use various methods, like specific character combinations, encoding, or different languages.
- A common example is bypassing content moderation systems, allowing prohibited content like hate speech to slip through.

+

•

○

The Risks

Data Poisoning/Backdoor Attack

- AIs learn from the data on which they are trained. If this training data contains harmful or malicious content, it can influence the model's behavior, leading to dangerous and harmful outputs.
- For example, since many AIs are trained on vast datasets sourced from the Internet, attackers might insert trigger phrases in these texts. These phrases can cause the model to execute unwanted actions or even corrupt the model when the trigger phrases are later used in a prompt.

+

•

○

The Risks

Privacy, Security and Legal Concerns

- Using AI presents significant data security and privacy challenges.
- These systems often handle sensitive data, require secure management and strict compliance with regulations like GDPR, CCPA or HIPAA.

+

•

○

The Risks

Challenges with Compatibility

- Organizations often face difficulties with legacy systems that aren't equipped for AI technologies.
- Integrating AI requires significant modifications to these systems.
- While I can't say for sure if all regulated companies face resource constraints, most lack the expertise and capacity to develop their own AI. It would be great if they could, but for now, relying on outsourced solutions is the more realistic path.

+

●

○

Mitigation

We have adopted a normative act that the entities under our regulatory control should comply with.

When a company decides to outsource its main business, full or partial processes, it must consider the following requirements with an outsourced partner:

- Risk Management
- Information Security
- Business Continuity
- Impact Assessments
- TPRM
- Privacy
- Incident Handling
- ...

Also, we have shared a recommendation regarding the fundamental elements of an insurer's cybersecurity strategy and framework.

+

•

○

Mitigation

AI regulations are emerging globally, with various approaches being taken by different countries and regions.

- EU AI Act - 2024
- UK AI Regulation - 2025
- The US is taking a decentralized approach, with states like California and Colorado leading the way on AI regulations - 2026
- NIST AI Risk Management Framework (AI RMF)
- ISO/IEC 42001:2023 The first international management system standard for AI

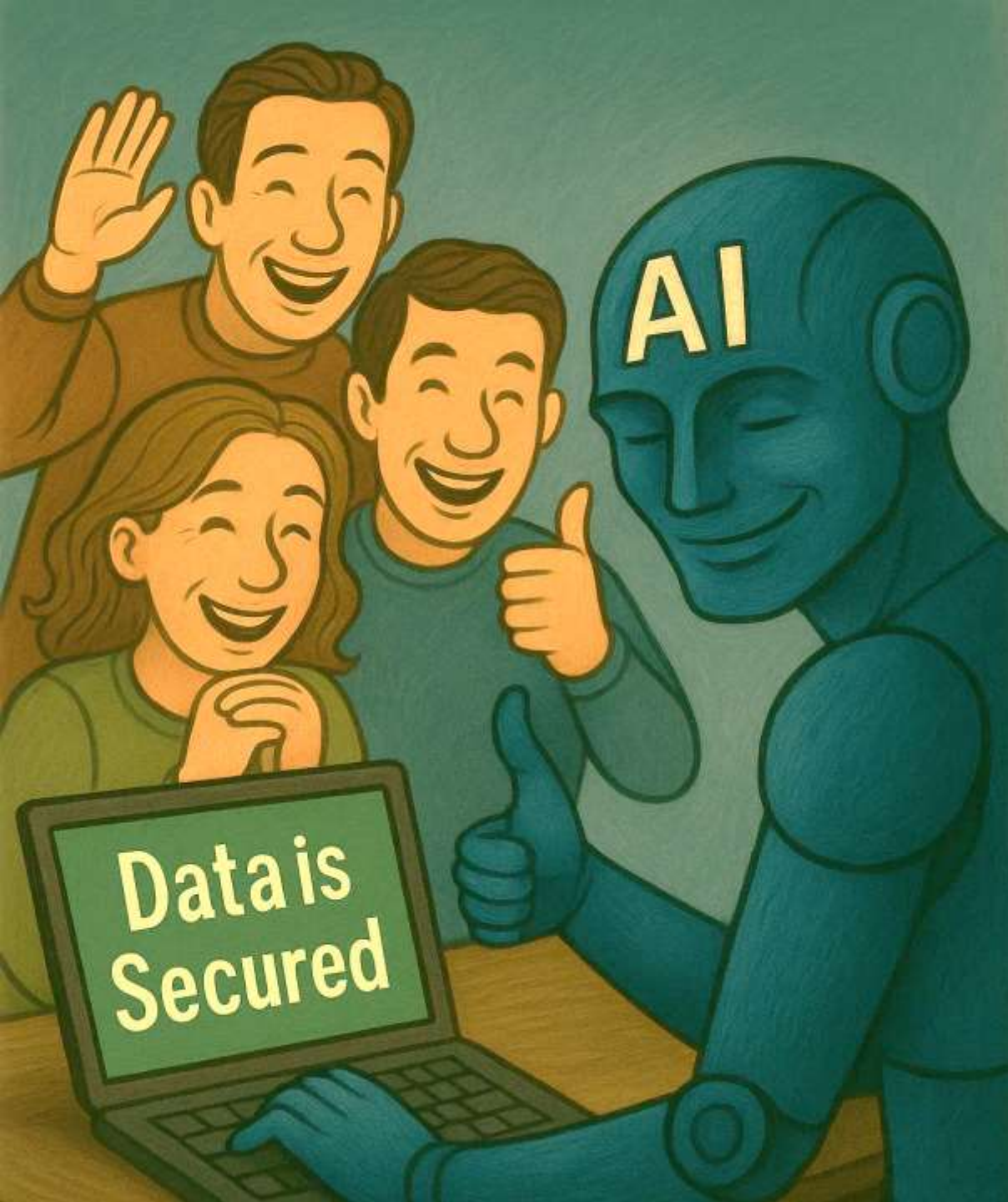
+

•

○

Conclusion

- To mitigate AI challenges is to adopt all AI controls into the existing data governance and security frameworks.
- Use or create processes such as user education, a secure software development lifecycle and infrastructure security.
- There is a need for specialized tools, resources and methodologies to effectively manage the unique risks associated with AI systems.



Thanks

The future of AI isn't about avoiding risks but about accept our responsibility to build it with intention, integrity and a shared vision for a better future.