“The present and future of Information Risk Management in the AI era”

before I start the presentation I would like to ask you a question. How many of you have had your user account stolen, your facebook, your mail system hacked? How many of you have lost data?
Now then imagine this threat in a corporate environment, thousands of users, thousands of mailboxes. Now, one of the main reasons for the existence of IRM is to protect them.

Introduction
Disclaimer, I'm not a designated speaker, I'm not authorised to talk about inside information, in fact it's strictly forbidden. If I said a colour that would refer to the bank, I'd be in trouble.

Today, I’m going to explain how Information Risk Management is operating and evolving in the age of the AI currently.
I work for a financial institute, one of the major ones in the EU, with a lot of subsidiaries in eastern europe. My company cooperates with the stock markets providing retail and institutional brokerage. I have been responsible for IT operations for around 15 years and nowadays i am shifting out from daily operations.
When I started 15 years ago, our biggest concern was someone forgetting their password. Now we're worried about AI models potentially learning our trade secrets. 🙂

2. oldal
Our company was set up as some kind of a startup in the past, we built everything from scratch. We had to set up each and every part of the environment, including network, servers, storage, creating some control over these things and so on. It helped me to see the big picture and also make the merge easier, due to the fact a few years later it required us to integrate ourself into a whole, enterprise level IT infrastructure. It required a lot of cooperation with the local points of gravity - i mean the parent’s bank’s Information Risk Management (IRM), we got involved in their agenda, processes and so on.

- Painful process

Daily collaboration with Information Risk Management has taught us valuable lessons about process maturity. As a small-to-medium enterprise, adapting to formal processes like ticketing systems and documentation initially felt like it was slowing us down. It's particularly challenging for smaller companies and startups to implement processes that may seem unnecessary or burdensome at first glance, especially with limited resources.

- Specific examples of interaction points where we had to ask for consent from IRM

Business as usual tasks, change requests like configuring the enterprise proxy rules to provide access to something on the internet for a specific groups of people
Creating new firewall rules for servers or applications
Implementing new VPN - virtual private network connections to have an encrypted access to 3rd party companies
Reporting anomalies like incoming phishing, scams via emails

3. Oldal
IRM organization structure

- Reporting lines working on the usual way:
    - Security Operations Center -> Chief Risk Officer > Board
        - Board of Directors are responsible for approving risk appetite and strategy on the long term and reviewing major incidents and risk reports quarterly
        - Chief Risk Officer - direct report line to BOD, oversees enterprise wide risk management, coordinates with other C-level executives

Teams of IRM and their tasks, responsibilies:

- Security Operations Center (SOC)

The SOC team comprises 15-20 members. While they are a relatively generalized team, meaning individuals are capable of handling various tasks. They operate with a flexible structure to cover the wide range of SOC responsibilities without having to be specialized in particular fields.

    - 24/7 monitoring and incident response, processing dozens of alerts on a daily basis of which are false most of the time like noise
    - Real-time threat detection and response
    - Security tool monitoring and management
    - Change request reviews and approvals like firewall rules
    - Incident triage and escalation
    - Vulnerability scanning coordination
    - Security alert investigation
    - First-line incident response
- Security Architecture Team
    - One of their key task is to review the security of newly deployed applications, it is an important and quite a hard task to make a decision the risk level of them.
    - Strategic security design and oversight
    - Security architecture review for new projects
    - Technology risk assessments
    - Security standards development
    - Cloud security architecture
    - Identity and access management design
    - Integration security patterns
    - Zero-trust architecture implementation

* Audit and Governance Team

- This team conducts regular internal audits to check compliance with security policies and coordinates external audits by the Hungarian National Bank and the Group, and develops a security awareness programme for staff. They are like the strict parents of IT - they say 'no' to everything first, then maybe 'yes' after extensive convincing. 🙂

    - You never want to be on their list. :) I made a mistake a few weeks ago and clicked on the url in an email offering valentines day gifts. I hope that I will not have to attend another security awareness training course. 🙂
    - Compliance and policy management
    - Policy development and maintenance
    - Regulatory compliance monitoring
    - Security awareness program
    - Risk assessment framework management
    - Compliance reporting
    - Control testing and validation

4. oldal

Core functions

- Risk assessments, frameworks: NIST, ISO27k
    - NIST - US National Institute of Standards and technology or Never ending IT security Tasks 😀, which is a checklist for security configuration baselines to mitigate cybersecurity threats.
      To bring an example, we use this to identify all the IT assets and data, sometimes it is quite harder than you think.
    - ISO27k - ISO 27000 family, collection of the best practice recommendations regarding information security management cover fields like privacy, confidentiality, security
      These are the rulesets which we use as a frameworks for Information Security Management systems. You can consider these as guidelines how to create access management, physical security, documentations, how to implement controls over the organization

- Regulatory compliance:
    - DORA - Digital Operational Resilience Act, it requires us to have robust IT risk management and incident response capabilities to ensure operational resilience. My favorite here is how to identify outsourced services and find their substitutes.
    - GDPR - General Data Protection Regulation, it mandates strict data protection measures for personal data, influencing our data security policies and procedures.
    - MiFID II - Markets in Financial Instruments Directive II, MiFID II impacts how we secure market data and trading systems to prevent market abuse and ensure fair trading
    - Furthermore, we operate under local regulatory requirements, with bodies like Hunguard setting standards. In Hungary, we face a particularly dynamic regulatory landscape governed by the HNB. Keeping pace is challenging due to the HNB's regulatory framework which can change very rapidly. New regulations are sometimes published in the official gazette overnight and require implementation within days. It requires agility and close monitoring of regulatory updates to ensure continuous compliance.

5. oldal

- Incident lifecycle and SOC operations

SOC have its own communication system beyond the normal channels and this is the place where they handle the security incidents. It can be originated from different sources like emails, phone calls, regular tickets and then IRM can open a security ticket based on them and then they can be followed by the global IRM entity.The escalation path for an incident ticket is determined by its severity. Less critical incidents may follow standard ticket workflows with defined SLAs. However, for high-severity incidents, escalation can be immediate and direct, potentially involving on-call personnel even during off-hours.

- Control design/systems monitoring.

Our control design follows a defense-in-depth approach, implementing technical, administrative, and physical controls aligned with NIST and ISO27001 frameworks. We employ continuous monitoring through a multi-layered system including SIEM solutions, network traffic analysis, endpoint detection and response (EDR), and automated vulnerability scanning. Critical systems undergo 24/7 real-time monitoring with automated alerting based on behavioral analysis and predefined thresholds. We supplement automated monitoring with regular manual assessments and red team exercises to validate control effectiveness. This comprehensive approach enables early detection of potential security incidents and provides assurance that controls are functioning as designed.

- Password vaults

Password vaults are critical security infrastructure that provide centralized, encrypted storage for privileged credentials.

- Policy creation and maintenance process

Our policy creation and maintenance follows a structured lifecycle approach. New policies are initiated based on regulatory changes, security incidents, or evolving best practices. Draft policies undergo review by multiple stakeholders including legal, compliance, operations, and business units. Each policy requires formal approval from the governance committee before implementation. We maintain a centralized policy repository with version control and conduct mandatory annual reviews of all policies.

6. oldal

AI impact on IRM

- **AI cloud solutions, transition to the cloud**

  On-premise solutions are not efficient due to the costs, scalability and speed of innovation coming from the cloud. AI cloud solutions represent significant advancements in efficiency and flexibility.

- **Current automation initiatives**

Office 365 AI features for security purposes (log reading, vulnerability checks, Copilot, Data Loss Prevention)

AI application to replace tier 1 tasks:

- Basic vulnerability scanning analysis
- Routine report generation

- Initial incident triage
- Compliance reporting

- **New risk landscape**

Testing LLM (Large Language Model) agents for automated threat intelligence analysis, security policy generation, and vulnerability report summarization

Providing developer support with AI tools while maintaining security

- **Skill evolution**: Evolution of IRM professionals' skills: from technical expertise to hybrid expertise (e.g., DevOps), with automation of lower-expertise tasks.

AI Agents

We dont have them yet.

AI Governance Challenges

- Data usage policies for AI - what can be accessible for AI
- Bias in AI outputs
- Accountability for AI decisions - who will be responsible for a wrong decision?
- Explainability of AI results
- Audit trails for AI actions

Developing AI ethics guidelines, establishing AI review boards, implementing strict data access controls for AI systems, and a "human-in-the-loop" approach for critical AI decisions.

7. oldal

- **Current limitations and trends**
  - Protection of company data from AI systems
  - The tension between the *competitive pressure* to adopt AI and the *data privacy/security concerns* of feeding sensitive data to AI systems, especially cloud-based AIs.
  - Increasing adoption of AI solutions alongside strict security protocols

8. oldal

Bright future and strategic priorities

The future of IRM might be AI systems protecting us from other AI systems 🙂

Our strategic priorities for the next 3-5 years include:

- Implementing a zero-trust security architecture across all systems

- Developing AI-powered threat detection capabilities with human oversight
- Creating a comprehensive retraining program for staff whose roles may be automated
- Establishing an AI governance framework that balances innovation with security
- Building strategic partnerships with specialized AI security providers while maintaining critical in-house expertise

- Societal changes, disappearing roles:
  This organizational evolution and job displacement will have significant societal implications. Preparing for these societal changes must be a key strategic priority. We need to consider how to support those whose roles are automated and ensure they have opportunities for retraining and new livelihoods.

- Geopolitical Concerns
  We (EU) are heavily reliant on outsourced services, especially from American companies. The extent of this outsourcing is irreversible. Coupled with the current geopolitical situation, this dependence poses a significant risk, because if we look at it, we can see that almost all LLMs - so called AI's are US based. I think this is an existential issue, the most important one. Everything must be done because we cannot afford to miss this technological revolution.

Good luck for everyone, buckle up.