The Present and Future of Information Risk Management in the AI Era

Disclaimer and introduction

Kovács János

Lessons from the Past

The journey from password problems to AI risks

Initial challenges: integrating from a startup to an enterprise-level IT infrastructure

Lessons learned from collaborating with IRM: the importance of processes, especially for startups and small companies

Specific examples of tasks requiring IRM approval

- Fw rules, VPN connections, endpoint defense, reporting function

IRM Organizational Structure

Overview of reporting lines: SOC -> Chief Risk Officer -> Board

Roles of the Board and Chief Risk Officer

IRM teams and their responsibilities, members:

- Security Operations Center (24/7 monitoring, incident response,)
- Security Architecture Team (application security, technology risk assessment)
- Audit and Governance Team (compliance, regulation)

Regulatory Compliance and Frameworks

Introduction to key frameworks (NIST, ISO27000 family)

Impact of major regulations like DORA, GDPR, MiFID II, especially in the Hungarian context

The HNB's dynamic regulatory environment, and the importance of rapid response

Incident Management and Controls

SOC incident management process, escalation paths

Control design, continuous system monitoring, vulnerability assessments

Password vaults and other critical security infrastructure

Policy creation and maintenance, lifecycle of them

The Impact of AI on IRM

Benefits of cloud-based AI solutions (cost, scalability, innovation)

Current automation efforts (O365 AI features, LLM agents)

New risks generated by AI (data access privacy, bias, accountability, explainability, audit trail)

Importance of AI ethics guidelines and the "human-in-the-loop" approach

Current limitations and trends

How to protect company data from AI systems

AI in the cloud concerns

Competitive pressure vs data privacy/security

Future Priorities and Challenges

Implementing a zero-trust security architecture

AI-powered threat detection with human oversight

Workforce retraining, preparing for new roles

Developing an AI governance framework to balance innovation with security

Conclusion

- The importance of preparing for societal changes
- Geopolitical concerns, EU dependency

Thank you