Managing cyber security risks

International Regulatory Conference 2025
Skopje, 20.05.2025

Nadica Josifovski
Advisor to the Director for Information Security
nadica.josifovski@aec.mk

Introduction

- ***Cybersecurity Risk Management*** *- the ongoing process of identifying, analyzing, and responding to cyber threats that could impact the confidentiality, integrity, or availability of digital systems*
- *Purpose - to reduce and eliminate the possibility of cyberattacks and data breaches*
- *Cyber Risk - the potential for loss, damage, or disruption to an organization's digital systems, data, or operations due to cyber threats or vulnerabilities being exploited*

Cybersecurity Risk Management - Prerequisites

- *Identification and management of cyber security assets*
- *Defining and understanding the business processes*
- *Identifying threats*
- *Identifying vulnerabilities*

Cybersecurity Risk Management Cycle

- *Identify Cybersecurity Risks (Cybersecurity Risk register)*
- *Assess Cybersecurity Risks (threat x vulnerability x impact)*
- *Prioritize Cybersecurity Risks*
- *Treat Cybersecurity Risks (avoid, transfer, mitigate, accept)*
- *Monitor & Review Cybersecurity Risk register*
- *Communicate and report*

Additional recommendations

- *Regulatory requirements*
- *Automatic tools for risk management*
- Artificial Intelligence
- *Dedicated department for Cybersecurity Risk Management*
- *Trained cyber security professionals*
- *Strategies and procedures for Cybersecurity Risk Managements*
- *Cybersecurity Risk Management as part of the organization's overall Risk Management Strategy*

Traditional vs. Risk Based Cybersecurity

Aspect	Traditional Cybersecurity	Cybersecurity Risk Management
Focus	Technology and threat prevention	Business impact and risk prioritization
Goal	Block all threats; achieve maximum protection	Manage risk to acceptable levels; balance cost and impact
Approach	Reactive (responds to attacks or vulnerabilities)	Proactive and strategic (assesses and mitigates potential risk)
Scope	Primarily IT and technical systems	Organization-wide (IT, legal, business, compliance)
Resource Allocation	Tries to secure everything equally	Allocates resources based on risk severity and value of assets
Success Measurement	Number of threats blocked or vulnerabilities patched	Reduction in risk exposure and improved resilience

Conclusions

- *A structured and strong Cybersecurity Risk Management process is essential*
- *Supports informed decision making, aligned with business objectives and risk tolerance*
- *Effective cybersecurity risk management is imperative for survival in today's digital world*
- *Risk-based cybersecurity moves security from being just an IT issue to a business enabler*
- *Not a one-time task—it's a continuous, evolving process*
- *Protect Sensitive Data and Business Continuity, Build Trust with Customers and Partners, Cultivate proactive culture*

You cannot eliminate all threats,

but with strong risk management,

you can control risks

by making informed decisions, minimize impact and protect what matters most.

Thank You!

nadica.josifovski@aec.mk