From Overwhelmed to In Control of Cyber Risk

By Emelie Ekholm, Senior Insurance & Risk Management Leader

Across industries, one pattern is unmistakable, cyber-related risks dominate risk registers. Whether labelled Cybersecurity, Information Security, Digital Disruption, IT & Cyber Risks, or Cyber & OT Security, nearly every company in their risk reports shows cyber risk as one of its top strategic and operational exposures.

This trend is not accidental. As organizations digitize operations, connect factories, adopt AI and integrate cloud services, the attack surface continue to expand. Cyber incidents no longer threaten only data, they threaten production continuity, physical assets, safety systems and the ability to execute strategy.

This article highlights the most common cyber risks, the controls used to manage them and practical tips to help organizations stay proactive, while also linking these efforts to standard cyber insurance coverage.

Why Cyber Risk Dominates Modern Risk Registers

Across companies cyber risk appears repeatedly because it affects:

- Strategic execution (digital transformation, AI adoption, customer trust)
- Operational continuity (production lines, logistics, connected products)
- Compliance (NIS2, data protection, industry regulations)
- Financial performance (business interruption, remediation costs, fines)
- Reputation (loss of customer trust, brand damage)

This consistency across companies and industries shows that cyber risk is not a niche IT issue, it is a core enterprise risk.

Common Mitigating Actions & Controls

Across industries, organizations use largely the same cyber controls, grouped into five areas:

1. Governance & Frameworks

Most rely on structured programs aligned with NIST, ISO 27001 or NIS2 to manage cyber risk across identification, protection, detection, response and recovery.

2. Technical Controls

Common measures include network segmentation, system hardening, patch management, vulnerability remediation, secure coding, IAM, MFA and EDR/XDR tools to reduce the attack surface (see footnote).

3. Monitoring & Detection

Companies use continuous monitoring, SIEM/IDS/EDR, logging, device discovery and IT/OT traffic monitoring to detect issues early.

4. Human-Factor Controls

Training, phishing tests, penetration testing, clear responsibilities and vendor requirements address human behaviour.

5. Business Continuity & Resilience

Incident response plans, recovery testing, backups, supplier continuity and OT/ICS resilience programs help maintain operations during cyber events.

A Practical Boost to Your Cyber Program

For organizations wanting clear, practical support, FM's publicly available Data Sheet on Industrial Control Systems, is an excellent complement to existing cyber controls. It provides engineering-based, actionable guidance, especially valuable for factories, automation, robotics and connected production lines. The data sheet may be helpful for teams to validate, refine or strengthen their current mitigating actions.

Area	Focus	Outcome
OT/ICS Security	Segment IT/OT, secure remote access, monitor networks and validate patches.	**Protect production and connected assets.**
Cyber Governance	Use NIST/ISO 27001 and align cyber risk with enterprise risk.	**Enable consistent risk management.**
Human Risk	Train users, test phishing readiness and control vendors/media.	**Reduce behaviour-driven incidents.**
Detection & Response	Use SIEM/IDS/EDR, log access and test response plans.	**Detect and contain threats earlier.**
Resilience	Maintain tested backups, recovery targets and tabletop exercises.	**Recover faster and sustain operations.**
FMDS 7-110	Apply FM guidance to OT architecture, hardening and vendor risk.	**Strengthen practical OT/ICS controls.**

How Cyber Insurance Responds When Things Go Wrong

Cyber insurance is closely tied to the real-world scenarios that appear in most cyber risk registers. Policies are typically triggered by four major events: data breaches, ransomware attacks, business email compromise/social engineering and cyber-driven business interruption. These incidents can lead to both direct costs for the insured and claims from external parties.

When activated, cyber insurance typically covers a wide range of costs, including forensic investigation, legal counsel, notifications, credit monitoring, crisis communications, call-center support, ransom negotiation and payment, system restoration, lost income, extra expenses and vendor-related outages. It could also cover third-party costs, such as customer lawsuits, regulatory penalties and PCI (Payment Card Industry) liability.

This combination makes cyber insurance a practical financial safety net that aligns closely with the risk scenarios many organizations face today.

Conclusion and Key Takeaways

- Cyber risk is a core enterprise risk, not an IT-only issue as it affects strategy, operations, compliance, finances and reputation.
- Most organizations already have a foundation, but consistency and maturity vary.

- Five control areas matter most: governance, technical controls, monitoring, human behaviour and resilience.
- FM's ICS Data Sheet is a practical complement, offering engineering-based guidance for OT/ICS environments, factories, automation and connected production lines.
- Cyber insurance aligns with real-world scenarios, providing financial protection when incidents occur.
- Proactive action reduces exposure significantly. Early detection, strong boundaries, tested recovery plans and not at least trained people, make the biggest difference.
- The goal is progress, not perfection. Continuous improvements across these areas build a more secure and resilient future.

Footnote

IAM, Identity and Access Management Processes and tools that control who can access systems, applications and data.

MFA, Multi-Factor Authentication A login method requiring two or more verification steps.

EDR, Endpoint Detection and Response Security tools that monitor endpoints (computers, servers, devices) for suspicious activity and respond automatically.

XDR, Extended Detection and Response A more advanced version of EDR that combines data from endpoints, networks, cloud systems and applications to detect threats across the entire environment.

SIEM, Security Information and Event Management A system that collects, correlates and analyses security logs from across the environment to detect threats.

IDS, Intrusion Detection System A tool that monitors network traffic for suspicious or malicious activity and alerts when potential attacks are detected.