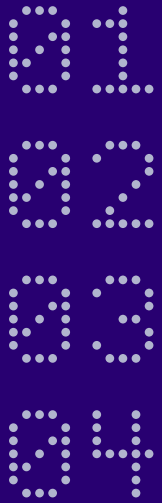
Cyber risk is business risk

How to use business knowledge and security competence in complex digital environments

14 March 2025/ Sigrun H. Bock, Head of Cybersecurity Professional Services

tietoevry

Topics of the day



01 Common understanding of the threat landscape

02 How to take responsibility for cyber risk

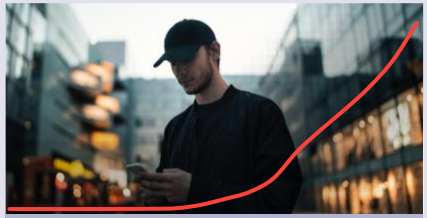
03 Market challenges and expectations

04 Control of cyber risks as competitive advantage

01

Common understanding of the threat landscape

Cyber risk affects the ability of the business to achieve its goals



Increased threat level

- The cost of cybercrime (such as Ransomware) is increasing.
- Geopolitical instability drives increased hostile activity.
- Industrial espionnage is actively used to create competetive advantages.

Regulatory compliance

- New laws and regulations to increase security in society.
- Industry standards evolve, and requirements are increasing.
- B2B customers are requiring “proof of compliance” in tenders.

Resourcing

- Skilled security resources hard to obtain and retain.
- Increased expectations, decreased budget.
- Long-term investments loosing efficiency.

Business complexity

- Digitalization of business without jeopordizing confidentiality, integrity and availabilty.
- Managing and ensuring security in a multi-sourcing scenario.

Increased innovation without reducing trust

Private and public sector are expected to be transparent and responsible, to protect customers' privacy and maintain trust as a critical societal actor

Cloud, Security, AI, Compliance

How to utilize modern digital services and technologies and secure customers information, privacy and critical information?

Automation and smarter solutions

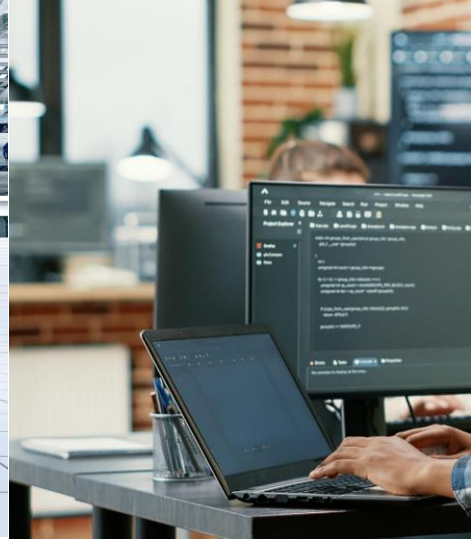
Companies in all industries are increasingly transforming their business with automated services and smarter end-user services to strengthen their competitiveness and efficiency.

Increasing amount of data

Sensitive and critical data – personal data and business critical information

Several international frameworks and certifications and the need of (re)classify information

External threats and fraud are increasing with more sophisticated AI techniques targeting sensitive data

3,4 MRD

Approx. 3.4 billion spam emails daily

90%

90% of data breaches via phishing

6 M USD

$6 billion paid in ransoms in 2021, expected to rise to $10.5 billion by 2025

30 MRD

30 billion attempted cyber attacks daily

Cyber security threat trends: phishing, crypto top the list © 2021 Cisco and/or its affiliates.

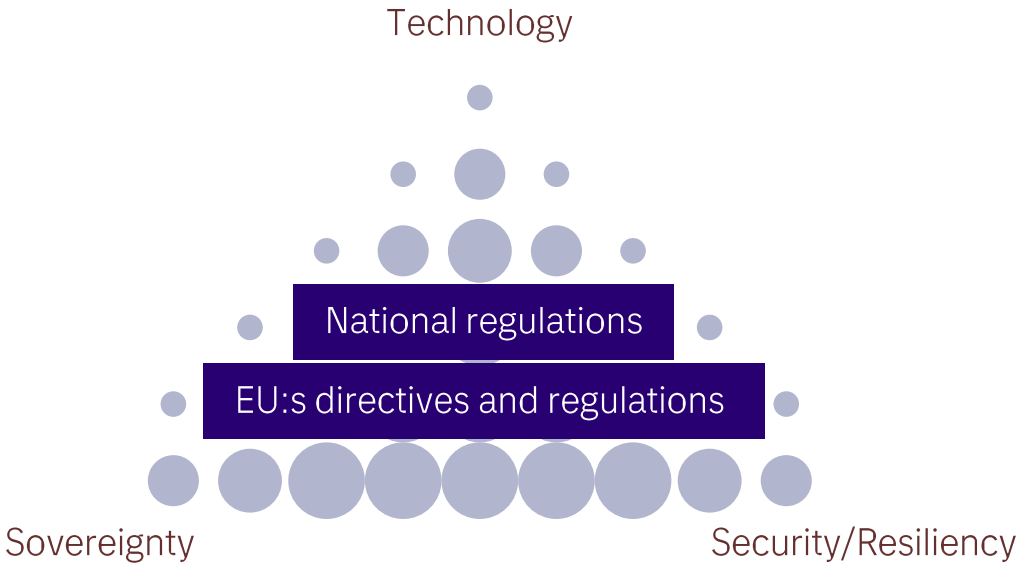
stationx.net phishing-statistics/

EU-rapport from ENISA
(European Union Agency for cybersecurity)

Microsoft 2024

How to take responsibility for cyber risk

Authorities must, through laws and regulations, give private and public businesses equal conditions for decisions that include data, technology and security.



Laws and regulations

NIS1 (2) Digitalsikkerhetsloven

- Clear definitions of "sectors" and "units"
- Risk management is management responsibility
- Requirements to reduce risk of cyber attack and minimize impact of security incidents
- Reporting requirements : 24 hrs / 72 hrs / 1 month (penalties will apply)

DORA / Sector-specific regulations*

- Risk management
- Cyber recilience
- 3-parties risk
- Autorisation of personnel
- Reporting requirements to authorities and penalties will apply

Sikkerhetsloven

- GNF and "*Skjermingsverdig informasjon*"
- Security-graded procurements
  - Graded information
  - Security clearance of personnel (grade K or higher)

Data privacy

- Schrems II; No transfer of privacy data outside EU
- !! EU EU-US Data Privacy Framework (2023)
- Possible Schrems III impact for global cloud providers (e.g. Google analytics was stopped by Schrems III)

*Lov om elektronisk kommunikasjon, Kraftberedskapsforskriften, Normen

Anchoring and ownership

Authorities (National state)

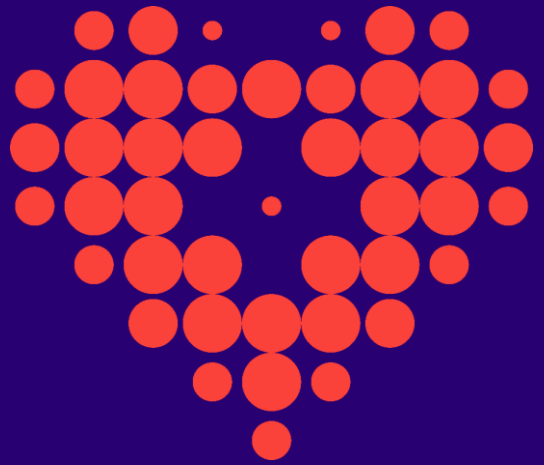
- Ownership for the implementation of legislation and compliance

Organisations (Companies)

- Integrate risk management into the business plan and determine the company's risk appetite
- Use risk management to value digital assets (data)
- Determine how the company will use its own and/or industry expertise in cybersecurity

IT-Industry (Tietoevry or others)

- Contribute to development and collaboration arenas in the society
- Support customers manage and structure security according to best practice frameworks and legal requirements
- Deliver products, services and expertise that support customers' strategic goals and day-to-day operations, as well as being part of customers' resilience in the event of major incidents and crises




Management's
understanding of risks
affects investments (time
and money) in cyber security

Risk assessments determine priority and level

Likelihood	Risk Assessment Matrix				
5	Medium/ High	Medium/ High	High	High	High
4	Low / Medium	Medium/ High	Medium/ High	High	High
3	Low / Medium	Low / Medium	Medium/ High	Medium/ High	High
2	Low	Low	Low / Medium	Low / Medium	Medium/ High
1	Low	Low	Low	Low / Medium	Medium/ High
	1	2	3	4	5
	Effect →				

WHY IS RISK HIGH ("Stop/delay in production"/ "Sensitive information falls into the hands of foreign states"/ "Broken supply-chain ")??

- Which IT resources are vulnerable and why?
- What is the cost (Consequence)?
- Who is responsible?
- When does it go from a serious incident to a crisis?

HOW TO REDUCE THE RISK OF SERIOUS SECURITY INCIDENTS (C-I-A)??

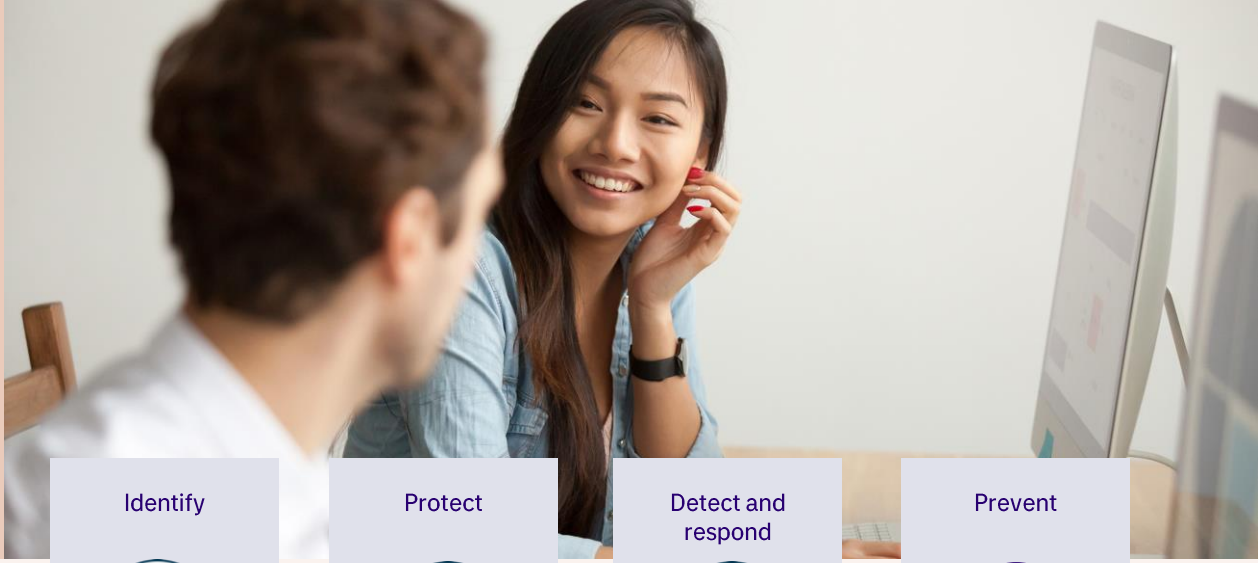
- Which IT resources are vulnerable and why?
- What is the cost (Impact)?
- Who is responsible?
- When does it go from a process activity to a serious incident?

WHICH ACTIVITIES SHOULD BE INCLUDED IN THE ACTION PLAN?

- Which IT resources are vulnerable and why?
- What is the cost (Impact)?
- Who is responsible?
- When does the mitigation plan revert to an exception to the plan?

How to reduce risk for a cyber attacks?

It is about building in effective controls at all stages. Information security can be compared to a puzzle



The pieces of the puzzle consist of

Identify

- Perform egular risk assessments of personal data and critical data (regulatory requirements, management documents, agreements)
- Make sure to have up-to-date continuity plans and routines
- Clarify roles and responsibilities (ownership of data and processes)
- Ensure compliance between risk, IT solutions and operational processes

Protect

- Protect IT equipment with the best security products and solutions on the market
- Test infrastructure and systems regularly
- Effective incident management
- Think that safety culture is fresh, and follow up measures with campaigns, testing and audits

Detect and respond

Prevent

Market challenges and expectations

How can we use security competence in the best way?

- Implementing right level of security controls to safeguard infrastructure and solutions is all about understand the business risk and how the threat landscape could impact the digital business values that needs to be protected.
- Strengthen governance, risk and controls in technical infrastructure, in operational procedures and culture.
- High adoption of new technology is embraced in every business' strategy. The view of regulation can be seen as an obstacle for enabling new technology or as safeguaring of individuals rights, fair competition or protection of the society.
- Risk management is key to utilize cloud solutions, artifical intelligence and sensor technology to provide services to the citizens without compromising privacy.
- Recruitment as well as retaining security personnel will be a continuous struggle. A shift in strategy to more agile resourcing together with vendors, partners and universities gives flexibility and capacity and reduce dependency on scare resources.
- Ensure security professionals belong to competence networks for personal development and collaborate with experts that are recognised as unique in the market

Case 1: We need to understand the customer's context and delivers expertise and services that mitigate the risk

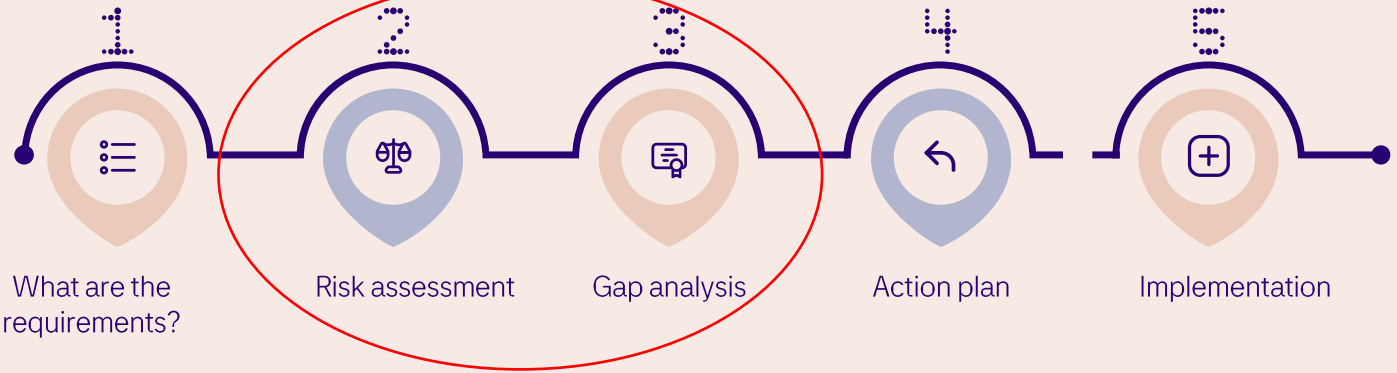
	Availability	Integrity	Confidentiality
Risk mitigation best-practise	Vulnerability Management	OWASP testing, certifications	LCM (Test) envionments*
Identities and access	Multi-factor	Zero-trust	Role-based access
Security incidents	Logging, handling, reporting	Logging, handling, reporting	Logging, handling, reporting
Compliance	Documentation, audits, standards, best practise,		

* Test instances, accessability, test data, libraries and common catalog services, integrations

04

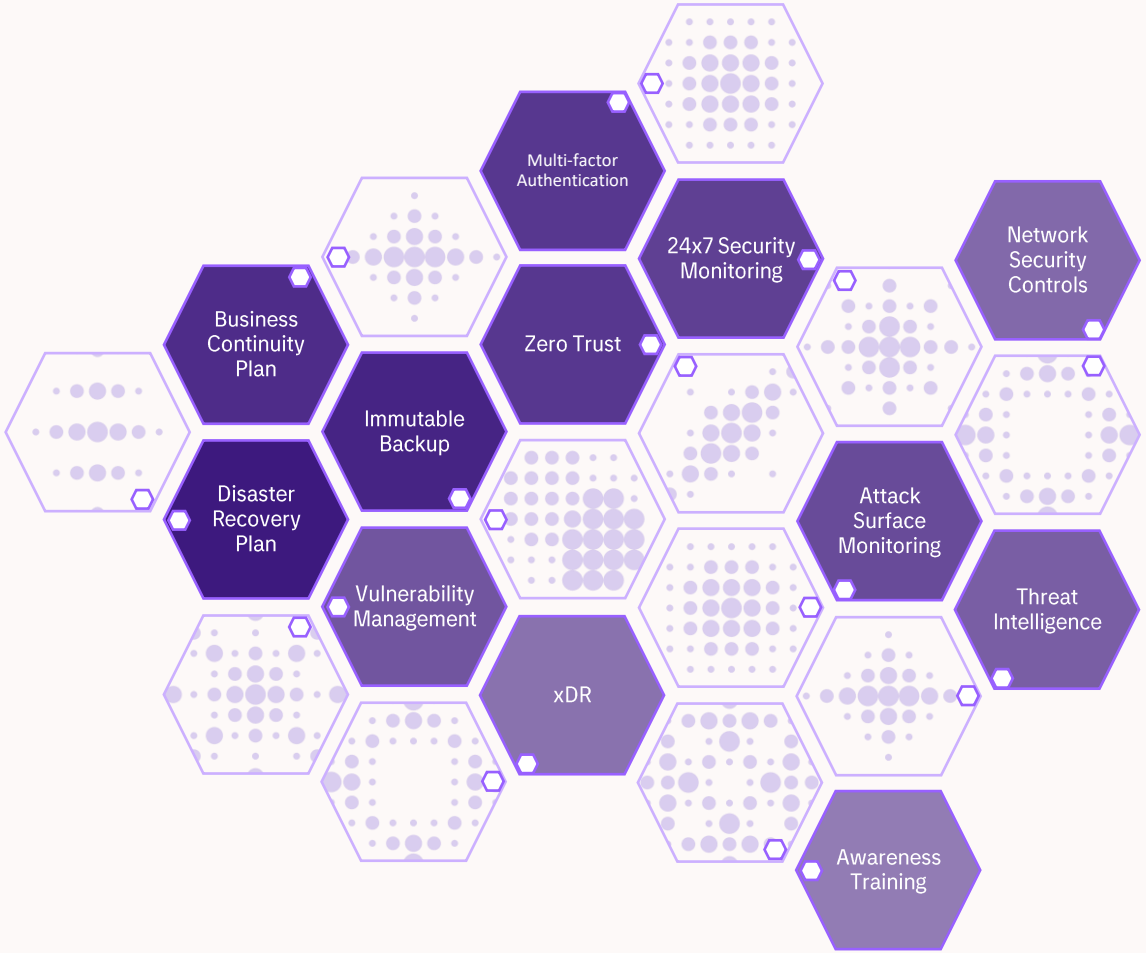
Control of cyber risks as competitive advantage

Digital resilience (“cyber resilience”) is built through 5 steps where we CAN’T skip 2 and 3!



Riskprogram for digital resilience

- With a risk-based approach, we accept that it is not possible to fully protect against ransomware, BUT we can manage the risk by implementing activities to minimize the likelihood of an attack, and by implementing activities to minimize the impact of an attack
- Based on known characteristics of ransomware attacks, these are some security measures that can help reduce the risk. These are often useful for other types of cyber threats as well
- Always consider cost-benefit, prioritize by risk and always ask the question "Why"!



Effective IT controls that create competitive advantages and meet new regulatory requirements

Everything is infrastructure and potential attach surfaces.

- Enable holistic risk management for all IT development and investments
- Continuosly scan and test every asset
- Install immutable Backup
- Perform attack surface monitoring

Ensure total autonomy.

- Build Zero trust into applications and transactions
- Build in access control in application Life cycle

Agile software development built on best practice security standards

- Build in OWASP top 10 controls
- Perform automated testing
- Implement feedback –loops
- involve 3.party auditors

Operational processes must always be prioritized

- Classify incidents and follow incident management
- Collaborate with 3rd parties
- Report on time
- Perform continuity tests regularly
- Ensure clarity in the contract (RASCI for all processes)

Questions?

tietoevry

Please contact me for more information

Sigrun Hansen Bock
Head of Cybersecurity Professional Services
Sigrun.bock@tietoevry.com

tietoevry