DReSC: Digital Resilience in Supply Chains

Abhishta
Associate Professor
Cyber Security Risk Management
University of Twente

TKI DINALOG
Dutch Institute for Advanced Logistics

UNIVERSITY OF TWENTE.

TU/e JADS Jheronimus Academy of Data Science

Topsector Logistiek

Security to Resilience

MAERSK MARKETS PEOPLE HARDWARE INDUSTRIES INVESTOR RELATIONS THE MAERSK GROUP

Maersk IT systems are down

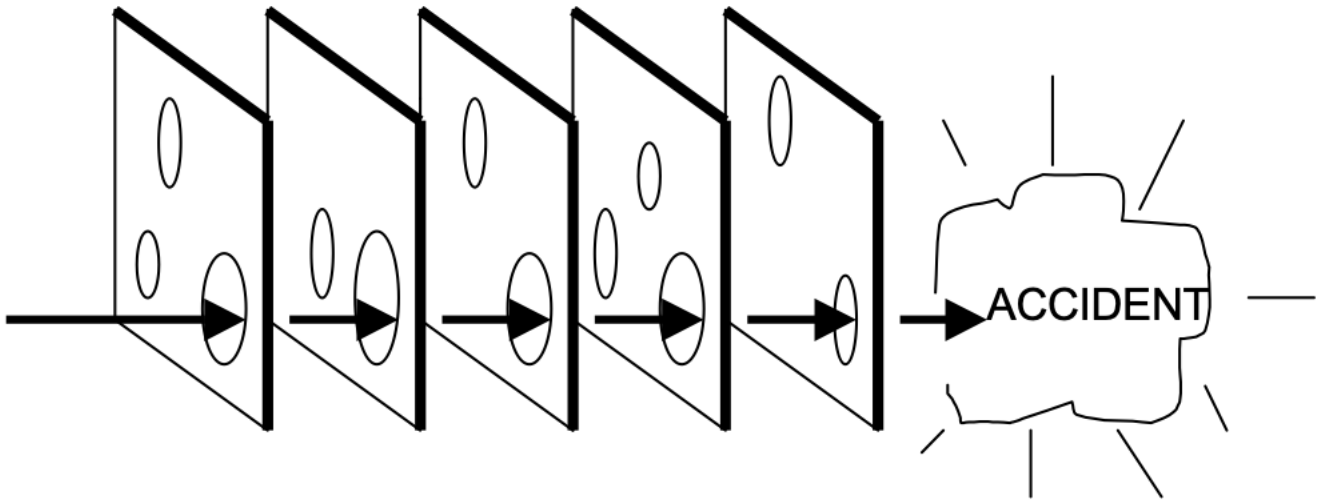
We can confirm that Maersk IT systems are down across multiple sites and business units due to a cyber attack. We continue to assess the situation. The safety of our employees, our operations and customer's business is our top priority. We will update when we have more information.

Follow our Twitter feed for more information.

Read the post

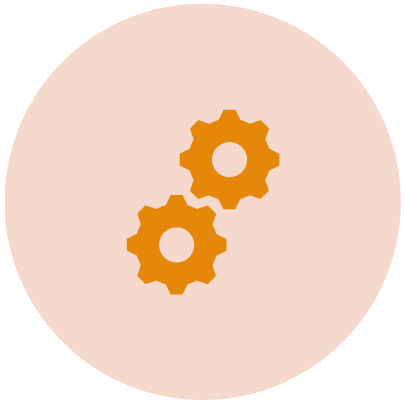
AI Generated

Swiss Cheese Model



TKI DINALOG
Dutch Institute for Advanced Logistics

What we need to build resilience?



TRANSPARENT
PROCESSES AND SYSTEMS

MONITORING

PLAN OF ACTION

TKI DINALOG
Dutch Institute for Advanced Logistics

NIS2 in brief

- Applies to essential and important entities across sectors like logistics, energy, health, finance and digital infrastructure.
- Requires cybersecurity policies, incident response plans, supply chain security, and encryption standards.
- Major incidents must be reported within 24 hours, with follow-ups and final impact assessments.
- Company leadership is directly responsible for compliance and must undergo cybersecurity training.
- Non-compliance can lead to fines of up to €10 million or 2% of global annual turnover.

TKI DINALOG
Dutch Institute for Advanced Logistics

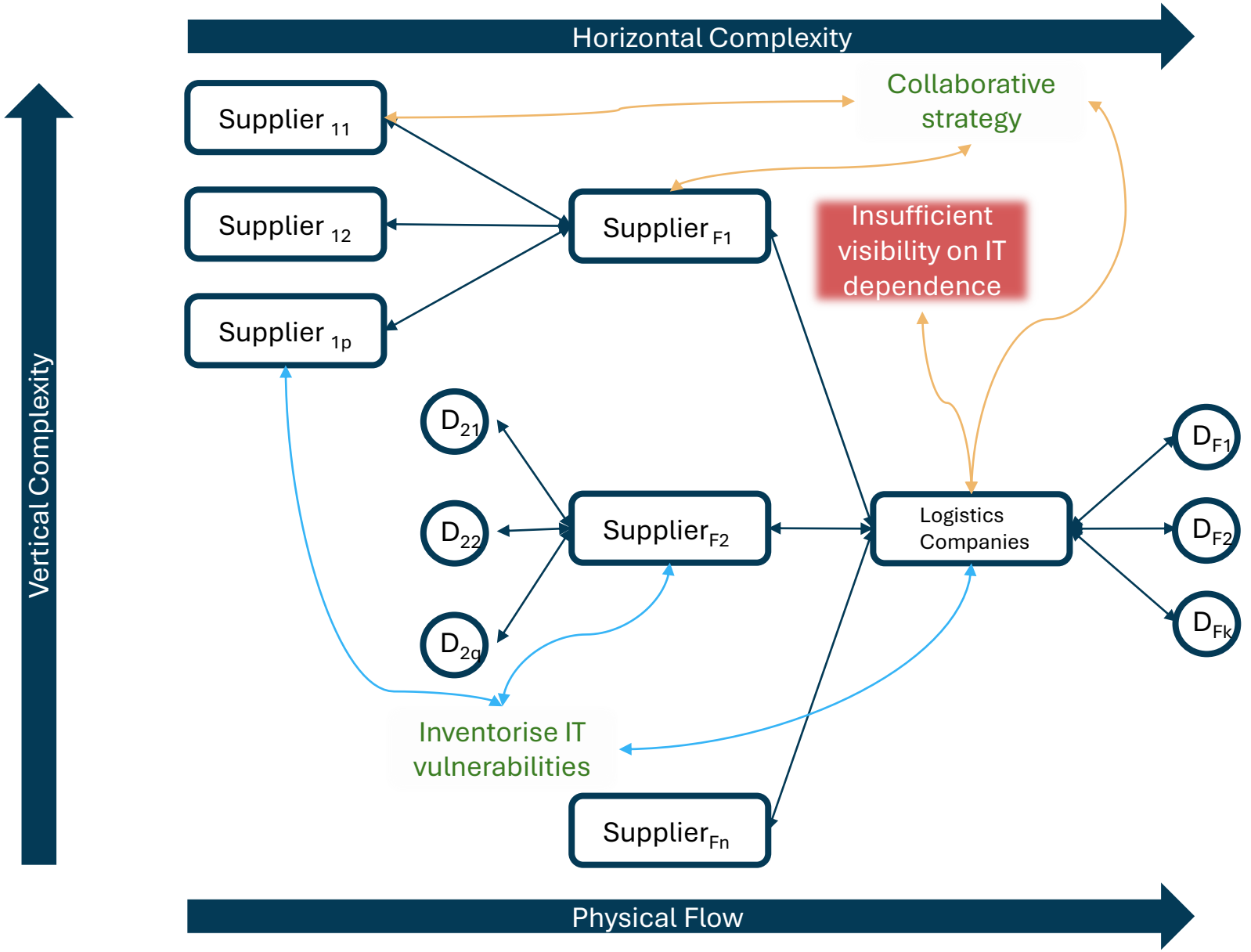
Popular Security Standards

ISO 27001

- **Risk-Based Framework**: Identify, assess, and treat information security risks using a structured, repeatable methodology.
- **Control Implementation**: Apply security controls from ISO 27001 Annex A, supported by documented policies and procedures.
- **Continuous Improvement**: Monitor, audit, and review the ISMS regularly to enhance effectiveness and respond to changes.

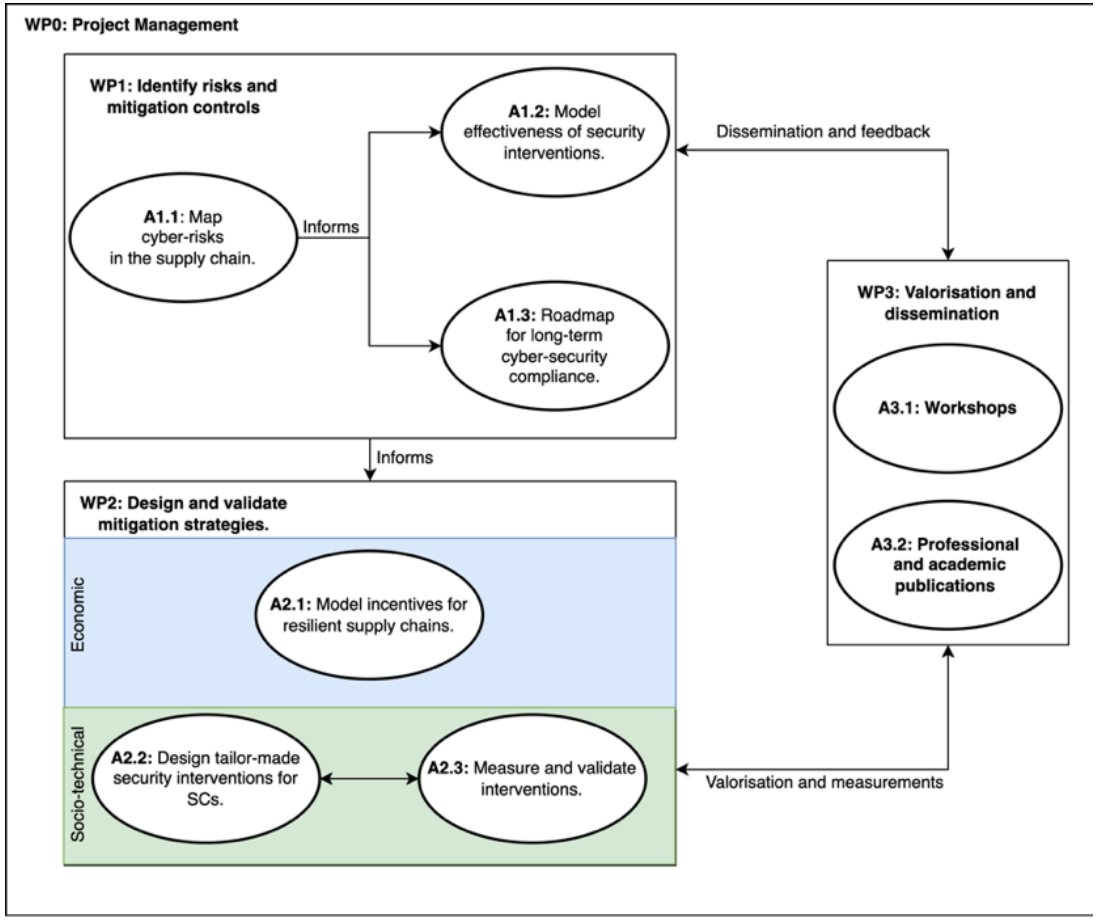
NIST CSF 2.0

- **Govern & Identify**: Define cybersecurity roles, responsibilities, and risks across assets, systems, and supply chains.
- **Protect & Detect**: Implement safeguards (e.g., access control, training) and monitor for anomalies or threats in real time.
- **Respond & Recover**: Act on incidents with structured response plans and restore operations while learning from disruptions.


Horizontal Complexity
Vertical Complexity
Supplier 11
Supplier 12
Supplier 1p
Supplier F1
Collaborative strategy
Insufficient visibility on IT dependence
D21
D22
D2q
SupplierF2
Logistics Companies
DF1
DF2
DFk
Inventorise IT vulnerabilities
SupplierFn
Physical Flow

TKI DINALOG
Dutch Institute for Advanced Logistics

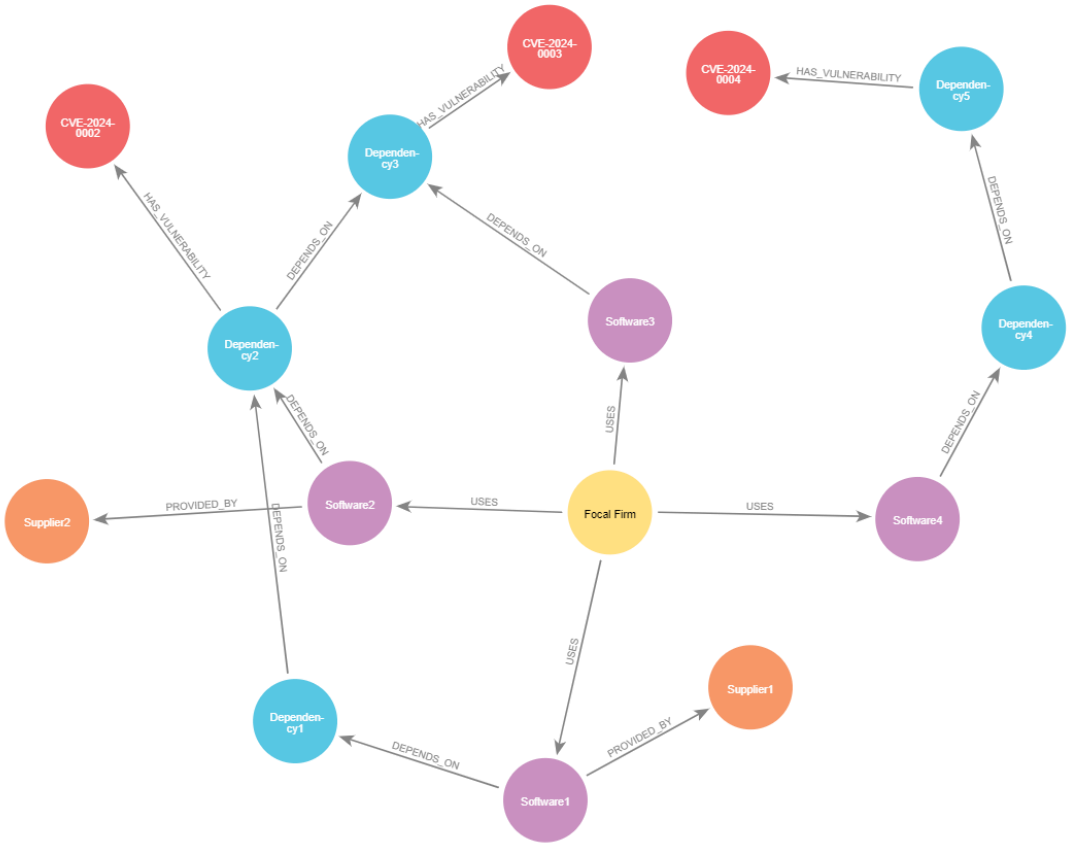
Our approach

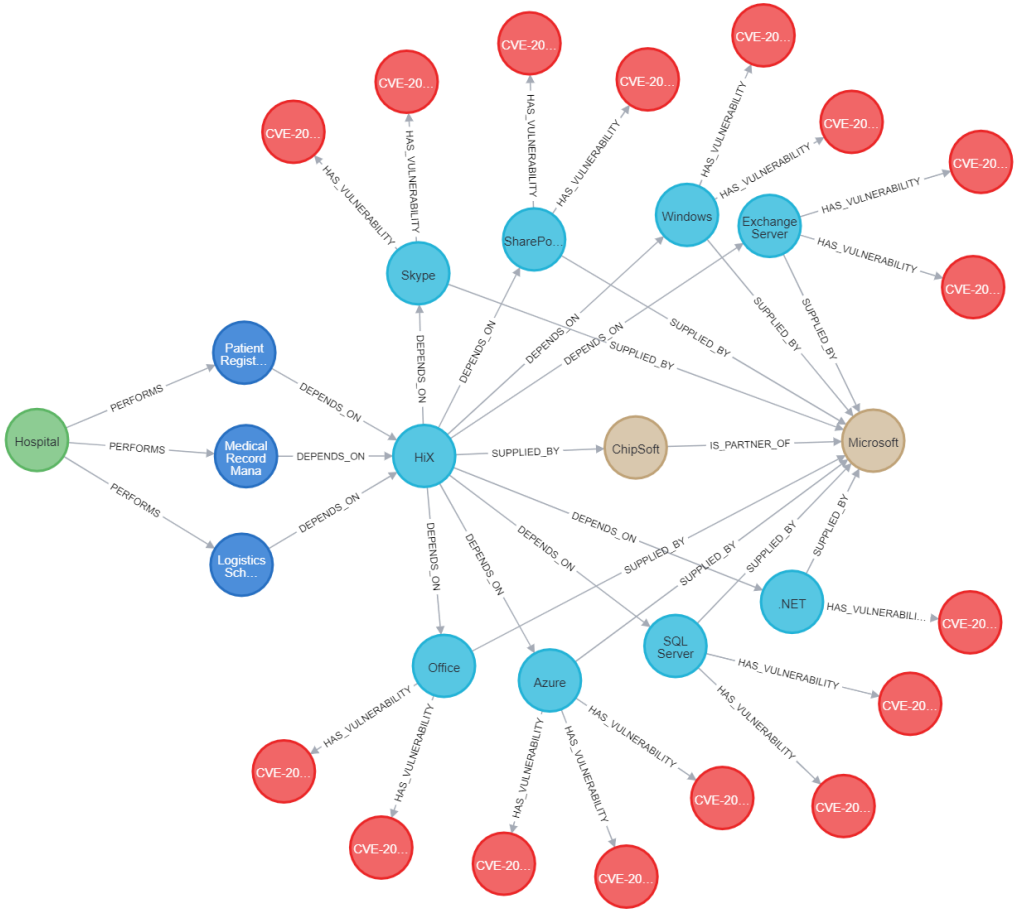


- Address both **technical and non-technical** cybersecurity risks.
- Align **actions to strategy**, and embed both into organizational **culture**.
- Use **continuous feedback loops** from real-world practice to improve.
- Prioritize by resolving **known dependencies** and **existing risks** first.

TKI DINALOG
Dutch Institute for Advanced Logistics

Dependency to vulnerability mapping





TKI DINALOG
Dutch Institute for Advanced Logistics

Using Knowledge Graphs for Role-Based Cybersecurity Training

Building tailored training for real-world security challenges

System Mapping Process

We identify critical business processes and map software dependencies to create a comprehensive view of the digital ecosystem.

- Map critical workflows
- Document dependencies
- Identify vulnerabilities

Role-Based Security Training

Our approach links vulnerabilities to specific roles and creates training content tailored to each department's needs.

- Connect systems to roles
- Build knowledge graph
- Create targeted training

Behavioral Economics Integration

Security decisions are affected by cognitive biases and real-world pressures, like staff delaying updates due to time constraints.

- Change behavior patterns
- Reduce security fatigue
- Address decay over time

Try it out!

dresc.nl

Any Questions

s.abhishta@utwente.nl

https://abhishta.org