COMET

Competence Centers for
Excellent Technologies

Supply Chain and Cyber-Resilience

Stefan Jakoubi
SBA Research

Bundesministerium Verkehr, Innovation und Technologie
Bundesministerium Digitalisierung und Wirtschaftsstandort
FFG Forschung wirkt.
wirtschaftsagentur wien Ein Fonds der Stadt Wien
FWF Der Wissenschaftsfonds.
netidee OPEN INNOVATIONS

SBA Research, © 2020

The creation of **VALUE**

usually requires a **NEED**

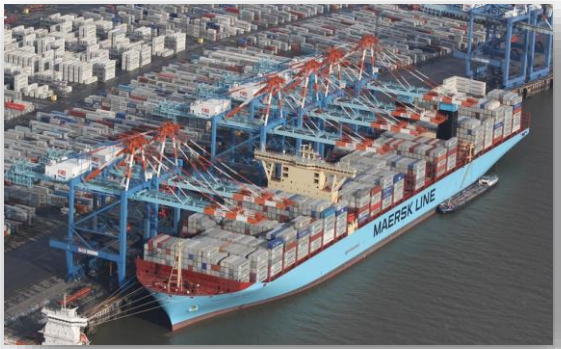
that is created by a **PROBLEM**

The Problem?

2010

Very Low probability
High impact

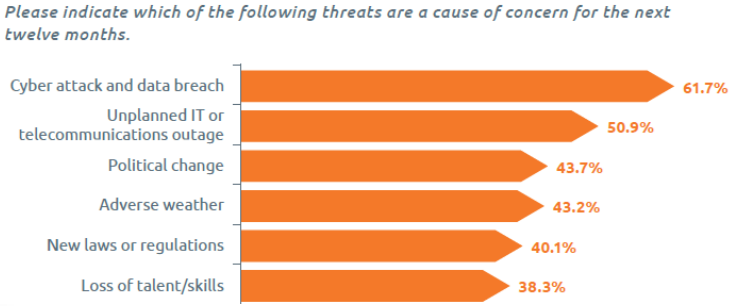
Eyjafjallajökull
(Iceland)



2017

High probability
High impact

Maersk only collateral damage…
… of 10 days offline
… approx. € 300 Mio. damage

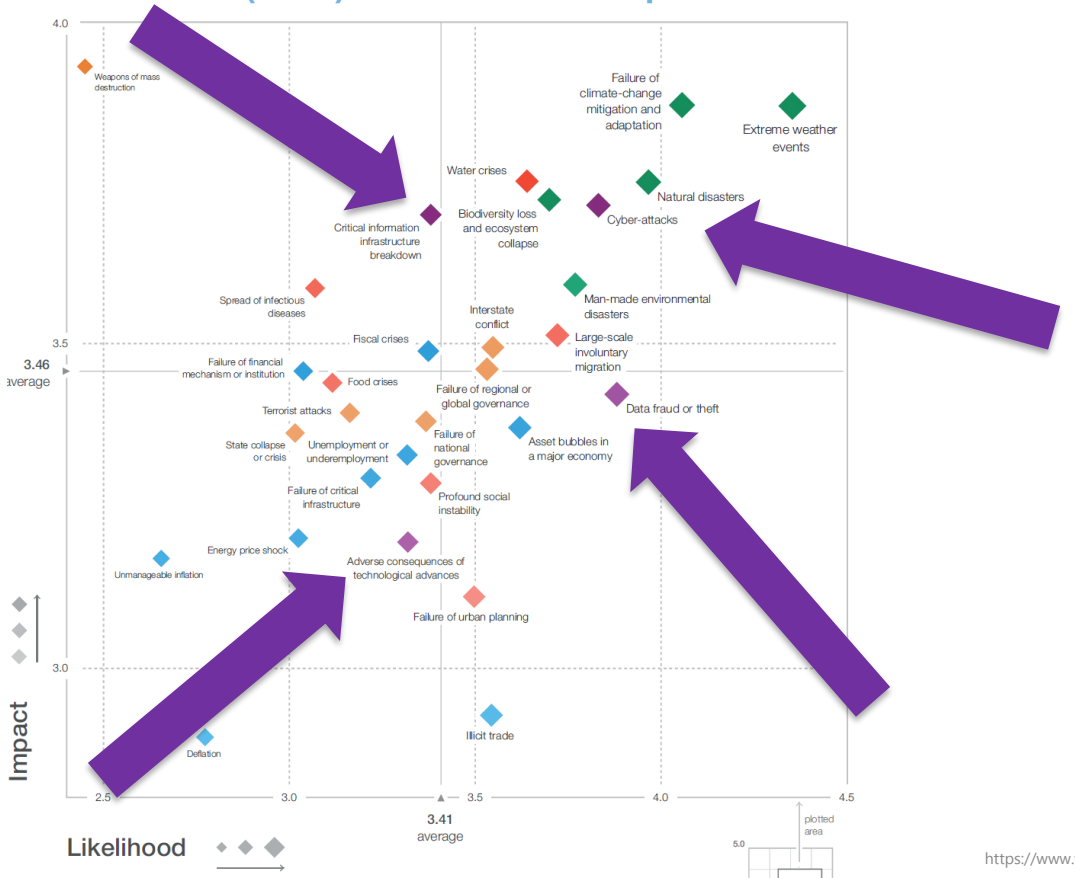


Expectation 2020+

https://www.thebci.org/resource/bci-supply-chain-resilience-report-2019.html

The Evangelists are Shouting

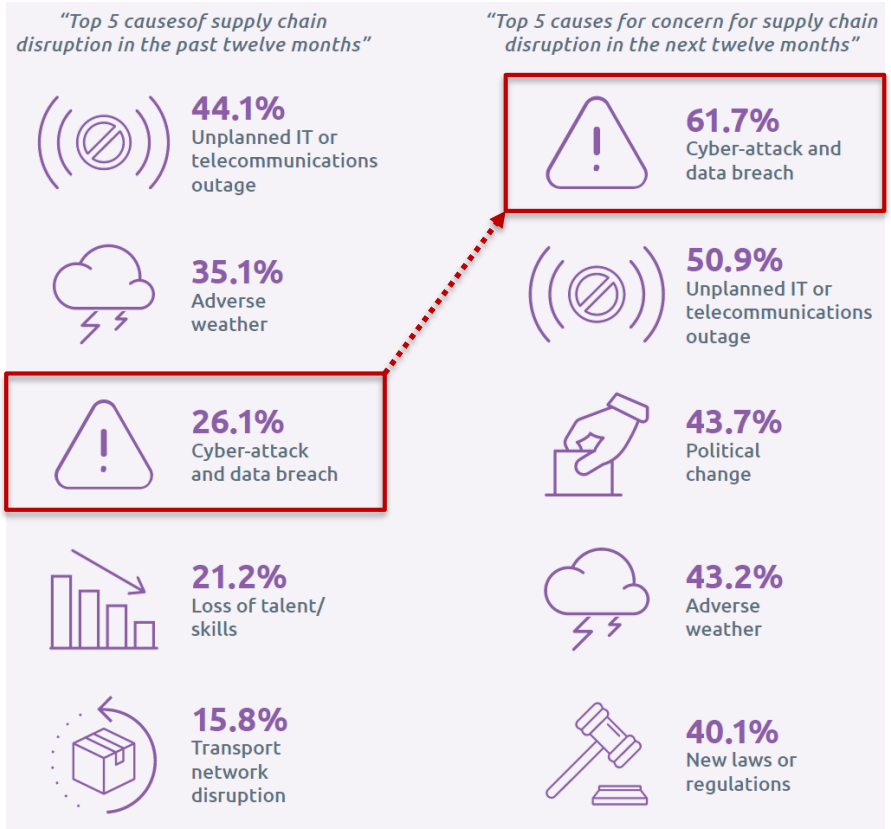
World Economic Forum (WEF): Global Risk Report 2019



https://www.weforum.org/reports/the-global-risks-report-2019

The Evangelists are Shouting

Business Continuity Institute (BCI): Supply Chain Resilience Report 2019



https://www.thebci.org/resource/bci-supply-chain-resilience-report-2019.html

The Evangelists are Shouting

ENISA: Threat Landscape Report 2020 :: Emerging Trends

04_ Supply chain and third party threats. The diversified supply chain that characterizes the technology industry today provides new opportunities for threat actors to take advantage of these complex systems and exploit the multiple vulnerabilities introduced by a heterogeneous ecosystem of third party providers.[16]

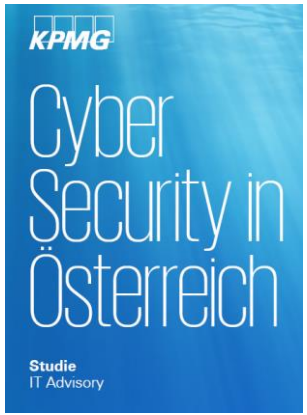
Also **Development, Provision and Maintenance** of digital goods and services:

- Dependence on (managed) service providers supporting my service
- Usage of 3rd party software libraries (special focus on open source reliability)
- Interconnection in the course of OT digitalization (e.g. predictive maintenance)
- …

https://www.enisa.europa.eu/publications/emerging-trends

Adoption By Companies?

Very low – at least the trust perception



Only **8% of companies have trust in security measures of their suppliers** and cloud-providers.

… while **only 19% invest in reducing 3rd party risks**.

Security still has to fight with **old (technological) debts**…

&

… while in parallel has to clean-up behind the **enormous speed-up by „agile & digitalization“** programs.

Challenges?

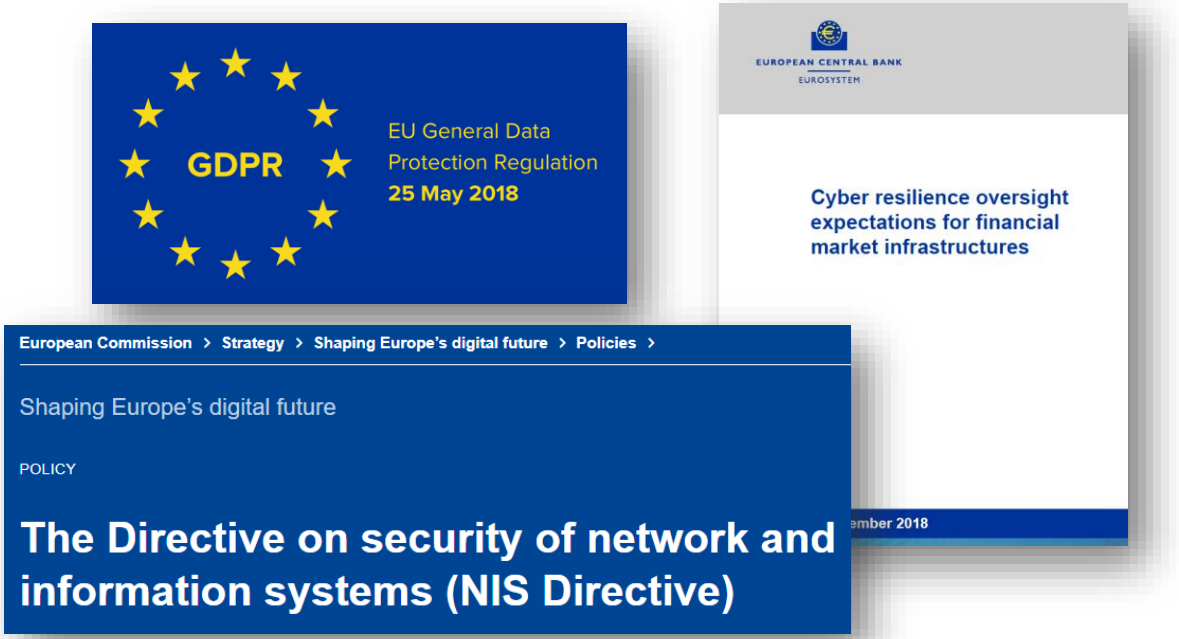
...theoretically, if everybody within the supply chain would do it's job...

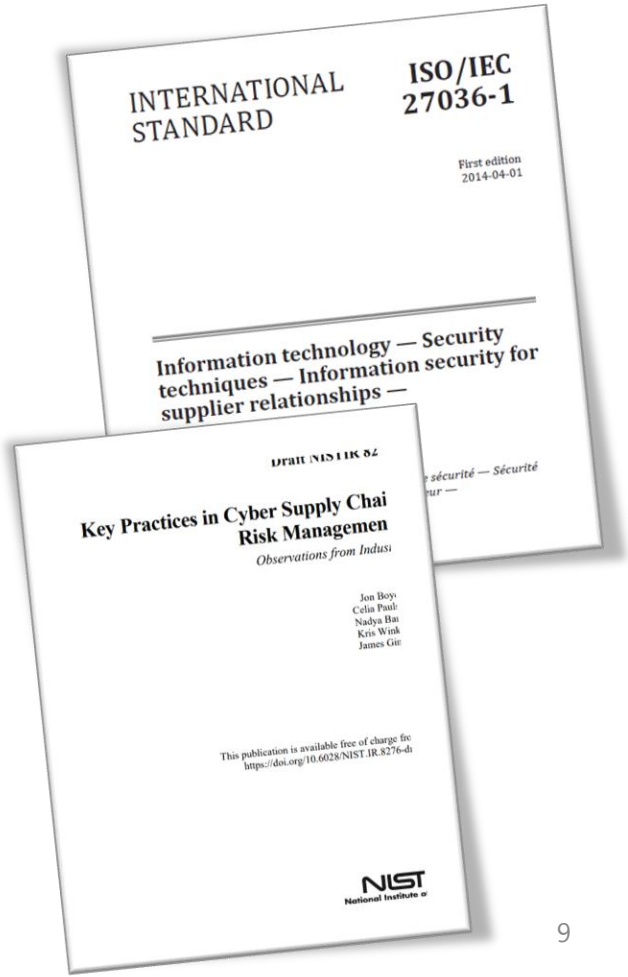
- **Cost**-Optimization
  - Standardization („Monocultures")
- Agile & Digitalization **Speed-up**
  - Cloud-Shift ("Outsourcing")
- Skill/Resource-**Shortage**
  - Outsourcing & Automation ("AI")

Research required to understand the impacts on resilience!

Regulators/Standards

Strengthen importance of 3rd party considerations





Observation

Studies & Reports, Conferences & Peer Groups, Market

1. **No clear/dedicated responsibility** = nobody in the driving seat
2. **No dedicated risk management domain** = lack of data for decision makers
3. **No x-tier supply chain cyber risk visibility** – if ever, than critical tier-1
4. **Reliance on contracts** – might support claims, won't rescue me
5. **Summit-Up: still not on the "due care agenda"** = lack of mgmt. awareness

Disclaimer: might not be true for regulated sectors

The Value?

„Flip the observation“

What can I do First Tomorrow?

For different levels of budget / maturity

- Embed „Supply-Chain-Cyber-Resilience“ into **Enterprise Risk Management**
- Ensure **3 lines of defense**
  1. Establish management responsibility
  2. Establish 3rd party risk management (keyword: integrated risk management)
  3. Establish (internal) audit function
- **Security incident monitoring** of critical suppliers

- Better visibility via **3rd party risk management tooling** (“better than nothing”)
- Review **insurance landscape** whether cyber risks are adequately considered
- (Outsource) **Supplier audits**
- Strengthen **incident response capabilities**

- **Identify (internal) responsibilities** and bring them together
- **Analyze critical suppliers** and address cyber security risks & posture
- Investigate **sensitive data flow** (“crown jewels”)
- Design **self-assessment questionnaire**; inclusion into procurement and acquisition processes

The creation of **VALUE**

requires a **CYBER-RESILIENT** supply chain

that is threatened by a lack of **AWARENESS**

Competence Centers for
Excellent Technologies

Stefan Jakoubi

Head of Professional Services / CISO

CISA, ISO27001 Lead Auditor & Implementer, AMBCI

SBA Research gGmbH

Floragasse 7, 1040 Wien

+43 660 5 10 20 40

sjakoubi@sba-research.org

Bundesministerium Verkehr, Innovation und Technologie

Bundesministerium Digitalisierung und Wirtschaftsstandort

FFG Forschung wirkt.

wirtschaftsagentur wien Ein Fonds der Stadt Wien

FWF Der Wissenschaftsfonds.

netidee OPEN INNOVATIONS