The road to resilience

Managing cyber risks

Einari Kisel – 23. February 2017 - Brussels

Table of Contents

Cyber risks: a priority for OECD countries

Cyber threats are among energy leaders' top uncertainty issues in **Europe** and **North America**

Key Findings of the report "The road to resilience: Managing cyber risks"

Available at:
www.worldenergy.org/publications

Key Findings

Interconnection and digitalisation increase risk

- Cyber risks today are growing in terms of both their **sophistication** and the **frequency of attacks**

- The **increasing interconnection and digitalisation** of the energy sector **continues to improve efficiencies** but comes with associated **increased vulnerabilities** and increases the complexities of the cyber risk management

Key Findings
Physical assets at risk

WORLD ENERGY COUNCIL

- Cyber attacks on energy infrastructure have the potential to **cross from the cyber realm to the physical world** if a cyber attacker were able to create a massive operational failure of an energy asset.

- Large centralised infrastructures are particularly at risk due to the **potential "domino" damage** that an attack on a nuclear, coal, or oil plant could cause.

Key Findings
Critical role for technology vendors

- **Technology vendors** can play a **critical role** in furthering, or hindering, the resilience of energy infrastructures.

- These firms must ensure that they deliver technologies that have **security standards** built into the products they are delivering.

Key Findings
Employees awareness: a key dimension

- The success of cyber-attacks very often depends on the **human failure** due to insufficient awareness of people on cyber risks at **all levels** of the organization.

- **Employees awareness** of cyber vulnerabilities must be included as **part of an effective cyber-security strategy**.

Key Findings

A core threat to business continuity

- Energy leaders are increasingly recognizing the importance of **viewing cyber-attacks as a core threat** to business continuity.

- By 2018 the oil and gas industries alone could be spending **US$1.87 billion** each year on cyber security.

Key Findings
Limited information sharing

- Although companies are increasingly recognising cyber as a core risk, there is **limited information sharing** amongst industry members and across sectors on cyber experiences.

- Improved information sharing would enable greater comprehension of the impact of cyber risks in energy companies and in the energy sector as a whole.

Key Findings

Cyber insurance market insufficiently mature

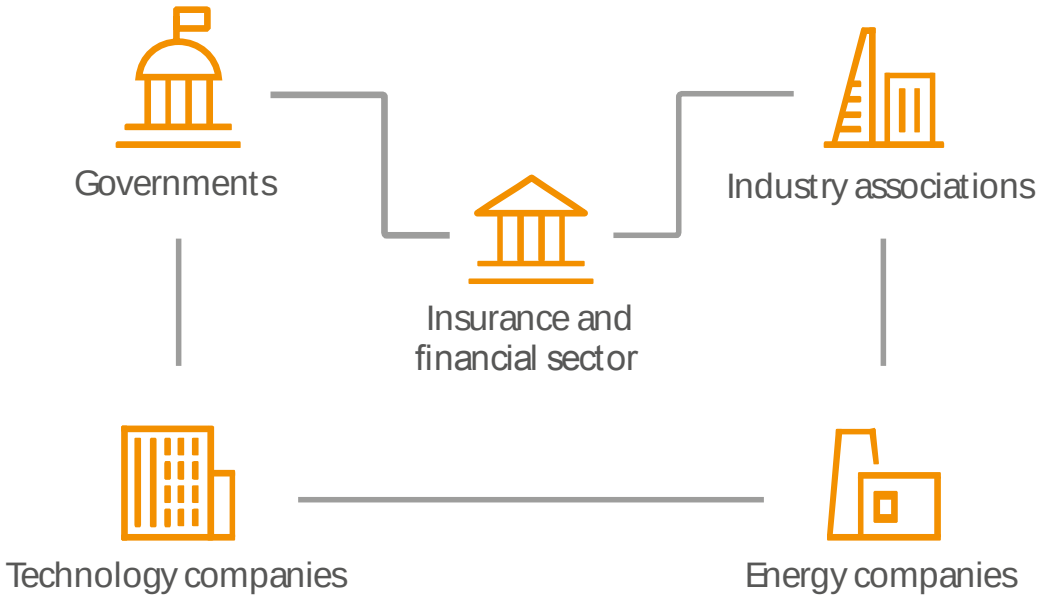
- **Cyber insurance** is one mechanism to help offset some of the potential financial losses from a cyber-attack.
- The limited historical data related to an **emerging** and **evolving** risk like cyber currently **restricts the maturity of the cyber insurance market**.
- However, the process of applying for cyber insurance in itself often proves to be **beneficial for companies**, as it obliges them to assess their own cyber practices.

Recommendations to stakeholders

Recommendations

All stakeholders must work together

1. **Technical and human factors**
2. **Information sharing on cyber risks**
3. **Risk assessment and quantification**
4. **Developing standards and best practices**



Recommendations
Energy companies

- Must effectively **assess** and **understand** company-specific cyber risks and **build** strong **technical** and **human** resilience strategies.
- Must **increase awareness** among **other energy stakeholders** to ensure that the broader energy community is included in resilience measures.
- Industry associations must support and stimulate **information sharing** and the adoption of **best practices**, conduct **peer evaluations**, and help the sector develop a robust and active cyber-aware culture.

Recommendations
Governments

- Must **support** strong responses from companies to cyber risks by stimulating the **introduction of standards** or imposing **dedicated regulations**.

- Governments must **support information sharing** across countries, sectors and within the industry and **improve international cooperation** on cyber security frameworks.

Recommendations
Insurance and financial sector

- Must **adapt coverage** to meet the ongoing evolution of cyber risk.
- Must **monitor** cyber risks covered within existing insurance products, **adapt** where necessary and **focus** on managing newly arising and changing accumulation risks
- Must **work with the industry** to improve awareness of cyber insurance products, support the energy industry in determining and collating critical cyber risk data and further develop the cyber insurance market.
- Must **respond to evolving cyber regulation** needs.

Conclusions

Increasing resilience is no longer an option – it is a must

WORLD ENERGY COUNCIL

- Cyber risks today are **growing in terms** of both their **sophistication** and the **frequency** of attacks
- Evolving from prevention of cyber risks to developing a **comprehensive operational strategy** is necessary
- Developing appropriate **technical measures** and **human awareness** is key
- Focusing on cyber resilience makes **business and political sense**.

Thank you

Einari Kisel

kisel@worldenergy.org