WM0824TU Deliverable 2

Group 2
Luca Morgese **5434033/s2576120**
Fazia Ghuman **4364554**
Jeffrey Steen **4641426/s1193074**
Harvey van Veltom **4350073**
Casper Kroes **4433882**

1 - Investigate what other actors can influence the security issue

Security issue: "What factors are the strategies and threats to companies in the energy industry:".
Besides the (Energy) company itself, other actors that revolve around the security issue with respect to the problem owner are

- Governments.
    - Key stakeholders in energy continuity
    - Different government policies and systems (governance) can differentiate the amount of resources for an Energy Company to access to deeper or wider levels of TI and cybersecurity as a whole [9][2]. More or less involvement of third parties into Energy cybersecurity determines different levels of strength against cyber attacks. Also depending on whether an Energy company is a country asset or not, national governments can have different incentives into supporting the security issue.
- Market actors:
    - Energy industries
        - Stakeholders because they would be the parties under attack
        - according to different market environments, Energy industries may find or not find TI outsourcing possibilities (free or premium TI providers). A wide and open market with concurring parties shall offer energy industries more advanced TI services, whereas a closed and regulated market may not host similar services (related info: [1]).
    - Other Energy Industries (consortium-factor): [2] the presence of trusts or consortia of cooperating energy industries can greatly contribute to cyber-risk preparedness and strategy against attackers - thus offering advanced threat environment shaping possibilities.
    - TI providers, both free and paid.:
      TI providers add to the overall level of knowledge of the threat environment.
      https://www.europol.europa.eu/newsroom/news/bt-joins-forces-europol-to-build-safer-cyber-space

2 - Identify the risk strategies that these actors can adopt to tackle the problem (1 point)

a. **Are there actors with different strategies? Why?**
b. **Have the strategies changed significantly over time in a way that reduces or increases risks?**

Governments risk strategy:

- Dedicate resources to securing IT infrastructure [3]
- assess criticality of Energy grid “components”,
- mandate/vision risk assessment reports for every Energy industry,
- build panel to assess Energy sector cyber risk,
- partner with ISPs to protect Energy Grid,
- design resilience capabilities for energy grid

Comprehensive view: [4]

A public-private initiative between DOE and energy industries:

- Cybersecurity Risk Information Sharing Program that aims to facilitate real-time bi-directional information sharing regarding threat information for the development of situational awareness tools
  https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity

Market actors strategies related to bringing TE awareness for (energy) industries:

- Indirectly related to the security issue as beneficiaries of energy supply
- respond to security issue with business model: provide as-useful-as-possible intelligence to energy industries.

Energy industries consortia:

- Multilateral super-party regulated partnership among Energy industries to share TI information, better shape TE and advance cyber-risk readiness (again,[2])

A - Actors have different risk management strategies as they belong to different sides of the security-issue environment. Governments have more direct power and varying interest to manage resources with respect to the security issue for individuated Energy Industries. General market actors respond with services built with a primary for-profit interest. Partner energy companies concur to a single cybersecurity front to enforce the most efficient, sector-specific and direct approach to counter cyber threats.

B - Rather than changed, strategies had recently evolved because of the relative novelty of the whole cyber setting. Risks tend to get higher as digital inter-connection and digital governance take hold, and cyber-threats become more powerful and organized [various sources]. Attack surfaces become greater, attackers become smarter, energy remains a critical societal asset. Cohesive and effective risk management strategies have to be devised by the multitude of involved actors (notes on incentives).

Select 3 actors (including the problem owner) involved in the security issue (you can draw on the previous assignment). For each one:

a. **(0.5 point) Identify one concrete countermeasure that they could take to mitigate the security issue,**
b. **(0.5 point) Analyse the distribution of costs and benefits (without quantifying) among the different actors that the deployment of the countermeasure would entail,**
c. **(1 point) Analyse whether the actors have an incentive to take the countermeasure,**
d. **(1 point) Briefly reflect on the role of externalities around this security issue.**

Three actors:

1. Specific Energy company (problem owner)
    a. Design and consider TE metrics, improve threat awareness by opportunely investing in TI resources.
    b. ROSI observations, block 2 of lectures: industry costs of cyber security - consideration on Energy Security as an asset to defend *at all costs* and which should not be part of the business model per se. Costs would target only the industry itself.
    c. They naturally have incentive to take countermeasures to protect their business as well as actually granting a reliable energy supply for the society.
    d. Benefit from externalities through Energy Companies Consortia.
2. Governments:
    a. Build a panel for national Energy Security, devise risk plans including ISPs and other stakeholders, support cybersecurity strategies
    b. Panel takes government budget to be created and run. Introduces additional layers of bureaucracy and responsibility for stakeholders. Benefit is that a coordinated strategy can align stakeholder interest, coordinating efforts from several parties for greater effectiveness.
    c. Government wants to maintain the country's infrastructure, which includes energy. Large faction of attackers are foreign, the government wants to protect borders.
    d. If more parties join the panels, more viewpoints can be considered when devising plans, resulting in a better overall performance. But by introducing more interested parties, the interests of an individual faction become less relevant to the whole.
3. Third-party Energy Companies
    a. Setup a consortium for TI and cybersecurity cooperation
    b. Institution of super-party organization to manage information and strategy sharing, costs amortized over consortium members, direct benefits.
    c. Natural incentive to better protect each own company and whole sector, normalize security profile over concurring actors leads to discard cybersecurity related competitive advantages, with consequences of sorts

d. Direct benefit from direct network effect: the more Energy companies join the consortium, the more information available to classify threat environment and setup readiness.

4. **(5 points) Identify the type of actor whose security performance is visible in the metric(s) you selected (e.g. ISPs, software vendors, countries). Note that this is not necessarily the problem owner, rather the unit of analysis in your metric.**
    1. **Identify different factors explaining (causing) the variance in the metric,**
    2. **Collect data for one or several of these factors,**
    3. **Perform a statistical analysis to explore the impact of these factors on the metric (link contains some examples and explanation).**

1: In the attack frequency per country analysis the unit of analysis are the countries (perhaps usable as proxies for their governments).
Possible causes for differences between countries are:

Factor	**Source in literature for relation**	**Source for (preferably) quantative data**
GCI	[5]	https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf
(Geo-)political rivalry	[6] [7]	
Effect size (i.e. potential damage done)	[6]	https://www.iea.org/data-and-statistics?country=WORLD&fuel=Energy%20supply&indicator=TPESbySource
Bias	None	
Real world social events	[8]	- Unsourceable because of inaccurate timestamping OTX data
Social, political, economical and cultural conflicts		https://ieeexplore.ieee.org/abstract/document/5725605?
Location (IP address)	[6] [7]	The OTX itself + a GeoIP module
Economic Impact of Cybercrime across Globe:		https://knoema.com/NLEGCC2018/economic-impa

		ct-of-cybercrime-across-globe-one-time-publication

1. **Statistical analysis to explore impact**

Ideas for quantitative analysis:

- Regression analysis to analyze cohesion between factors (Factor Analysis on top of that might provide even more insight here). For example: Build a predictive model to predict attack frequencies per country as we got them from the OTX and use any or all of the above variables to test which factors would have predictive power to predict the amount of attacks.

If we want to do it qualitatively:

1. This article investigates the cyberthreat profile for the power sector (US) on three key actors

   https://www2.deloitte.com/content/dam/insights/us/articles/4921_Managing-cyber-risk-Electric-energy/DI_Managing-cyber-risk.pdf

   another one for the US:
   https://info.publicintelligence.net/INL-CyberThreatsElectricSector.pdf

   there's a ton of info in that one.

   attacks per country and per sector in EU, but not energy specific:
   https://fronteirasxxi.pt/wp-content/uploads/2018/06/MMC-FireEye-Cyber-Risk-Report.pdf

   Economic impact of cybersec in Energy Sector

   https://www.econjournals.com/index.php/ijeep/article/view/5283

   Deloitte report on managing cyber risk in Power sector
   https://www2.deloitte.com/us/en/insights/industry/power-and-utilities/cyber-risk-electric-power-sector.html

[1] B. Farrand and H. Carrapico, 'Blurring Public and Private: Cybersecurity in the Age of

Regulatory Capitalism', in *Security Privatization*, O. Bures and H. Carrapico, Eds. Cham: Springer International Publishing, 2018, pp. 197–217.
[2] 'Energy Sector Cybersecurity Preparedness', *Energy.gov*. https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity (accessed Oct. 05, 2020).
[3] 'National Cybersecurity Strategies', *ENISA*. https://www.enisa.europa.eu/topics/national-cyber-security-strategies (accessed Oct. 05, 2020).
[4] D. Healey, S. Meckler, U. Antia, and E. Cottle, 'Cyber Security Strategy for the Energy Sector', European Parliament, Directorate General for Internal Policies, Oct. 2016. [Online]. Available: http://publications.europa.eu/resource/cellar/8cf0f709-fcb9-11e6-8a35-01aa75ed71a1.0001.01/DOC_1.
[5] ITU, 'Global Cybersecurity Index 2018'. 2019, Accessed: Oct. 05, 2020. [Online]. Available: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.
[6] M. B. Line, A. Zand, G. Stringhini, and R. Kemmerer, 'Targeted attacks against industrial control systems: Is the power industry prepared?', in *Proceedings of the 2nd Workshop on Smart Energy Grid Security*, 2014, pp. 13–22.
[7] K. Vasileiou, 'Cybersecurity in the energy sector: a holistic approach', Master's Thesis, University of Piraeus, 2019.
[8] A. C. Sharma, R. A. Gandhi, W. Mahoney, W. Sousan, and Q. Zhu, 'Building a social dimensional threat model from current and historic events of cyber attacks', in *2010 IEEE Second International Conference on Social Computing*, 2010, pp. 981–986.
[9] EECSP, 'New report on Cyber Security in the Energy Sector published', *Energy - European Commission*, Mar. 03, 2017. https://ec.europa.eu/energy/news/new-report-cyber-security-energy-sector-published_en (accessed Oct. 05, 2020).

Task division

Casper Kroes: Contributed to subquestion 4 including the literature research, and contributed to proofreading.
Luca Morgese: outlined and contributed to points 1, 2 and 3 with related research.
Fazia Ghuman: Contributed to 4, general literature research for overall refinement.
Jeffrey Steen: Contributed to 1 and 3, literature research, proofreading.
Harvey van Veltom: General proofreading.