Way forward for good European cyber security rules

Vattenfall Position

December 2020

Omnipresence of Information Technologies makes electricity generation assets, grids and consumers “smarter”, leading to development of intelligent energy systems that are to cater for the energy transition today and in the decades to come. At Vattenfall we define critical staff members and assets: Technical Infrastructure (OT and IT systems), Information, Staff, Physical, Goodwill (Reputation) within our new SMS (Security Management System) that support our key processes in the business with utmost care and security for the entire supply chain.

We count that the EU policies and regulatory framework will support us at effectively operating our infrastructure in the view of cyber resilience, societal welfare and stability. We welcome the European Commission’s efforts to adopt a comprehensive regulatory framework for cyber-security both at horizontal and sectorial level. We hope that the revised framework will greatly contribute to harmonizing cyber maturity and resilience across the EU.

This paper sets our views on the opportunities and challenges related to adopting a good, future-proof, efficient and operational regulatory framework, taking into considerations latest discussions about the matter.

In principle, we support a risk-based approach to cyber resilience, combined with mandatory baseline security measures, taking into account confidentiality, integrity, availability and traceability of data. Their implementation could be verified by technical checks, audits or IT compliance tests that we find more effective than mandatory certification of the IT security management systems (ISMS). We believe that baseline security measures will support further investment into operational IT and OT security. Checks and audits, combined with other measures addressed in this paper:

- accountability of vendors, strengthened particularly by transparency and defining basic requirements;
- improved sharing of indicators of compromise; and
- investment in cyber skills of employees.

are the way forward to increase critical infrastructure’s operators cyber resilience and accountability.

Contact person: Mikołaj Jasiak, Policy Adviser, Public and Regulatory Affairs EU

mikolaj.jasiak@vattenfall.com

Vattenfall is a European energy company with approximately 20,000 employees. For more than 100 years we have electrified industries, supplied energy to people's homes and modernized our way of living through innovation and cooperation. Our goal is to make fossil-free living possible within one generation. Everything we do and the decisions we take shall lead to this goal. This is the basis of Vattenfall’s strategy, and we advocate for a regulatory environment that makes this transition possible – in the energy sector and beyond in transport, industry etc.

VATTENFALL

Background

Tackling climate change and a transition to a low-carbon economy remains the biggest challenge of our time. It is a policy priority for the EU institutions, national governments and energy undertakings alike. For that purpose Vattenfall's mission is to enable fossil-free living within a generation by phasing out fossil fuels from energy production, growing the share of renewable energy sources, increasing electrification of transport and industry as well as increasing the share of active consumers. Energy transition goes hand in hand with digitalisation, understood as a an ever-greater availability and granularity of data and its use in optimising existing operations and development of new services. Energy systems need then to open up for more variable generation, small producers and IoT devices along the supply chain. Those trends, on the other hand, raise numerous concerns about exposure to cyberattacks, jeopardising the security of energy supply or the data privacy. The fact that energy infrastructure is a critical asset and is generally characterised by numerous interdependencies and a high level of complexity calls a for a particularly careful approach to the matter. It should be kept in mind that electricity grids are already now developed and managed in accordance with strategies and resilience towards a sudden loss of the production units or consumption in distribution grids.

Cyber security challenges at the time of energy transition

In the energy sector we identify efficient, secure and stable supply of energy services in the changing environment of more variable renewable generation and ever-increasing digitalisation as the main challenge within cyber security domain. Cyber-attacks and threats pose a challenge to the availability of energy and to the integrity of the management and distribution systems as well as data. The types of attacks range from disclosure of confidential data to the modification or destruction of it. The range of actors is broad, from state actors to criminal groups and hacktivists. Different interests lead to attacks on nearly all systems available at some point. Current situation requires then a comprehensive security protection analysis, done with consistency and precision in order to avoid unnecessary complexity and costs. For Vattenfall, all these developments and the corresponding regulation mean that we need to increase security requirements regarding business operations, procurement, technical solutions, outsourcing, staffing, information handling, or incident handling and reporting, e.g.:

- longer and more complex procurement processes, requiring approval from authorities, limitations regarding which countries that are allowed to deliver services and systems;
- increased number of staff which require vetting, restrictions on how we do outsourcing and mandatory incident reporting to the authorities;
- correct classification of significant volumes of data (and systems); which data falls under the purview of the law, and which does not, in order to avoid unnecessary encryption and limit the negative impacts on energy companies.

Recommendations

- **General remarks**

Vattenfall welcomes of the European Commission's effort to tackle cyber security at the EU level through revision of the NIS Directive as well as the ECI/CIIP Directives at the horizontal level as well as energy- specific legislation: sector-specific legislation on critical infrastructure and the network code on cyber-security. Such approach to the regulatory framework is a promise of establishing a comprehensive set of directly applicable measures, institutional environment and information-sharing aimed at spreading good practices. All entities of a certain criticality providing essential services to our society should be subject to similar EU-wide cybersecurity requirements. The European regulatory environment should then result in harmonizing the levels of maturity, resilience and cyber-security by design.

This multi-level process, however, should take into account the need for clarity, implementation feasibility, coherence and co-related timelines. In particular, given that, cyber security rules, as part of national security, are also addressed in multiple diverse acts of national law as we. **We**

would like to bring the attention of the decision-makers to ensure that definitions and concepts applied in all the revised and new legislative acts should be streamlined. The scope of each act should be clearly separable from others or, in case of co-dependencies, they should be explicitly interlinked.

Technological neutrality. The EU framework should be, as far as possible, technologically neutral in order not hinder R&D or European competitiveness. New technologies should not immediately 'rock the boat', if baseline security measures for products are applied in certain environments and combined with a certain degree of resilience.

Data specificities. The EU framework should take into account that not all data and communications have the same need of protection. Security requirements should be based upon criticality, confidentiality, integrity availability and traceability. However, misclassifications such as excessive use of 'highly confidential' category may lead to unjustified limitation to the use of data and hampering innovation.

Governance For us, as an operator of critical infrastructure, it is the most important that European information security authorities are extremely well interconnected in the area of sharing Indicators of Compromise and providing threat assessments for critical infrastructure sector. Given that, there is a limited need to have a separate EU body dealing with the same matters. We see no need to have an additional higher layer for threat assessments, compliance monitoring/audits or monitor compliance with the network code.

- **Accountability of critical infrastructure operators**

The European framework should have a risk-based, systematic approach and it should be aimed at OT security measures. Risk-based, systemic approach should be followed by an implementation phase, while some security measures (e.g. perimeter security and separation of assets, compensating security controls) could be classified as "baseline security measures", thus their implementation would not require a full risk analysis beforehand. The ISO 27000 and IEC 62443 series of standards as well as other best practices could provide a good point of reference for such measures, if complemented with some further functional technical interpretation. We find, however, that **technical checks and audits are more efficient instruments for assessing the implementation than mandatory certification regarding information security management systems (ISMS)**. It should be kept in mind, that ensuring cyber resilience requires, first and foremost, investment in OT security measures. We are concerned that certification on management systems, could result in broadening the scope and costs of the ISMS administration, and steer the focus away from the necessary operational investments. In particular, for smaller companies certification could prove too expensive. Baseline security measures, **technical checks and audits, combined with additional measures addressed in this paper, are the most effective way forward to facilitate critical infrastructure's operators accountability for secure and reliable operations.**

- **Accountability of vendors**

We are asking the decision makers to take into account that even large companies may have a relatively weak negotiating position towards vendors, while cyber resilience of their products and services is one of the key aspects of the overall operational security and cyber resilience. Operators of critical assets should have the right to choose services and products in accordance with their suitability for the intended usage and performed risk assessments. **There is a number of measures that could enable us to perform appropriate risk assessments and make it possible to select suitable products**:

Transparency It should be easier for operators of critical assets to assess the security of products and systems offered by vendors. Currently it is sometimes difficult to procure a service at the level of security desired by an operator, or services that meet the criteria desired

by an operator. Services, as defined by an operators in accordance to its risk assessment, are often offered at a higher price than the vendors' standard services. Vendors, should be then obliged to be more transparent about security performance of the offered services, their development and delivery.

Basic level of security for services and products (not certification) Currently there is no basic level of security for services and products. **A basic level of security should be required in the processes of production and delivery of products or systems along the entire supply chain**. Vendors should be also required to communicate openly about vulnerabilities of their products throughout their lifetime. A specified certification or a product assurance scheme may not be the best way forward. Challenges related to the vendors' offer remain, even though there are already existing certification schemes, which are used to a certain extent. The issue then is not that products or systems are not certified (it should be underlined that not all the new products will be certified upon development). Certified products can be also a disadvantage for non-regular exchange of components and other operational aspects.

Long-term availability of security patches There should be an obligation on vendors to provide security patches for a long term. This obligation can be balanced by appropriate SLAs regulating fees for availability of security patches. The Life Cycle Management of products by a vendor shall be open and transparent enough for the operators. This makes it possible for OES to do adequate risk assessments for procuring the right products. If the manufacturer does not (any longer) provide security updates for systems or components, there should be a transition period for the operators until these are replaced. For the further use of these assets, the operator should be obliged to implement compensatory security measures.

Standard contractual clauses Another mechanism that could support critical infrastructure operators in monitoring cyber resilience of vendors' services is contractual clauses obliging vendors to allows operators to audit vendors' activities. Currently operators miss leverage to access information on operations performed by service providers.

- **Information sharing**

The first step to ensure effective information sharing should be to increase operators' **ability to produce indicators of compromise (IoCs)** and to increase recipients' **ability to process them**. Currently, there is a high number of indicators of compromise that recipients are not able to 'consume'. National authorities could be a support to companies in pre-selecting and filtering information relevant for particular industry areas.

We would like to see a **voluntary, rather than mandatory scheme** for sharing the IoCs. A voluntary scheme, based on trust, driven by the willingness to share relevant information could be more effective than the same mechanism perceived as a compulsory compliance exercise. A scheme could be organized on a platform, where not only operators of critical infrastructure, but also national authorities can access. Should sharing the IoCs be compulsory, the sharing requirement **should not include vulnerabilities, commercial or sensitive data**.

- **Skills' building**

Last, but not least we would like to underline that cyber resilience relies on people. The European framework should facilitate **building talent and investing in people**. Given that around 20% of the post-COVID19 recovery funds are to be related to advancing digitalisation of the European economy, we would like to call upon the EU decision-makers to ensure that a part of these funds is destined at fostering digital skills in the area of cyber skills, going beyond the mere awareness of cyber security challenges.

In the area of cyber security, it is crucial that staff members have a solid understanding of interdependencies between cyber resilience and business operations, e.g. classification of data and communications, time constraints, data sharing restrictions or additional costs.