



INFRASTRUCTURE



PETRAS Briefing:
Understanding Disruptive Powers of
IoT in the Energy Sector (Power2)



How to Talk about Cybersecurity of Emerging Technologies

A Report to Board Level Executives in
the Energy Sector

Dr Ola Michalec
Bristol Cyber Security Research Group
University of Bristol



Contents

About PETRAS	3
Introduction	4
Understanding the Role of Cybersecurity in Energy Innovations	5
Three Cybersecurity Tropes that Need to Retire	7
Questions to Ask your Technical Teams	9
Questions to Ask other Board Members	9
Organisations and Initiatives to Follow	10
Further Reading	11
Acknowledgements	11

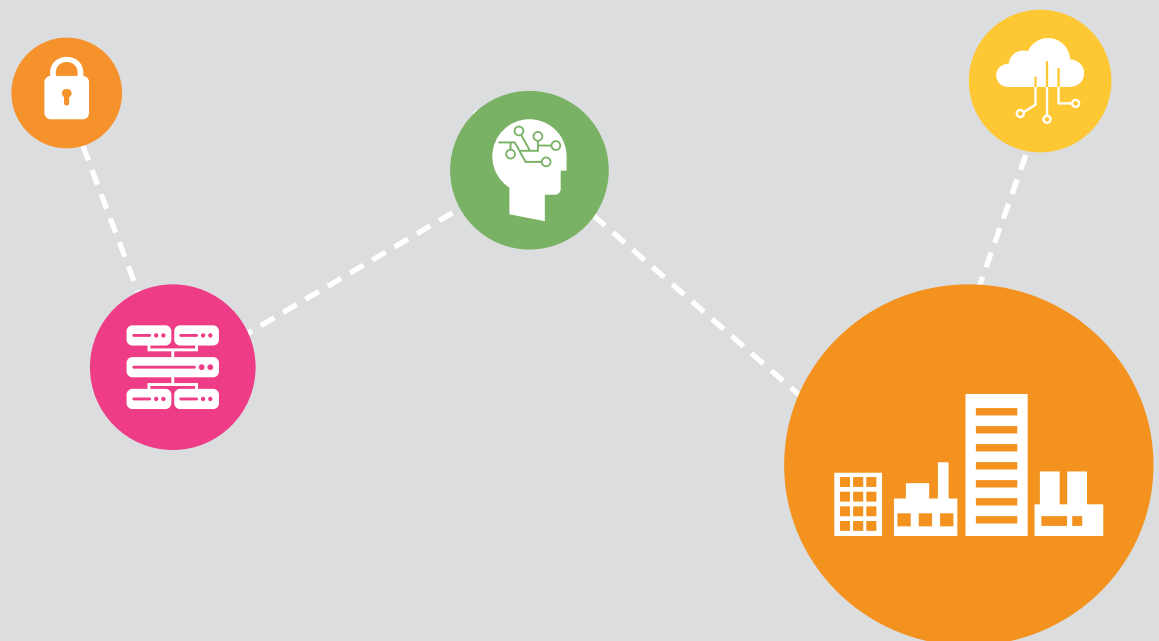


About PETRAS

The PETRAS National Centre of Excellence for IoT Systems Cybersecurity exists to ensure that technological advances in the Internet of Things (IoT) are developed and applied in consumer and business contexts, safely and securely. This is done by considering social and technical issues relating to the cybersecurity of IoT devices, systems and networks.

The Centre is a consortium of 22 research institutions and the world's largest socio-technical research centre focused on the future implementation of the Internet of Things. The research institutions are: UCL, Imperial College London, University of Bristol, Cardiff University, Coventry University, University of Edinburgh, University of Glasgow, Lancaster University, Newcastle University, Northumbria University, University of Nottingham, University of Oxford, University of Southampton, University of Surrey, Tate and the University of Warwick.

As part of UKRI's Security of Digital Technologies at the Periphery (SDTaP) programme, PETRAS runs open, national level funding calls which enable us to undertake cutting edge basic and applied research. We also support the early adoption of new technologies through close work with other members of the SDTaP programme, such as InnovateUK, supporting demonstrations of new technology and commercialisation processes.





Introduction

Reaching the Net Zero target is undoubtedly the biggest challenge facing the modern society. With [over 76%](#) of energy consumed in the UK originating from fossil fuels according to the Department for Business, Energy and Industrial Strategy ([2021](#)), the energy sector has a key role to play. Collectively, we need to build new capacity as well as upgrade the existing infrastructure to meet the challenge. This will be complemented by a step-change in culture: enabled by novel pricing mechanisms, a shift in social norms, or the rise of prosumption¹.

If adopted successfully, the advances in digital technologies will be fundamental for meeting the emission targets. From R&D work on flexible storage and distribution of energy, through more efficient tariffs informed by smart meter analytics, to, real-time demand side response thanks to smart household appliances, each of these innovations brings a promise of novel efficiencies and insights.

However, this ongoing digital transformation proclaims the introduction of new actors, products, start-ups, and even business models. The landscape is becoming ever so complex which creates challenges for effective collaboration. If professionals across the domains like IT, engineering, energy markets, sustainability and business operations cannot find the common ground, we risk overlooking our main objectives: the delivery of sustainable, affordable, resilient, and secure energy supply to the UK residents.

Numerous standardisation and regulatory initiatives are currently being developed to support the digital transformation of the energy sector: from Ofgem's [Digitalisation Strategy](#), Smart Appliances [PAS Standard](#), to the Network and Information Systems Security ([NIS](#)) Regulations. Finalising assurance schemes and policy enforcement will take time. In the meantime, we still need to uphold the interoperability, safety, reliability, and cybersecurity of energy systems. This is crucial for digitalisation agenda gaining widespread public support – or even – public enthusiasm. As such, we cannot take the success of digital transformation for granted. While no one can predict the future, we can still be its active co-creators.

¹ Here 'prosumption' refers to the combined consumption and production of energy, e.g., by households with solar panels



This report will help you with a successful digital transformation by:

- Outlining the role of cybersecurity in energy innovations
- Advising how to start conversations about cybersecurity without the technical jargon
- Providing prompts for discussions for you and your technical teams

Who should read this report?

This report is aimed for board level executives in the energy sector: operators of essential services, start-ups, digital services providers, licenced entities, generators, etc and other companies offering energy-related services and products.

Understanding the Role of Cybersecurity in Energy Innovation

Traditionally, energy and digital innovation were entirely different domains motivated by divergent principles and requirements. Energy sector, commonly understood as a highly regulated critical infrastructure, prioritised reliability of supply, workplace safety and protection of consumer interests. Meanwhile, the culture of innovation focuses on other goals, for example, [*a quick return on an investment \(Ball, 2021; p.91\)*](#), [*disrupting previous business models \(McDowall, 2018, p.243\)*](#) to [*solving societal problems \(Mazzucato, 2018, p.803\)*](#). Now that energy and digital innovation domains are converging, we need to reconsider their key organising principles. After all, it is vital to introduce innovative technologies while being cognizant of the wider context in order to avoid unintended vulnerabilities and harms.

Although cybersecurity might be a relatively new requirement for the digitalising energy sector, it is important to note that it does not exist in separation from other priorities. Cybersecurity has significant overlaps with safety, reliability, innovation, and trust.

First, cybersecurity needs to be aligned with **safety**. Energy sector is not just concerned with virtual processes, there are numerous examples of physical equipment assured for safety of workers and the pub-



lic. Malicious attempts to interfere with digital systems can have very tangible effects for the physical processes (see, for example, cases of [Stuxnet](#) nuclear centrifuge attack, or the [Ukrainian power grid attack](#)). However, quite often, technologies operating those critical functions do not support traditional cybersecurity measures (like patching or firewalls) as they comprise of [legacy systems](#) originally built for running time-critical processes rather than networked computing. Therefore, you need to ensure that the engineering and software professionals in your organisation are aware of each other's goals and actions.

Second, cybersecurity needs to be aligned with **reliability**. Your customers experiencing technical issues with your product might not realise whether they are caused by a malicious attack or an unintentional error. Root cause analysis is time consuming, meanwhile bad publicity can seriously harm your company overnight. What is at stakes, however, is the collective success of digital transformation in the energy sector. Errors are much more than a temporary inconvenience as we are designing a system where we are all reliant on software and internet connectivity. Gaining and maintaining public trust from the beginning is critical. You can achieve this by promoting collaborative approach when it comes to [interoperability initiatives](#) and robust testing procedures.

Third, cybersecurity should mobilise **innovation**. While we acknowledge that start-ups might not have the same capabilities to hire specialised teams like large and mature players, it is worth stressing that the [energy innovation ecosystem](#) in the UK supports cybersecurity by offering advice and inviting to standardisation initiatives. Furthermore, cybersecurity can promote innovative product development by deployment of modular and open-source software which helps to [overcome vendor dependency](#).

The regulatory landscape is evolving; it is a matter of time before various energy organisations will have to demonstrate appropriate assurances to be considered a trustworthy business partner. In fact, this is already happening in some areas like [critical infrastructures](#) across Europe, [the EU consumer IoT markets](#) and the [UK Government procurement](#). Secure digitalisation of the energy sector will therefore require an unprecedented level of collaboration between a wide variety of



actors who need to speak the same language and collectively understand the importance of cybersecurity to the core areas of business. Hence this report calls for board members considering **cybersecurity as an operational (rather than a solely technical) concern: a leverage of safety, reliability, innovation and, ultimately, trust** in the digital transformation.

Three Cybersecurity Tropes that Need to Retire

As cybersecurity enters the domain of energy innovations, we need to reconsider outdated advice and unhelpful jargon.



Scaremongering does not work anymore

People are now commonly aware of cybersecurity because of the extensive news coverage. However, *gaining awareness doesn't automatically equate with taking effective action*, especially when alert fatigue creeps in².



We need to move beyond perimeter security

The *boundaries of risk* go beyond geographical boundaries of your organisation or your customers' homes. Securing distributed energy systems requires thorough mapping out of your dependencies including supply chains and remote work locations.



Cybersecurity cannot be left only to technical experts

As your innovative ideas are leaving field trials and entering cities, offices, and homes, you will be required to involve the public in cybersecurity conversations. Perhaps your customers will be requested to update their smart home devices, set up a secure password for their electric vehicle charging account, or customise their peer-to-peer trading preferences. Each time you set up a security process (e.g. verification, automatic updates), you need to tailor the user interface to your consumers' levels of understanding. Failing to do so encourages digital exclusion and poor usability of digital innovations.

² Alert fatigue refers to people getting desensitised to safety alerts when overwhelmed with such messaging and busy with day-to-day work.



Therefore, as an industry, we need to be able to communicate the importance of basic cybersecurity hygiene. To achieve this, we need to let go of excessive jargon, abbreviations and military metaphors (such as cyber kill chain³, wargaming⁴, cyber Pearl Harbour⁵).

Consider the following future risks unique to smart energy systems:

- What are your assumptions about user acceptance, upscaling and 'correct' storage or energy consumption? What can happen if these assumptions prove wrong?
- What are the risks to markets and regulations? How vulnerable are we to tampering with energy prices, errors due to automated trading or policy failure or policy failure when setting tariffs?
- What novel harms can arise from the adoption of smart home appliances? How can we prevent invasive advertising, domestic violence or snooping on tenants?

When introducing new security measure, start small and iterate.

Create a proof of concept for feedback, iterate to improve it, think about how scale it up to create culture change across the whole organisation. Co-design process will improve trust of your colleagues and business partners!

³ the Cyber Kill Chain framework is a model for identification and prevention of cyber intrusions activity. The model identifies what the adversaries must complete in order to achieve their objective.









⁴ Wargaming is a type of cybersecurity training in which the competitors must exploit or defend a vulnerability in a system or application, or gain or prevent access to a computer system.

⁵ Cyber Pearl Harbour is rhetorical figure stating that a hypothetical disastrous cybersecurity attack would galvanise a major scale war.




Questions to Ask your Technical Teams

Consider the following questions to improve mutual understanding between technical experts and managers.

-  How can we better monitor and report on the security of our systems over time?
-  Do you know what systems you have, how they are connected, what information they hold and who uses and controls them?
-  How do we establish thresholds for anomalous events in regular monitoring?
-  Where are our claims about the levels of risk come from?
-  How can I better understand what X vulnerability/threat actor means to our organisation?
-  How can we learn from well-publicised past cyber attacks? Which lessons aren't transferrable to our sector/organisation?
-  What is the budget for maintenance of this security measure for X years?
-  What is the budget for upgrading this legacy system? How does it compare to the cost of dealing with a cyber incident?

Questions to Ask your Board Members

We recommend you embed the following questions in your regular risk management processes. Remember, both the energy sector and cybersecurity landscape will evolve, therefore you need to ask these questions in multiple stages of product development.

-  **Dependency mapping:** What suppliers, assets and people are we the most dependent on? What can we afford to go down and what can't we afford to go down?



Cascading risks mapping: What happens to your organisation and customers if a particular computer system goes down? What are the consequences in terms of finances, recovery time, safety, equipment damage, disruption of services? How long can we continue business as usual in the event of a system/data outage? How much data loss can we suffer before business-as-usual processes are interrupted?



Incident response planning: What would a proportionate response to the worst-case scenario look like? If a major cyber incident happens, how do we share information in order to stop it happening repeatedly, share the lessons and learn together?

Organisations and Initiatives to Follow

- The [National Cyber Security Centre](#) offers comprehensive advice for board members.
- The [Energy Systems Catapult](#) accelerates the transition to Net Zero by supporting innovators to commercialise, and helping design and deliver the future energy system.
- [IoT Security Foundation](#) organises knowledge exchanges and facilitates working groups collaborating on emerging assurance frameworks.
- [British Standards Institution](#) develops standards for energy smart appliances – see PAS 1878 standard on system functionality and architecture.
- [Flex Assure](#) is a voluntary code of conduct for the providers of flexibility services
- [SPRITE+](#) is a network of researchers and practitioners working on improving security, privacy, identity and trust in digital technologies through collaborative events and sandpit funding.
- The [PETRAS National Centre of Excellence](#) is a research consortium exploring security of IoT innovations together with practice-based user partners.
- The [PETRAS Power2 Project](#) delivers a roadmap for tackling socio-technical challenges on the security and privacy of IoT in the governance of the energy sector.



Further Reading

Judson E., Soutar, I., Mitchell, C (2020) [*Governance Challenges Emerging from Energy Digitalisation*](#). Discussion Paper.

Maidment, C, Vigurs, C., Fell, M.J. and Shipworth, D (2021) [*Privacy and Data Sharing in Smart Local Energy Systems*](#). Report.

Michalec, O., Milyaeva, S., Rashid, A. (2021) [*Regulating digitisation of critical infrastructures: we need diverse experts to translate cybersecurity risks into the sector-specific contexts*](#). Policy briefing 2.

Michalec, O., van der Linden, D., Milyaeva, S. and Rashid, A. (2020) [*Regulating digitisation of critical infrastructure: cybersecurity decisions must be based on robust evidence*](#). Policy briefing 1.

Michalec, O., van der Linden, D., Milyaeva, S. and Rashid, A. (2020) [*Industry Responses to the European Directive on Security of Network and Information Systems \(NIS\): Understanding policy implementation practices across critical infrastructures. Symposium on Usable Privacy and Security*](#).

Topping, C., Dwyer, A., Michalec, O., Craggs, B., Rashid, A. (2021) [*Beware Suppliers Bearing Gifts! Analysing coverage of supply chain cybersecurity in critical network infrastructure sectoral and cross-sectoral frameworks*](#). *Computers and Security*.

Acknowledgements

We would like to thank Energy Systems Catapult and PETRAS Consortium for sponsoring this piece of work. We would like to also extend our gratitude to 30 experts in the domains of energy and cybersecurity who shared their insights with us. Finally, many thanks to Sharad Agarwal, Anthony Mazeli, Jake Verma, and Tabitha Dunn for event facilitation.