EXPERT OPINION

Cybersecurity at the heart of tomorrow's energy

Energy does not escape digital technology. At a time when our societies are constantly evolving, the energy transition has become a major challenge for both cities and companies. In order to succeed, they need to leverage digital transformation. On a local level, these are real and immediate issues for elected representatives and decision-makers. Cybersecurity has spectacularly become the hot topic of conversation and it is open to question as to how it should be addressed. In this paradoxical context, there is an opportunity behind the question "How can a secure digital transformation be designed to access the benefits of the energy transition?"

The link between digital technology and the energy transition is not often discussed. However, there is a strong connection between these two areas.

In 2020, 23% of our energy will come from "renewable" sources. This level of production involves introducing new sources, such as wind and solar energy, so-called "intermittent" energy as they are dependent on environmental conditions. We are about to transition from a centralised production model, as we know it, to a decentralised energy model. Current knowledge does not enable us to have the large-scale storage means required; it is clear that maintaining the balance between consumer needs and production needs will be the key to success. But everything changes quickly and we can see disruptive prospects appear in the initiatives of the entrepreneur Elon Musk in his recent project concerning individual battery storage.

Digital technology: sustainable regulation intelligence

With the new energy model comes numerous responsibilities, energy production and sources, themselves diverse as they will supply numerous networks and will ultimately require a new form of regulation and balance between consumer needs and distribution capacity.

Regulating the balance between energy supply and demand in a decentralised model inevitably involves digital technology.

De fait, l'équilibre entre l'offre et la In fact, the supply-demand balance is a challenge. Let's take the example of an electric car: "In the evening, I go home, I connect my car to a standard electric meter and the next morning the battery is charged. I can then head off again. This seems simple. With a diesel engine: I go to the petrol station, it takes three minutes to fill up the tank and then I drive off again. But if I wanted, similarly, to "fill up" my electric car in 3 minutes, the energy required would need to be… the whole district's supply! ".

It is at this point that digital technology steps in. The major changes to energy production and consumption, the substantial transformation in terms of management, with this new regulation in mind, require intelligent sensors, networks and systems, and applications that can be used on the move. Digital technology becomes a real key vector for success.

A new sensitive and exposed vertical

To address these matters, we need a global approach at the city level in particular, for which we perceive the major changes cities will undergo with the "Smart City" concept in the management of energy and transport networks.

Change management involves a commitment from eco-citizens and new interactions. Experiments are being set up on regional platforms. Innovative concepts will be developed where the objective is to accelerate the transition (continuous networks, smart equipment for residential accommodation, adaptive digital services, storage devices, etc.). The issue of security is certainly a cornerstone and with the presence of digital technology, cybersecurity becomes an issue that must be addressed with discernment.
On a local level, elected representatives and decision-makers must share a secure vision of energy and the digital world. For the eco-citizens of tomorrow, this involves developing the suitability of new interactions with the energy systems, whether this concerns direct consumer actions or indirect actions like measuring consumption and paying invoices.

The energy transition is an economic sector that is sensitive and exposed. To guarantee its success, we must have trustworthy digital services.

Just like in any economic sector, there are risks of intrusion related to the value of the information which will result in theft and resale on parallel markets. There are also risks related to fraudulent use or deliberate attempts to interrupt a service. The energy transition attracts greed. Certain players will go on the attack and offensive by seeking and finding vulnerabilities. So, how do we deal with the balance between digital technology, synonymous with progress, and the vulnerabilities of cyberspace?

To make this energy transition successful, we must have trustworthy digital services. Unexpectedly, this is why cybersecurity is featuring at the heart of tomorrow's energy. The solutions are out there.

Protection must be an integrated and collaborative approach

The delay between intrusion and detection was 270 days! This example shows at what point the issue of security is strategic, and at what point it falls into the context of digital-controlled energy.

As is the case in all sectors, there are two important pillars of security: prevention, based on a global strategy connected to the levels of hierarchy with all of the services of the organisation and sites; and protection, which should be given special attention as regards detection and defence of each system. Because intrusion threats exist. It also affects energy systems, and all the more so as their model will be decentralised and collaborative, and therefore more at risk.

In this context, it will also be necessary to combine defence capabilities and not neglect training, as we are fully aware of the importance of the human element. Attackers often target networks, and not necessarily a single target. Isolated protection is certainly important, but it is necessary to do more than that by developing methods where protection and detection approaches are also networked and themselves become collaborative. Within the sector, this concerns the relationships between tier 1 energy suppliers in the production and distribution chain, but also the other players in tiers 2 and 3 of the subcontracting chain.

Our conviction is that a shared cybersecurity centre, connecting all of these players, makes it possible to decentralise the advanced mechanisms of detection for each contributor, and therefore to equip everyone with first class powers of protection. This approach is already applied within large groups and their SME suppliers.

The major changes to energy production and consumption, the substantial transformations concerning energy management and a new method of regulation will require digital technology to be a key vector for the success of the energy transition. It is therefore essential to combine the defence capabilities and not neglect training, as we are fully aware of the importance of the human element. Cybersecurity is at the heart of this dramatic change.

Author

Didier Bosque

Innovation Director at Sopra Steria

He leads the Albatros cybersecurity programme, which objective is to boost a collaborative and federative dynamic at a sector level.

Sopra Steria - Corporate Communication & Marketing
contact-corp@soprasteria.com
www.soprasteria.com