
Perspectives
HITACHI
Inspire the Next
The world needs a cybersecurity ecosystem for a resilient electric future
January 2022
Hitachi Energy

Index

The world needs a cybersecurity ecosystem for a resilient electric future

Pierre-Alain Graf

Cybersecurity Lead
Hitachi Energy

Thomas Tschersich

Chief Security Officer
Deutsche Telekom

Anders Gustavsson

Head of Global Connected Solutions
Securitas

The energy industry is one of the world's top three target sectors for cyber attacks. Not least recent events such as the ransomware strike on the Colonial Pipeline which disrupted fuel supplies to the US Southeast, a data breach at Danish wind turbine maker Vestas, and a cyber attack on the nuclear unit of Brazil's Eletrobras have reminded us how vulnerable to cyber crime the energy sector still is.

What these incidents highlight again and again is that we need much deeper cybersecurity collaboration in order to advance the world's energy system to become more sustainable, flexible, and secure. It's only when we operate in a joint ecosystem where we trust to share cybersecurity information that we can truly build joint resilience. Realtime yet responsible information exchange is the future, especially as the decentralized energy system of our low-carbon world will require exponential growth in new electric and digital connections.

What benefits will a resilient cybersecurity ecosystem bring to the energy sector? What hurdles need to be crossed to enable its full potential? These are some of the questions we have asked two leaders at the cutting edge of information technology (IT) and operational technology (OT) security: Thomas Tschersich, Chief Security Officer at Deutsche Telekom, and Anders Gustavsson, Head of Global Connected Solutions at Securitas. Alongside global security expert Pierre-Alain Graf, Cybersecurity lead for Hitachi Energy, they discuss in the following interview the need for a switch in mindset to build strong, trusting partnerships.

Why cybersecurity matters in energy

Q: Why is cybersecurity becoming so important within the energy sector?

Pierre-Alain Graf (P.-A.G.), Hitachi Energy: It's very simple: electricity, and energy more generally, is the backbone of societies. If you switch off electricity, everything is gone. It's a very critical domain that really needs to be protected.

In military doctrine, disabling infrastructures has always been the first wave of attack. Therefore, critical infrastructures, especially the power sector, have become part of cyber warfare. Compromising the cyber space is a very cheap and effective way to gain and remain in control.

Utility companies have been used to working pretty much independently. Cybersecurity incidents now present an ecosystem challenge because it's not just one utility that is being targeted but the weakest link somewhere in a country's power system. The energy sector needs to constantly adapt its defense, which it didn't use to do quite so often before. Utility players need to think of themselves as being part of an ecosystem because none in the sector are fast enough to meet all the threats alone. This is the main reason why it's so important to really address cybersecurity in a very open and proactive way, especially with emerging and widespread cybersecurity vulnerabilities, such as the recent Log4j/Log4Shell. The ongoing events surrounding this situation potentially expose existing risks across critical infrastructures, including power, while also highlighting the need for an industry-wide collaboration to better detect and respond to cybersecurity incidents.

Thomas Tschersich (T.T.), Deutsche Telekom: When I was studying electrical engineering almost three decades ago, it was not a very connected (energy) industry. It may sound a little paradoxical but as we strive to build a carbon-neutral world, we need more energy to electrify sectors like transport while connecting supply and demand in order to balance the energy system. With increasing connectivity, cybersecurity is assuming an increasingly important role. We're not only talking about power substations but also about decentralized energy production like solar panels on private houses. Criminals can make use of these growing connections in energy by introducing malicious commands in order to take control. This clearly shows that simply due to the amount of additional connectivity, we now have an increasing demand for protecting those communication systems.

“

It may sound a little paradoxical but as we strive to build a carbon-neutral world, we need more energy to electrify sectors like transport while connecting supply and demand in order to balance the energy system. With increasing connectivity, cybersecurity is assuming an increasingly important role.

Thomas Tschersich

Energy at risk

Energy is among the top three target sectors for cyber attacks

Source: IBM Security, X-Force Threat Intelligence Index 2021

Source: Deutsche Telekom

Anders Gustavsson (A.G.), Securitas: From a crime point of view, whether you're stealing information or wanting to attack a society, the easiest way in the past has been to hit a base station or to go for a power station. Today, if you don't want to get dirt on your hands, cyber intrusions are the easiest option. Why should a potential intruder take the risk of physically placing a bomb on a piece of infrastructure if they can choose the easy way and simply buy themselves a hacking service or tool to make it through a data center? Critical infrastructure such as data centers, communication base stations, or power plants are increasingly at threat from growing connectivity. The downside of having implemented very strong physical security is that criminals now increasingly opt for cyber attacks.

“

Utility companies have been used to working pretty much independently. Cybersecurity incidents now present an ecosystem challenge because it's not just one utility that is being targeted but the weakest link somewhere in a country's power system.

Pierre-Alain Graf

Q: What kind of a threat is deeper electrification posing to cybersecurity?

T.T.: Without electricity, cybersecurity won't work. Electricity infrastructure is one of the most critical elements of our society and installing all these additional connections is making it more and more vulnerable. This means that the attack surface is growing for cyber criminality, which is in general not a bad thing by itself, but we need to really improve in dealing with this vulnerability and should dedicate our full focus to it to stay in control. Physical security also becomes more important as greater connectivity means more of the critical equipment is placed into outdoor equipment in the field rather than inside substations only. We do need that growing connectivity but it's a burden and an opportunity at the same time.

P.-A.G.: We have a great saying that the future is uncertain, but it is electric. Why do we need to connect more deeply? In order to move to a carbon-neutral energy system we need to change the whole electricity system architecture. A fundamental principle of the electricity market is that you consume it as close as possible to the production source. But with offshore wind, for example, that's really hard. So, there is a need to have a more intelligent network with lots of different interconnections, microgrids, and different technologies working together. This entails the need to communicate faster and more deeply, which again requires higher protection on cybersecurity.

Electricity infrastructure has also become more attractive for criminals and hackers to manipulate given the growing but delicate convergence of physical and cyber infrastructures. I remember that when I started working at Swissgrid nobody would even think of entering a power station because it was simply too dangerous. Today, one can disrupt the integrity of critical energy assets not only through physical intrusion but also through virtual attacks, from anywhere around the globe, simply by gaining control of key assets. As the notion that electricity assets are dangerous has gone, physical asset security has assumed a new, important dimension. But only in parallel with an integrated cyber response. Both are increasingly critical.

A.G.: Growing connectivity and digitalization make attacks on individual assets much easier because they all need to communicate. We can easily build Fort Knox-type physical security around infrastructure that is centralized, but today's decentralized way of working makes this more difficult. This should urgently prompt the cybersecurity sector, across industries and infrastructures it serves, to harmonize security processes and best practices that rapidly detect vulnerabilities and prevent potential cyber attacks.

> So, there is a need to have a more intelligent network with lots of different interconnections, microgrids, and different technologies working together. This entails the need to communicate faster and more deeply, which again requires higher protection on cybersecurity.

Pierre-Alain Graf

Q: How important is cybersecurity to safeguard and increase electricity grid resilience?

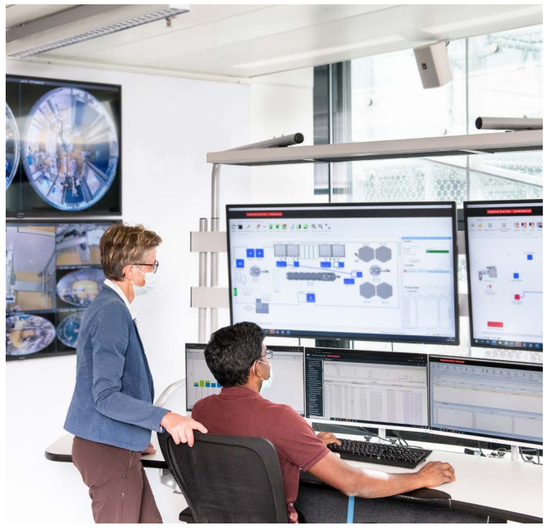
P.-A.G.: I think it's crucial. What we need to do in the electricity sector is to look at our assets through the lens of the cyber world because there are some fundamental differences. If you take the standard resilience assessment from an electricity network operator's perspective you might see an issue occurring in one area, or two if you're really unlucky. From a cybersecurity point of view, threats appear in multiple areas at the same time. This means that electricity grid resilience needs to be assessed from a completely different perspective because we are constantly facing the threat of multi-attack vectors.

T.T.: The challenge of a more interconnected future is of course that criminals can compromise resilience because the infrastructure is all remotely controlled. Therefore, we need to build a solid defence against those potential kinds of attacks. For example, companies sometimes need to rely on public Internet to connect remote locations, but adequate protection must be in place to shield them from cyber attacks. I would argue that companies need some form of cyber assurance to provide resilience in an interconnected world, much like physical backup is being employed for standard electrical network resilience.

> Physical security also becomes more important as greater connectivity means more of the critical equipment is placed into outdoor equipment in the field rather than inside substations only. We do need that growing connectivity but it's a burden and an opportunity at the same time.

Thomas Tschersich

Adopting an ecosystem mindset



> A change in mindset is needed in moving from thinking in silos to realizing that once you have information about an attack, you can help others protect themselves. By bringing information together, everyone is able to build a better defense.
>
> **Thomas Tschersich**

Q: What needs to change to support an ecosystem mindset?

P.-A.G.: The first dimension of ecosystem thinking should be: how do I share information in a trusted and confidential way? How do I share it effectively and rapidly? The recent cyber assault on Vestas was an example in point. In a press statement, Vestas shared key information not only with its customers but with the whole industry as soon as the attack was discovered. As a supplier or manufacturer, it's not good enough to just inform your customers, we need to find another way to exchange information and involve key stakeholders.

The second dimension of ecosystem thinking should be about looking beyond your own walls. By nature, we still think like we did in the Middle Ages: we have built our fortress and within its walls we feel very secure. But the reality in cyber defense is that there are no walls because these new tools that have come out have been designed to bring them down.

Attack vector recognition and exchanging that information are, in a nutshell, essential to the survival of electricity systems. Companies need to jointly prepare for the worst-case scenario and think about what information they will share with whom and how. It's only a matter of time that it will happen.

T.T.: Firstly, the mindset of 'everything is secure and controllable because I have it under my desk' needs to be changed. It was true until the technicians of the telecom operators drilled a hole through the wall and connected the entire world to those systems.

Secondly, we need to overcome corporate silos. In some enterprises I have seen one Chief Security Officer (CSO) is taking care of IT, one CSO is looking after the security of the production network and another CSO is responsible for the personal security staff. They're all sitting in their silos and that's what we need to overcome. As CSOs, we have the privilege to bridge these silos and to bring the discipline of security together. Attackers have no regard for responsibilities in our organisations, they only care about launching a successful attack.

There's a third aspect too which relates to the willingness to share information. A change in mindset is needed in moving from thinking in silos to realizing that once you have information about an attack, you can help others protect themselves. By bringing information together, everyone is able to build a better defense. And this also applies beyond company boundaries.

Q: How else do you see cyber attacks evolving?

T.T.: Cyber attacks are not only happening simultaneously, but also rolling in waves across the globe. One of the problems in the digital world is that, for example, Europe and the US are now just 20 milliseconds apart. That's how quickly a data package can move between the two continents. This reality allows attackers to exploit a weakness in a software program on a different continent, requiring us even more to be prepared to defend 24/7. In addition, we are facing a challenge with so called Zero-Day vulnerabilities that are not yet known in the public domain, and which are very difficult to protect against as hackers exploit the flaws before developers can even have a chance to address them. If a company falls victim to a "zero-day" attack but is then not sharing information about the incident, others are unable to protect themselves against the same threat. That's the idea behind our joint service: to collect this kind of information, to make it more widely available for others to protect themselves. We put them under a security umbrella so to say.

A.G.: It's important for the modern company to have a CSO who covers all aspects of security, physical as well as cybersecurity. Nowadays all physical systems need to be protected against cyber threats. This goes back to the need to create an ecosystem mindset. The physical and cyber worlds are becoming much more intertwined. Look at 3D printing, for example, or omni channels in the retail space where one day customers order on the Internet and the next day, they visit a shop.

"Zero-Day"

Describes recently discovered security vulnerabilities that hackers exploit before developers can address them

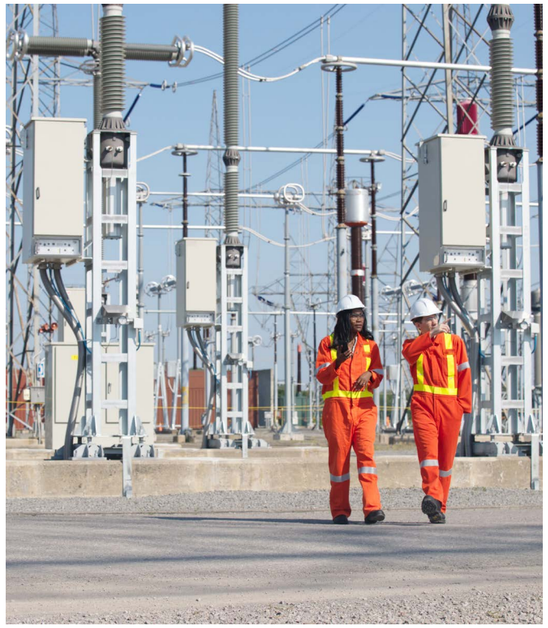
> Nowadays all physical systems need to be protected against cyber threats. This goes back to the need to create an ecosystem mindset. The physical and cyber worlds are becoming much more intertwined.
>
> **Anders Gustavsson**

Role of responsible disclosure

Q: What examples can you mention that illustrate the benefits of data sharing?

P.-A.G.: There are quite a few examples but it's tricky to speak publicly about them because we'd breach the confidentiality agreement intrinsic to information sharing. Nevertheless, information sharing is a central piece of collaboration within an ecosystem. The question is: how can you make sure your customers feel safe and in return help you protect your own operations?

One example I can mention involves a European utility which fell victim to a copper theft incident a few years ago. The burglars attacked one of Europe's largest substations which at the time didn't have any video surveillance or cybersecurity in place. Since these elements were not monitored, the company had to go to great lengths to assess the physical damage but also whether the criminals had inserted any bugs into the IT systems. If proper security measures had been in place, the utility could have acted much more quickly and alerted customers as well as the wider industry.



T.T.: From a cybersecurity perspective, the most basic and accessible level of sharing information is integrated into each of our desktops: the antivirus program. This is a piece of software that is constantly sharing what we call IOCs (Indicators of Compromise) or parameters that determine whether a file is malicious. In cyber defense, this is what we're doing on a daily basis: analyzing threats. This enables us to identify a suspicious Data Pattern, URLs or IP address that we can share with our clients and the wider industry. We're collecting up to 100,000 new IOCs every single day. Nobody can gather all this intelligence on their own. In order to have a 360-degree view of our infrastructure and to be able to protect it, we need to have access to as many data sources from as many companies as possible.

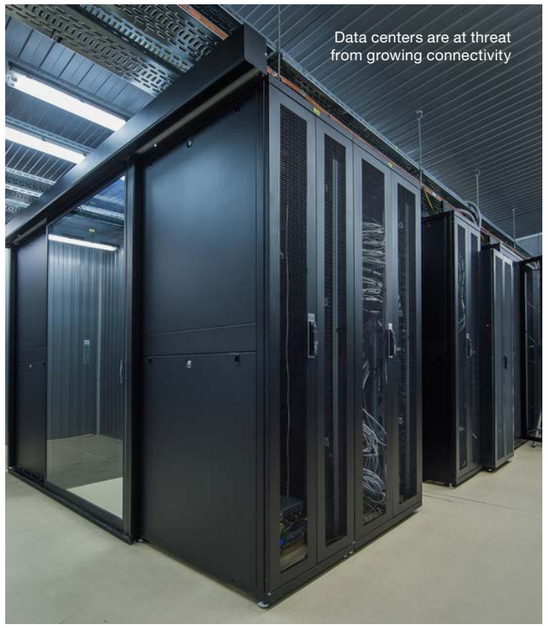
> Nevertheless, information sharing is a central piece of collaboration within an ecosystem. The question is: how can you make sure your customers feel safe and in return help you protect your own operations?
>
> **Pierre-Alain Graf**

Up to

100,000 new IOCs

Every day, up to 100,000 new IOCs are collected, which determine if a file is malicious

> What we do need to share with our customers is information on how to detect whether they are vulnerable or whether there is an attacker trying to intrude in their systems, and in other cases, what was the root cause of their success.
>
> **Thomas Tschersich**



Data centers are at threat from growing connectivity

Q: Are there any limits to information sharing?

T.T.: Of course, we need to talk about what we are sharing. We're not sharing information on how to best exploit a vulnerability. That is only given to the vendor who is responsible for fixing it. They are then given enough time to address the issue before we speak publicly about them. This is what we call responsible disclosure. We are also not sharing classified or privileged information like personal data. What we do need to share with our customers is information on how to detect whether they are vulnerable or whether there is an attacker trying to intrude in their systems, and in other cases, what was the root cause of their success.

A.G.: The benefit of sharing information is exactly that: identifying a weakness and showing others how to address it. Another point of sharing is being open about the impact on your business. A good example of this was the cyber attack on logistics company Maersk in 2017. It was not a rocket science-type of attack, but they were very open about sharing the consequences of the attack on their business, which cost it up to $300 million. These types of transparency and information sharing are also good for business.

P.-A.G.: Unfortunately, I think the globe is falling apart into different camps. I can clearly see this within my work as Co-Chair of the cyber resilience group at the World Economic Forum. But interestingly, everyone has the same concerns on electricity network resilience, which is 'we need electricity for our country, and we feel threatened by the other side'.

I believe we need to go beyond sharing information and develop a legal framework, such as amending the Geneva Conventions treaties to include a non-attack on critical infrastructure such as electricity networks. The moment you cut off electricity and water, you have casualties and massive damage, which nobody wants. Let's be realistic, that's only a wish at the moment, but that's the kind of ambition we need to strive for as an industry.

Looking ahead

Q: What practical changes are needed to encourage an ecosystem mindset?

P.-A.G.: One very big question mark is whether we can harmonize global security rules. On the cyber side, there are so many rules and regulations that are different from country to country, but they essentially address the same issues. It just increases the operational costs but doesn't enhance security.

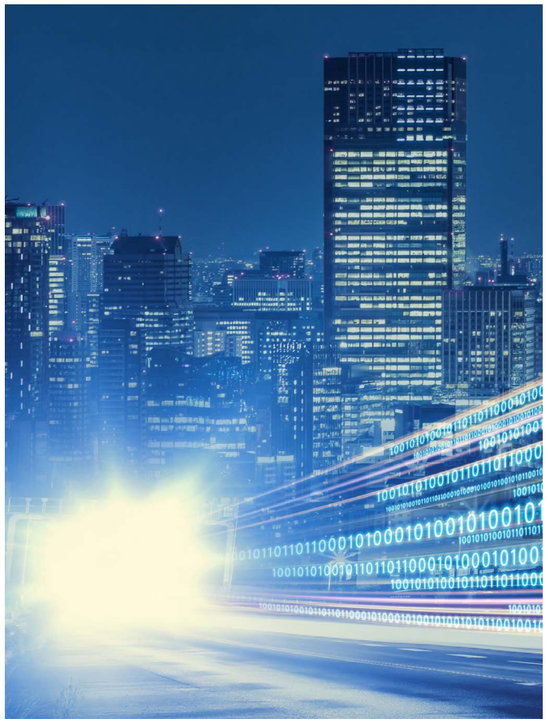
T.T.: It's fair to say that every country has the same kinds of vulnerabilities, which include dependence on energy and telecommunications. It should be in our own interest to harmonize the rules around addressing our security risks globally. I would agree with what Pierre-Alain said: we need to somehow come to a cybersecurity agreement comparable to the Geneva Conventions, otherwise we will harm each other, the attackers as well as the defenders.

Q: What motivates you personally to work in this sector?

T.T.: That's an easy one: make the world a safer place. It's not just me but also the team behind me. We want to apply our passion to giving something back. The team behind me is really working towards that, towards making the world a better place and fighting for good.

A.G.: That also applies to Securitas. We strive to help make our clients safer. For us, this is a really good collaboration because we see that there's a need, but we don't have the capacity to do it all ourselves.

P.-A.G.: The power sector is a fascinating and critical one. It has always been about fostering development and advancement of society. Another thing that motivates me is that I really enjoy discovering new dimensions. Like us three partners working together – that's been a huge discovery. At Hitachi Energy, we are advancing the world's energy system to be more sustainable, flexible and secure. As the pioneering technology leader, we collaborate with customers and partners to enable a sustainable energy future – for today's generations and those to come. And this excites me.



> From a cybersecurity point of view, threats appear in multiple areas at the same time. This means that electricity grid resilience needs to be assessed from a completely different perspective because we are constantly facing the threat of multi-attack vectors.
>
> **Pierre-Alain Graf**

> It's fair to say that every country has the same kinds of vulnerabilities, which include dependence on energy and telecommunications. It should be in our own interest to harmonize the rules around addressing our security risks globally.
>
> **Thomas Tschersich**

Hitachi Energy - Advancing a sustainable energy future for all

Hitachi Energy Ltd.
Brown-Boveri Strasse 5
Zurich, Switzerland (HQ)

hitachienergy.com