How cybersecurity is becoming crucial in the digital age

Credit: Neoen

Cybersecurity | A string of high-profile cyberattacks on energy infrastructure highlights the vulnerability of solar farms as they become increasingly reliant on digital systems. Alice Grundy looks at the rising threat of cyberattacks and the measures asset owners can take to mitigate the risks

Cybersecurity can easily fly under the radar, just as a hacker weaves through systems and sifts through files undetected. The documented cases of cyberattacks on the energy system are hardly a page-spanning list, and the number of cases on solar assets even fewer. But that doesn't mean the risk is as slight. What is largely considered to be the first cyberattack on a power grid took place in Ukraine in 2015. It is also considered to be one of the most dramatic cyberattacks in the energy sector; in a scene that should be straight out of a spy movie, an operator in the Prykarpattyaoblenergo control centre was locked out of their computer, watching as their curser moved independently from any of their own actions. The attack took out 30 substations and caused a blackout that took six hours to fully resolve.

The knowledge that a cyberattack could – and has – caused blackouts seeped into other events. When the UK had a major blackout on 9 August 2019, initial suggestions seen on social media were that it was a result of a cyberattack, although within hours these rumours were squashed. It was, in fact, a result of a lightning strike that triggered faults in an offshore wind farm and gas-fired power station, and not a result of a cyberattack.

Whilst cyberattacks on solar farms specifically are not commonly reported, this could well change. Digitalisation is creeping into the solar industry, automating processes and making components smarter. And where there are increases in digital technology, the threat of cyberattacks is never far behind.

The trend of digitilisation in solar raises the threat of cyberattacks

Digitalisation and the effect of lockdowns

The solar sector is embracing digitalisation little by little. The lockdowns that were put in place due to the COVID-19 pandemic have resulted in a speeding up of digitalisation efforts. Companies both in and out of the energy sector have become more reliant on digital tools for their day to day running, with many employees working from home. Significantly more business is therefore being conducted via calls and emails over a face-to-face conversation between colleagues. Whilst this may have affected the awareness of the importance of digital services, it has also increased the risk of a cyberattack.

"The threats and dangers have grown during the lockdown period because of that increased reliance," according to Geoff Taunton-Collins, senior analyst at renewables insurer GCube. Taunton-Collins says that when compared with other risks solar assets see, the cybersecurity threat level is "reasonable but growing".

This is echoed by Marek Seeger, information security manager at SMA, who says that solar is "becoming a more interesting target for hackers" as the technology takes a larger role in power supply as a result of decarbonisation and decentralisation efforts.

In particular, small and medium-sized solar systems are in danger, he says, with >1MWp plants usually integrated, connected and maintained "in a professional way that includes all relevant safety measures".

One way hackers can artificially create a malfunction in a PV system is to launch cyberattacks to the inverter controls and monitoring system, according to Ali Mehrizi-Sani, associate professor at Virginia Polytechnic Institute and State University and co-author of a 2018 paper assessing the cybersecurity risk of solar PV units with reactive power capabilities.

"This is a vulnerability that can be, and has been, exploited to attack the power system," he says, pointing to how the large number of PV units in the power system – including rooftop solar – means that there are "lots of attack points", underscoring the importance of cybersecurity at the inverter level.

Keeping cybersecurity measures up to date is therefore incredibly important for solar installers and operators, particularly due to the 15-20 year lifetime of a solar farm, meaning that cybersecurity will need to continue to develop as the farms age, with up to date measures allowing operators to stay ahead of hackers.

This can, however, be made difficult by a lack of awareness over cybersecurity. Cyberattacks on renewables assets are underreported, according to GCube's Taunton-Collins, occurring because it's "easier to keep quiet than other industries".

Most cyberattacks result in data breaches, such as the cyberattack on EDP in April 2019. The Portuguese energy firm was hit with a Ragnar Locker ransomware, with over 10TB of sensitive company files stolen. When third-party data is leaked, it has to be reported to the authorities of the country it occurred in, as well as an alert sent to the people whose data has been stolen.

However, attacks on renewables assets are more likely to be business disruption attacks, which are private and internal, due to many not holding third-party data. Asset owners therefore often have no reason to publicise that an attack has taken place. Furthermore, releasing information on this sort of attack can hurt the reputation of both the company and potentially of the industry itself, leading to some asset owners keeping quiet.

Credit: BayWa r.e.

As a potential weak spot, inverters are the focus of a research project in the US looking to develop new measures for protecting PV systems

One cyberattack on a solar farm that did end up hitting headlines, however, was on US solar operator sPower, which occurred in 2019. It didn't result in any blackouts, and sPower – which owns and operates over 150 renewable generators in the US and recently concluded financing for the 620MWdc Spotsylvania Solar Energy Center, its biggest ever project – has been unsurprisingly tightlipped about the incident.

Pay out or lose out

There is a wide variety of outcomes when a solar asset owner is targeted by hackers. When hit with a ransomware attack, the figures demanded by hackers can climb to astronomical heights. The asset owner is then left with two choices: pay up to resolve the situation or replace its computer systems completely and start afresh. However, this itself is not a perfect solution. Replacing computer systems is a costly and time-consuming endeavour. Everything must be migrated over to the new system, a disruption which can often be underestimated by asset owners.

In 2016, a SABELLA tidal project in France was rendered inoperable for two weeks as a result of a ransomware cyberattack. Similarly, Norsk Hydro was attacked by ransomware in 2019. The company – which deals in both renewable energy and the manufacture of aluminium – didn't pay the ransom, a decision that left it recovering for many months after and cost it over £45 million.

"These things can really quite cost you when they hit, as Norsk Hydro found," Taunton-Collins says.

It's not just the costs of replacing systems; fines can be levied by the grid operators of the country affected. If a particular asset has an agreement in place to provide a certain amount of energy but is unable to due to a cyberattack, then fines or penalties may be imposed due to the failure to meet targets, resulting in a shortfall or, in extreme cases, a blackout.

With the stakes – and resulting costs – so high, measures which can mitigate the risk and protect asset owners from cyberattacks are crucial. Daily backups of data are a start, particularly of important or pertinent data. Staff training, as well an access of least privilege system – meaning that workers only have access to systems required for their jobs rather than everyone having access to everything – are also measures that can help boost security. Alongside this, multifactorial identification and changing passwords from the default – which are often available online and therefore easy for a hacker to get a hold of – can help.

SMA's Seeger suggests that to help solar assets improve their security across the board, there needs to be "central and uniform directives on an EU level". Manufacturers also need to ensure that their devices adhere to the highest standards of cybersecurity while installers and operators must provide for secure integration, he continues.

Seeger points to how the inverter manufacturer is a part of SolarPower Europe's Digitalisation and Solar Workstream. In May 2017, SolarPower Europe's Digitalisation and Solar Taskforce published its 'Seven Commitments on Digitalisation', with an aim of helping the solar industry fully transition to digitalised solar.

Among these were commitments to data protection and cybersecurity, with the document stating that "we will champion data protection", and recommending that all active parties in the solar industry implement "state-of-the-art" data protection alongside committing to putting "stringent cybersecurity measures" in place.

The taskforce then called for policy changes to help guarantee these high standards. Mercè Labordena, senior policy advisor for digitalisation at SolarPower Europe, says that due to new threats being created and those already existing evolving, the European solar industry needs to "constantly adapt its response".

This requires a holistic approach to be adopted, Labordena continues, helping to "increase the cyber-resilience of the solar industry and working together on all levels, from citizens and companies, to member states".

Innovating to keep up

However well protected an asset is, it is still possible for it to be hacked. New solutions are, however, being developed to help to keep up with the evolving threats.

A research project is underway in the US, led by the University of Arkansas, with an aim of developing systems to protect solar technologies from cyberattacks. The project – dubbed Multilevel Cybersecurity for Photovoltaic Systems – was awarded US$3.6 million from the US Department of Energy (DOE) Solar Energy Technologies Office, and is to focus specifically on inverters with a plan of addressing issues such as supply-chain security and real-time intrusion detection methods. Researchers are also looking into identifying and mitigating vulnerable spots, control system security and safety protocols.

Commenting at the time of the original project announcement in April 2020, principle investigator, professor Alan Mantooth, said that the DOE was aware of the "critical importance" of protecting solar systems, with the new research group "nicely qualified" to help address the problems around cybersecurity.

On that note, a new US solar cybersecurity initiative was created in June 2020. The Cybersecurity Advisory Team for State Solar (CATSS) was created by the National Association of State Energy Officials and the National Association of Regulatory Utility Commissioners, with additional support provided by the US Department of Energy Solar Energy Technologies Office.

The CATSS is to identify model solar-cybersecurity programmes and actions for states to take in partnership with utilities and the solar industry, creating actionable solar cybersecurity strategies and roadmaps.

It is hoping to work with both federal and private-sector stakeholders to mitigate cyber risks, using a state-led advisory group and dialogue with solar and cybersecurity experts to advance education, tools and access to technical assistance.

The question remains, however, as to whether the onus should be on the industry to put in place the innovations and high levels of cybersecurity measures needed to protect their own systems and assets, or if governments should be legislating to ensure a standardised, high level of security is met.

"Since Europe has an interconnected power transmission system, uniform European specifications should play the leading role here," SMA's Seeger suggests when asked about the topic. However, he continues to argue that aside from that, manufacturers should be putting the highest priority on the cybersecurity of their products, stating that these high levels of security standards can only be achieved if all the parties involved, including manufacturers, plant owners and operators, "make constant efforts to ensure adequate cybersecurity".

Whilst it isn't the most common problem for a solar farm to run into, the threat of a cyberattack is still present. Not only that, it is ever-evolving and becoming more prevalent as solar transforms into an increasingly digital-reliant industry.

Energy infrastructure is "one of the most critical assets of a modern society and a backbone for its economic activities", SolarPower Europe's Labordena says, with cybersecurity and data protection no longer isolated issues, due to the "ever-increasing integration of all sectors of the economy via electrification" and the adoption of digital technologies. As more devices become digital, smart and connected to the power system, the risk of cyberattacks will only continue to grow with them.

As Labordena puts it: "For this reason, cybersecurity needs to be at the top of the agenda of Europe and the European solar industry".

The same could no doubt be said for solar markets around the world. ■

ROADMAPS AND POLICY DECISIONS:
How cybersecurity factors into policymakers' agendas

Cybersecurity for the energy system – and solar PV in particular – has not necessarily been overlooked by policymakers across either the EU or the US. In the EU, a report from the Energy Expert Cybersecurity Platform (EECSP) was published in 2017, making several recommendations to the European Commission on cybersecurity in the energy sector.

Four priorities were outlined, including setting up an effective threat and risk management system, an effective cyber response framework, continuously improving cyber resilience and building up the required capacity and competences in cybersecurity for the energy sector.

Following this, in 2019 the European Commission published its recommendation on cybersecurity in the energy sector. It highlighted how the main issues relating to cybersecurity in the energy sector are namely real-time requirements – with some elements of the sector finding it difficult to implement cybersecurity due to having to work in real-time - cascading effects due to the interconnection of electricity grids and gas pipelines across Europe and the combination of legacy and state-of-the-art technology.

Several measures to solve these issues were outlined, including – but not limited to – recommendations for energy network operators to apply the most recent security standards for new installations wherever adequate, as well as formulating tenders with cybersecurity in mind. This would include demanding information about security features and compliance with existing cybersecurity standards.

Meanwhile in the US in 2017, Sandia National Laboratories was given funding by the US Department of Energy (DOE) Energy Efficiency and Renewable Energy Solar Energy Technologies Office to create a five-year roadmap for photovoltaic cybersecurity.

This roadmap identified several existing barriers – the unpredictability of cyber threats, the regulatory uncertainty of PV cybersecurity and the insufficient sharing of threat, vulnerability, incident and mitigation information among the government and industry – and set out six clear goals to achieve in the following five years.

The DOE stated in March 2019 that the roadmap was helping to create "a path for improving cybersecurity" where there are "clear roles and responsibilities for government, standards development organizations, vendors and grid operators".

Then in June 2020, the DOE released a cybersecurity roadmap for wind, stating that whilst it was wind-specific, the roadmap's strategies were "likely to be applicable to other forms of energy".