What renewable asset owners need to know about cybersecurity and NIS2 compliance

Cybersecurity continues to grow in importance for solar asset owners. While increasingly sophisticated attacks target our sector, regulators are not standing idle. This April, the European Commission moved to cut funding for solar projects it deems insecure[1]. In parallel, the implementation of NIS2 gives regulators powerful new enforcement tools that can lead non-compliant players to serious financial and operational consequences. In this article, Uri Sadot, Managing Director of SolarDefend and Chair of the Digitalisation Workstream at SolarPower Europe, explains where those risks sit and what action asset owners must take.

In recent years, renewable energy has moved from being an 'additional infrastructure' to being 'critical infrastructure'. This happened because renewables reached a critical mass. Last June, solar energy alone became the main source of electricity in Europe[2], for the first time. As reliance on solar assets grows, the focus at a policy level now shifts from how much energy is produced to how reliably it can be depended upon.

This shift is creating new regulatory challenges around how to ensure this new infrastructure class is secured from cyberattacks. It is also sharpening focus on energy sovereignty, with policymakers increasingly aware of the need to build reliable energy supplies that do not rely too heavily on single-source geographies like China.

After years of dependence on Middle Eastern oil, Russian gas and American liquefied natural gas, Europe does not want yet another digital dependence, this time on China. It seeks a resilient energy system capable of operating through periods of geopolitical instability and global disruption.

To support this, the European Union is rolling out a series of intertwined regulations that include NIS2, the Cyber Resilience Act, the revised Cybersecurity Act, the Industrial Accelerator Act and the Network Code on Cybersecurity, creating a wide 'fishing net' with cross-sector coverage.

What does NIS2 mean for renewable asset owners?

NIS2 raises the number of regulated companies in Europe from thousands to over 160,000[3]. So if you own a few solar plants of about 150 MW in total, the days of being off radar are over. NIS2 gives national regulators the power to hold executives liable and impose fines up to 2% of their parent company's annual turnover. For asset heavy businesses operating on relatively tight margins, this could create significant financial exposure.

The EU aims to increase pressure on industry to invest in secure, sovereign systems. While NIS2 requirements for the solar sector vary by

country, they all place an initial focus on continuous visibility into your plant.

Put simply, visibility means knowing what devices are inside the plant, and how securely they are configured. This translates into continuous asset inventory reporting requirements and conformity audits against recognised standards such as IEC 62443. While it is unclear yet what is meant by 'continuous' visibility, estimates range from annual inventory audits to 'evergreen' real-time monitoring.

For utility-scale asset owners, the guesswork around responsibility is over. Asset owners can no longer rely on complex SPV structures or outsourced operational models to distance themselves from liability. You are now on the regulator's radar, with greater accountability and significant financial consequences for non-compliance, similar to those introduced under GDPR.

Under NIS2, responsibility ultimately sits with the asset owner, as the party that has the authority to implement risk mitigation measures and oversee how the asset is managed. In the event of an audit or a breach, regulators will look closely at who had control and decision-making power across the site and its operations.

As this is a new development for the industry, many asset owner companies do not have a CISO, or an in-house SCADA Director who is responsible for overseeing the compliance conformity process. In those cases, the responsibility lies with the CEO, who will typically assign this responsibility to a Chief Information Officer, a Chief Digital Officer or various other functions within the organisation.

What is the real risk?

Most asset owners, investors, financiers and insurers now recognise that cyber risk is increasing, but there is often less clarity on how that risk manifests itself across renewable portfolios. While NIS2 introduces a new layer of compliance risk, those requirements ultimately exist to mitigate a much broader and growing cyber threat landscape.

Uri Sadot

Every connected asset, whether a solar inverter, wind turbine controller or communications gateway, has a digital point of entry. In theory, securing these systems is no different from securing a physical site. Access should be controlled, monitored, logged and restricted to authorised users, with multiple layers of permissions inside the plant and access rights regularly reviewed or revoked as needed. In reality, this level of control is often inconsistent.

A common challenge lies in visibility. Many portfolios have been built through acquisitions over time, leaving asset owners without a complete inventory of what exists within each site. Legacy devices can remain connected but unmanaged and unpatched, creating blind spots that are difficult to monitor and easy to exploit.

At the same time, third-party access is widespread. OEMs, monitoring providers and control system vendors frequently require remote connectivity that operates without supervision, introducing additional pathways into operational environments that are typically not controlled.

Recent incidents illustrate how these vulnerabilities can be exploited. The coordinated cyberattack in Poland in December 2025[4] demonstrated how attackers can identify weak access points and act at scale. By gaining access to 30 sites simultaneously, including wind and solar plants, the attackers demonstrated that they understand the aggregate risk of distributed solar. Once inside the plants, they disrupted communications, thus denying visibility and control from operators, forcing manual intervention and creating operational disruption.

The losses to plant owners were estimated in tens of thousands of euros per plant, comprising destroyed equipment and weeks of man-hours manually operating the plant onsite. In this case, shutting off energy generation was not the primary target, but the incident could have had far more serious consequences.

A similar cyberattack targeted satellite provider Viasat, as its global communications infrastructure was being used by the Ukrainian military. But as a knock-on effect, German wind farms relying on Viasat for remote monitoring and control lost connectivity, leaving operators unable to manage their assets despite continued generation. The result was over 10 gigawatts of offshore wind capacity[5], a massive amount, being taken offline.

A consistent pattern is emerging. Renewable assets are increasingly connected, reliant on third-party access, and often lacking full transparency over what is happening inside their own networks.

What solutions are available?

Physical cybersecurity infrastructure has historically been underinvested in. Current options come from a small number of providers whose solutions were originally designed for large, centralised power plants. These approaches do not translate easily to renewable portfolios made up of multiple distributed sites with varying configurations, technologies and ownership histories. As a result, many solutions lack the flexibility needed to address the diversity of assets within a modern renewable portfolio.

There are also significant cost challenges. Pricing isn't offered through a scalable model; instead, costs are based on a single gigawatt-scale facility. However, what may be financially viable for a major site is often unviable when applied to smaller plants.

As a result, asset owners are often faced with a choice between solutions that are too costly to scale or too generic to address their specific risks, or both. The industry is still in the process of adapting, and there remains a gap between what regulation is beginning to require and what the available solutions on the market deliver.

In response, a new generation of cybersecurity providers is beginning to emerge, specifically focused on the needs of distributed renewable energy. Rather than adapting legacy approaches designed for large power plants, these solutions are being built from the ground up with the realities of solar and wind portfolios in mind, making them better suited to address the practical challenges asset owners face today.

How asset owners can better protect themselves

For renewable asset owners, the priority now is to move from general awareness to a structured response. This begins internally. Cybersecurity needs to be clearly understood at the executive level, not just as a technical concern, but as a business risk with operational and financial implications. That understanding must translate into budget allocation and clear ownership within the organisation.

Once the budget has been assigned, attention should turn to fundamentals. Remote access must be secured, ensuring that only authorised users can connect and that those connections are properly controlled. Communication architecture between central systems and individual plants needs to be robust and designed with security in mind. Visibility into the plant is critical.

Asset owners need a clear and up-to-date inventory of all devices and systems within their portfolios, alongside monitoring capabilities that provide real-time insight into activity. This is both a fundamental requirement of NIS2 and a tenet of cybersecurity. As the saying goes, you can't secure what you cannot see.

Additional layers of protection can then be introduced. External penetration testing can identify weaknesses before they are exploited. Intrusion detection systems can provide early warning of suspicious activity. Cyber threat intelligence, including monitoring of darknet forums, can offer insight into emerging risks and potential exposures. Given the complexity of modern portfolios, these capabilities are often best delivered by specialist providers who can support ongoing monitoring and compliance.

The takeaway

Renewable energy is becoming more important to the global energy system with each passing year. As with any critical infrastructure, the race is now on to ensure it is secure. Regulation is now firmly in place and is likely to become more demanding. To survive in this environment, asset owners need to adapt with the times. It is therefore critical that renewable energy asset owners get ahead of the curve.

Those who act now will be better positioned to protect their portfolios, demonstrate compliance and navigate what is becoming a far more demanding operating landscape. The question is no longer whether cybersecurity measures are needed, but whether asset owners can implement them quickly enough.

This shift is already visible across Europe. In Italy, the urgency is tangible, with the national cybersecurity agency directly engaging with asset owners and setting a clear expectation that compliance must be achieved by 31st October 2026.

Belgium has also now opened its first NIS2 audit window, marking the beginning of active regulatory enforcement and giving the industry an early indication of what practical compliance scrutiny will look like.

In the DACH region, Germany is taking a leading role in shaping how NIS2 will be applied, with its cybersecurity authority, BSI, actively influencing standards at the EU level, while Austria has already introduced measures around aggregated power production that are expected to expand to Germany.

Although Spain remains one of the last five in the EU yet to formally transpose NIS2 into national law, the Iberian blackout last year exposed structural vulnerabilities, particularly the challenges of operating at the grid edge with limited support from neighbouring countries' energy production and a heavy reliance on renewables.

Across these markets, the message is consistent. While timelines and approaches may differ, the expectation that asset owners take responsibility for cybersecurity is already firmly established and accelerating.

Improving cybersecurity readiness can also help modernise operations. The digitalisation and standardisation needed for cybersecurity often improve efficiency, reducing unnecessary site visits, identifying failing equipment earlier and helping improve overall uptime across renewable portfolios.

For asset owners, the starting point is to find a specialist partner who can help improve visibility across their sites, understand how assets are being accessed, and identify vulnerabilities that may already exist within the portfolio.

solardefend.eu

References

[1] Originally reported by South China Morning Post: https://www.scmp.com/news/china/diplomacy/article/3350056/eu-cut-funding-chinese-inverters-quiet-offensive-replaces-grandstanding.

Subsequently picked up by Euronews: https://www.euronews.com/my-europe/2026/05/04/eu-moves-to-ban-high-risk-inverters-from-china-over-cybersecurity-threats and Reuters: https://www.reuters.com/business/finance/china-strongly-opposes-eu-move-bar-funding-projects-using-chinese-inverters-2026-05-07/

[2] Eurostat: https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20250929-3

[3] Glocert International: https://www.glocertinternational.com/resources/guides/nis2-applicability-essential-vs-important-entities/

[4] CERT Polska: https://cert.pl/en/posts/2026/01/incident-report-energy-sector-2025/

[5] Reuters: https://www.reuters.com/business/energy/satellite-outage-knocks-out-control-enercon-wind-turbines-2022-02-28/ and EnergyWatch: https://energywatch.com/EnergyNews/Renewables/article13782329.ece