RISK AND REWARD

Rafael Narezzi *discusses how the drive for more efficient, transparent renewable energy systems is also creating a rapidly expanding cyberattack surface*

The energy sector is fast becoming one of the most visible and vulnerable targets for hackers and attackers. As energy systems become more digitalised, decentralised, and remotely operated, they are emerging as prime targets for politically motivated attacks, where even a single successful breach can cause widespread disruption.

With the acceleration of renewable energy, as countries strive towards net-zero goals, the stakes have become even higher. This distributed grid model, defined by connected assets like wind farms, solar, energy storage and electric vehicle charging infrastructure, has increased the attack surface. Add to this, the risk of supply chain attacks targeting third-party suppliers open to compromise, and we now have a perfect storm with real-world consequences.

Last year's well-publicised power outage in Spain saw the Spanish Cybersecurity Institute question many of the country's smaller and medium-sized energy providers, notably the solar and wind farms, about their cybersecurity as part of the investigation. While an attack was eventually ruled out – the issue was an unmanaged surge in voltage – it raised serious questions about the possible cybersecurity shortcomings of renewable energy assets.

More recently, the co-ordinated attacks on Poland's power grid – targeting wind and solar farms – are further evidence that threat actors understand just how to manipulate multiple remote locations simultaneously to destabilise critical power networks.

SCADA SYSTEMS RISK IN RENEWABLES

As renewable energy becomes more deeply integrated into critical infrastructure, growing reliance on digital control technologies may be unintentionally increasing the vulnerability of the systems that underpin the energy transition.

Digitalisation is foundational to how wind farms, solar and battery storage sites are managed. Operators rely more on interconnected control systems like SCADA (Supervisory Control and Data Acquisition) and broader operational technology (OT), to monitor performance, remotely control assets and maximise uptime.

From this digitalised landscape, a threat has emerged in the form of a new class of malware built specifically to exploit industrial environments. One example is IOCONTROL, a modular cyber weapon observed in targeted attacks against critical infrastructure.

It is designed to infiltrate and control everything from industrial routers to human-machine interfaces (HMI) and programmable logic controllers (PLC). What's more, it operates with stealth and precision. For renewables operators it is a clear reminder that OT environments are no longer flying under the radar; they are squarely in the crosshairs of attacker's sights.

This stealth is what makes it so concerning. By leveraging legitimate protocols like MQTT – commonly used for machine-to-machine communication in industrial settings – it can blend in with normal traffic, evading traditional detection methods. Its modular design also allows it to adapt to different environments with minimal effort, making it highly portable across different renewable assets, whether that's solar farms or offshore wind installations.

Renewable energy operators often share common SCADA architectures across assets, which, while operationally efficient, becomes a liability when malware is used to exploit these architectures. Attackers gaining a foothold through a vulnerable device, like an unpatched router or internet-exposed HMI, can move laterally, escalate privileges and take control of critical systems. In some cases, the command infrastructure can even be buried within the OT network, enabling long-term persistence without raising alarms.

For renewable energy operators, the consequences are clear. Back-door access into SCADA systems, whether through modular malware like IOCONTROL or other APTs, need to be treated as a frontline cybersecurity issue, requiring a layered approach. This means patching vulnerable endpoints, isolating networks, monitoring for anomalies in protocols like MQTT and deploying platforms that offer deep visibility into OT environments.

Operators rely more on interconnected control systems like SCADA to remotely control assets and maximise uptime

TRANSLATING RISK INTO FINANCIAL IMPACT

Operational downtime and disruption to essential services from an attack are the tip of the iceberg for energy operators. Factor in financial and reputational loss, together with insurance implications and the consequences go very deep indeed. A 98-megawatt wind turbine site, for example, could lose as much as $1.9-million from a week of downtime. By quantifying it in this way, senior executives are better able to understand the real financial consequences and can make informed decisions about relatively modest security investments that significantly reduce their risk exposure as a result.

Compliance is becoming more important and complex too. Look at a sector like banking where cybersecurity is treated as core operational risk. Banks are classified as critical infrastructure, with their licence to operate directly tied to regulatory compliance. Boards and executives are personally responsible. This drives proper budgets, strong cyber hygiene and continuous oversight.

Energy, particularly in renewables, has not fully reached the point where cybersecurity is treated as a core operational risk. Though Centrii is building highly decentralised, digital energy systems that society depends on, the problem is that in many cases, cybersecurity is still treated as a technical issue rather than a leadership responsibility.

To get a better understanding of how cybersecurity is shaping the renewables landscape, last year we collaborated with AECOM on a global survey of senior decision-makers, including senior financial and operational leaders, asset managers, developers and technology providers.

FROM THIS DIGITALISED LANDSCAPE, A NEW CLASS OF MALWARE HAS EMERGED AS A THREAT

There was a mixed response to how businesses are adapting investment and operational strategies in the face of cyber threats. While cybersecurity is recognised as a business risk, renewables companies will need to significantly improve cyber resilience to mitigate the potential consequences of cyberattacks in an increasingly complex geopolitical context.

Respondents in particular noted that regulatory compliance is becoming more demanding, requiring stricter supplier risk management with mandates such as the NIS2 Directive in the EU – an EU directive expanding cybersecurity rules for critical sectors, including energy, with stricter risk management, reporting and penalties.

POOR VISIBILITY

The goal to protect energy generation and energy assets has not changed. It is more important ever. But what has changed is the way companies do it. It's no longer just about technical risk, but evolving to think about financial energy risk. It's no longer about red flags and anomalies, but about uptime, compliance exposure and asset value. It's no longer about risk detection, but the much bigger consequences of energy disruption. For many energy operators, the most common problem is a lack of visibility.

The Poland wind turbine incidents are a clear example; with router hijacking and remote manipulation made possible because connectivity existed without adequate operational visibility. Once edge routers were compromised, attackers could influence dispatch and control layers downstream. This is not a sophisticated espionage story, it is basic connectivity risk compounded by weak monitoring.

This is consistent across the sector with too much trust in vendor connectivity and limited insight into internal OT communications. But also, no financial mapping of what disruption would actually cost. Failure is rarely catastrophic on day one. It's accumulated blind spots that eventually become major operational exposure. In distributed energy systems, visibility is not optional. Without it, decentralisation becomes decentralised risk.

In summary, the rise of renewables like solar and wind is transforming how we generate electricity – and how we live – but it's also opening new doors for cyber threats. Cybersecurity cannot be the afterthought of sustainability and clean energy; it must be the backbone of it. If we don't secure the future of energy, we risk powering progress with vulnerability ●

Picture credit: AdobeStock

THE RISE OF RENEWABLES LIKE SOLAR AND WIND IS TRANSFORMING HOW WE LIVE – BUT IT'S ALSO OPENING NEW DOORS FOR CYBER THREATS

INDUSTRY EXAMPLE

In 2022, a ransomware attack disrupted Deutsche Windtechnik, temporarily cutting off remote access to nearly 2,000 turbines. This attack didn't just cause operational delays; it highlighted how fragile the digital backbone of the renewable sector has become.

CASE STUDY

Three large-scale solar power plants in the UK faced growing cyber threats due to the integration of OT systems. These sites, with a combined capacity of 25MW and capable of delivering clean electricity to over 60,000 homes, operated with a mix of legacy devices and modern networked systems. This made them vulnerable to ICS/SCADA attacks, remote access breaches, a lack of unified visibility across devices, and difficulty in maintaining NIS2-level compliance.

To address this, a multi-layered approach was implemented, combining 24/7 monitoring with policy-driven controls, resulting in a 40 percent reduction in incidents within three months, improved NIS2 audit readiness, operation uptime and systems performance, and also investor confidence.

SURVEY STATS

The majority (95 percent) of asset owners interviewed allocate only 1 or 2 percent of annual revenue to cybersecurity, integrating it into broader risk management rather than treating it as a standalone priority

One in ten companies surveyed stated they had already suffered a cyberattack, highlighting the immediate and growing risks facing the industry

70 percent believe cyber threats will significantly worsen in the near future and cite supply chain vulnerabilities as a top concern

With modern cyber attackers leveraging AI and automation, 96 percent of respondents report automated and AI-enhanced cyberattacks as a growing concern

Despite this, only 18 percent of companies regularly upgrade critical network security equipment, such as routers and firewalls.

Source: AECOM Insights

Rafael Narezzi is the Co-Founder of Centrii (formerly Cyber Energia) and an OT cybersecurity expert with over two decades of experience as a business and technology leader for global enterprises.

OT environments are no longer flying under the radar; they are squarely in the crosshairs of attacker's sights