The trusted megawatt: cyber resilience you can evidence

Hybrie De Jager, Compliance Specialist at Centrii, examines how NIS2 is reshaping cyber resilience in the wind sector, from supplier risk and governance to operational recovery, and why operators need to be able to evidence a 'trusted megawatt'.

PES: Hybrie, thank you for joining us. Cybersecurity has been a priority for the wind industry for some time, but the conversation is moving beyond technical protection. How is the arrival of NIS2 changing the way organisations think about cyber resilience?

Hybrie De Jager: A cyber incident does not follow the organisational structure around a wind farm. It can spread across turbine systems, remote connections and supplier relationships, while authority remains split between owners, asset managers, O&M providers and technology partners. NIS2 changes less about the number of controls required and more about how closely management oversight is linked to decisions made under pressure.

The real test comes in the first hour of disruption. Who sees enough of the picture to act, and who can disconnect a supplier or

suspend generation? The measure that matters is decision latency: the time between the first warning and a coordinated, authorised response.

PES: Early enforcement suggests NIS2 is about much more than ticking compliance boxes. What has changed, and why are governance and accountability becoming as important as cybersecurity itself?

HdJ: In wind energy, cyber resilience has grown from a technical concern about protecting systems into an organisational capability that tests whether the whole operating ecosystem can recognise disruption and act with a single purpose. NIS2 reinforces that shift by placing cybersecurity within governance, where management bodies must approve risk management measures and prove that supply chain and continuity arrangements work in practice.

Governance sets the priorities and risk boundaries; accountability keeps decision-making authority visible once activities are delegated. That matters because a wind farm may be owned by one entity, managed by another and supported by several specialist suppliers, each performing its role without anyone seeing the complete picture.

PES: Some Member States are already moving into active supervision, with Lithuania among the early examples. What lessons are emerging, and what should Europe's wind sector be paying attention to?

HdJ: Lithuania is an early indication of cyber resilience moving from policy into active supervision of the energy sector. Its focus on control system cybersecurity audits and declarations for generation and storage assets shows assurance becoming tied to evidence from the asset itself rather than corporate policy alone.

The deeper lesson is that cybersecurity is moving closer to the operational credibility of generation. Installed capacity no longer tells the whole story; what matters is whether output remains safely controllable and recoverable during digital disruption. This suggests a new strategic concept: the trusted megawatt, generation supported by secure control systems, clear accountability and demonstrated recovery.

PES: The renewable energy sector has its own unique challenges, from operational technology and distributed assets to complex supply chains. How do these characteristics make NIS2 compliance different for wind operators compared with other industries?

HdJ: NIS2 applies common principles across critical sectors, but in wind those principles meet a distinctive operating reality. Wind operators must preserve trusted control of generation across dispersed and often unmanned assets that run operational technology with long lifecycles and narrow patching windows, tied directly to worker safety and grid interaction. They also depend on suppliers who may each control part of the environment or hold essential evidence.

Recovery is therefore rarely a matter of restoring data alone. It means safe turbine control, verified configurations and a carefully sequenced return to generation. Compliance becomes credible only when generation remains trustworthy under digital pressure.

PES: Cybersecurity has traditionally been viewed as an IT responsibility, but NIS2

seems to place much greater emphasis on organisational leadership. Tell us what that means in practice for boards, executives and operational teams.

HdJ: NIS2 does not turn directors into cybersecurity operators, but it makes cyber risk much harder to treat as someone else's responsibility. The management body is expected to approve risk management measures and oversee their implementation; executives translate that direction into authority and investment, while technical teams and suppliers implement the measures and provide the evidence that they work.

The strategic issue is decision architecture, because every unclear handover during an incident consumes time. If remote access appears compromised, who may suspend it? If an OEM recommendation conflicts with local operational concerns, who has final authority? Mature accountability answers those questions before the incident, so that trusted information reaches a person empowered to make the consequential decision.

PES: The wind industry relies on an extensive network of suppliers, manufacturers and service providers. How should organisations approach third-party risk under NIS2, and what are the biggest pitfalls to avoid?

HdJ: Leaders need to look past supplier lists and understand the chain of operational capabilities around each asset. A manufacturer may provide remote diagnostics while an O&M provider administers access, and the most consequential risk often sits in the handover between them. Conventional assurance falls short: commercial spend does not indicate operational importance, and a promise of emergency support means little if it has never been exercised.

The stronger objective is portable resilience. A wind farm need not duplicate every supplier record, but it must retain tested, contractually enforceable access to the information, authority and recovery support it needs within regulatory timescales. An organisation may delegate activity, but a megawatt is not fully trusted if its resilience belongs to someone else.

PES: Organisations increasingly need to evidence how cyber risk is governed and managed. What documentation, reporting or audit trail should operators be thinking about now to show they meet regulatory expectations?

HdJ: What NIS2 rewards is a traceable record of how a cyber risk moves from discovery to decision, treatment and verification. The valuable evidence is not the volume of policy documentation but the ability to reconstruct what happened: the issue identified, the authority exercised, the exception accepted and the improvement that followed.

That record becomes an organisational memory. People and suppliers change, but the reasoning behind material decisions remains available, and reporting can then show ageing exceptions, recurring weaknesses and recovery results rather than a single compliance percentage. Over time, it can also connect issues to the capacity affected and the investment required.

PES: As organisations prepare for NIS2, where do you see the biggest misunderstandings? Are there areas where companies believe they are well prepared, but in reality still have significant gaps?

HdJ: The greatest gaps usually sit outside traditional control assessments. An asset-owning entity may retain accountability while the critical work is performed by asset managers, O&M providers and manufacturers, leaving logs, patch information and recovery evidence outside the organisation. A procedure can look complete even when the information needed to use it is dispersed across several parties.

Add unclear authority for installing OEM updates, incomplete oversight of supplier identities and uncertainty over who determines that an incident is reportable, and you have a preparedness illusion: controls look mature individually while their dependencies remain untested. Readiness is revealed at the boundary, where responsibility and action must move between organisations quickly enough to protect the wind farm.

PES: For operators that are still on their NIS2 journey, where should they focus their efforts over the next 12 months to strengthen both compliance and cyber resilience?

HdJ: Start by confirming scope, leadership oversight and the principal gaps against the applicable risk management and incident reporting requirements. The work then becomes tangible through a trusted megawatt trace. Rather than mapping the entire ecosystem at once, take one dependency critical to generation, such as turbine remote access or an OEM control platform, and follow it from management oversight down to wind farm operation.

Establish who controls the system, who can authorise action, where the evidence is held and what happens if that supplier becomes unavailable. Then test whether the parties can recognise disruption and begin recovery. One trace will not complete NIS2 preparation, but it exposes real gaps while creating a repeatable method that can be applied gradually across further dependencies.

PES: As enforcement gathers pace across Europe, how do you see expectations evolving over the next few years, and what does 'good' cyber governance look like in a mature, resilient wind organisation?

HdJ: Expectations will move from periodic compliance reviews towards continuous, evidence-led assurance of how wind farms are controlled, monitored and recovered. At the same time, digital twins, cloud-connected

Hybrie De Jager

platforms and selective uses of AI will increase visibility while creating new dependencies on connectivity, data quality and external providers.

Mature governance will therefore operate as a decision system rather than a committee structure. Leadership will understand which technologies support critical generation, what authority has been delegated and how the wind farm reaches a safe state when technology fails. Where automation influences operational decisions, the conditions for human intervention must remain clear, because automated action must not create unowned consequences. The outcome is a trusted generation portfolio.

PES: If there was one piece of advice you would give wind operators preparing for increasing regulatory scrutiny, what would it be?

HdJ: Treat the next wave of European regulation as a connected development rather than a series of separate compliance projects. NIS2 focuses on organisational resilience, the Cyber Resilience Act strengthens vulnerability management across the lifecycle of digital products, and the AI Act and the EU's Strategic Roadmap on digitalisation and AI in the energy sector show how governance is evolving as energy technology becomes more automated.

Reassuringly, they rest on many of the same foundations, so operators do not need a separate operating model for each new instrument. A common digital assurance spine, giving visibility of connected products, critical suppliers, vulnerabilities and recovery capability, can serve regulatory reporting, incident response and future technology adoption alike. Organisations that move early turn regulation into operational confidence: clearer authority, better supplier relationships, safer adoption of technology and a generation portfolio that remains trusted under pressure.

The strategic question for wind leaders is no longer only, 'Are our systems secure?' It is, 'How much of our energy generation remains trusted when technology, suppliers and decision-making are tested at the same time?'

centrii.com