
Is your biggest cyber risk the one you cannot see coming?
The better the question. The better the answer.
The better the world works.
EY
Shape the future with confidence

From generation plants to transmission and distribution systems to interconnectors, the assets operated by the UK's power and utilities sector are critical to the proper functioning of our economy and society. To fulfil this role more effectively, companies are deploying new technologies to digitise and automate their operations and interactions at a rapid pace. The benefits in terms of greater efficiency, reliability and sustainability are clear. But so are the downside risks – not least around cybersecurity.

Recent experience has underlined this issue. Over the past few years, several power operators have suffered cyber attacks that have disrupted their operations and raised wider questions about the resilience of our critical energy infrastructure. And these are not isolated incidents. Research by the security vendor Semperis has found that **62% of UK electricity and water utilities were targeted** by cybercriminals in the past year – with more than half of these suffering disruption or data loss as a result.

Two converging shifts

For power and utilities operators, the threat of cyber attack isn't new: evidence suggests it's been growing steadily since 2018. But what is new is the acute nature of the threat. And it's now being exacerbated by two parallel sets of shifts — one external to power companies, and one internal.

Externally, geopolitical instability is causing the threat landscape to evolve and expand at a rate never seen before, as sophisticated, well-funded state-sponsored attackers become increasingly active alongside financially motivated cybercriminals. Regulators are responding with more intrusive requirements around cyber disclosure and resilience, intensifying the imperative for companies to act.

And internally, the shift to green energy is pushing the sector to become more digitalised and increasingly reliant on data to balance demand and supply. This results in an expanded and more attractive attack surface for cyber adversaries. A particular challenge is that rising connectivity across a vast array of assets and devices is resulting in operational technology (OT) facing the same level of threat as information technology (IT) — meaning it now requires even more protection.

Four actions to strengthen cybersecurity: and how to take them

Bottom line? As new tech-savvy entrants come into the energy market, any incumbent power company that fails to embrace new technologies is putting its future survival at risk. But if it pursues digitisation without putting cybersecurity front and centre of its strategy and thinking, the risks may be even greater.

With this in mind, here are four actions that power and utility organisations can implement today to strengthen cybersecurity across their business and operations. Every working day, we're supporting clients across the sector in taking these steps – helping them realise the full benefits of digital technology without compromising on cyber resilience.

1 | Involve cyber from the start of every initiative – including through "security-by-design"

Whether you're planning the construction of a new power plant or connecting up a renewable asset to the grid, it's vital to take cybersecurity into account from the get-go – not treat it as an afterthought. The EY Global Cybersecurity Leadership Insights Study 2025 found that the earlier the chief information security officer (CISO) is involved in a project, the greater the business value created. However, this early involvement isn't happening often enough: only 13% of CISOs in our study said they were consulted early when urgent strategic decisions were being made – yet those CISOs also reported creating more value than those who were consulted either late or not at all.

With power companies increasingly adopting agile approaches to developing digital services, an effective way to ensure the right cybersecurity input from day one is to adopt "security by design", embedding security features from the very start of the initiative. This approach is vital when developing Artificial Intelligence (AI) solutions – which are pivotal to managing the supply from intermittent renewable sources, and depend on a mass of real-time data that presents an attractive attack vector.

The need to involve cyber from the start also extends well beyond solution development. For example, any acquisition or expansion into a new market or geography may open up cyber risks that must be recognised and tackled in advance.

2 | Secure the supply chain by understanding third parties' exposure

Many recent cyber breaches across various industries have resulted from attackers gaining access to core systems via third-party suppliers. This risk is on the rise in power and utilities, as the ongoing decentralisation and digitalisation of the energy system sees a growing number of vendors and ecosystem partners join the supply chain. The risk for power companies is that some of these third parties may have less rigorous security measures in place, making it vital to assess their cyber defences before linking up with them.

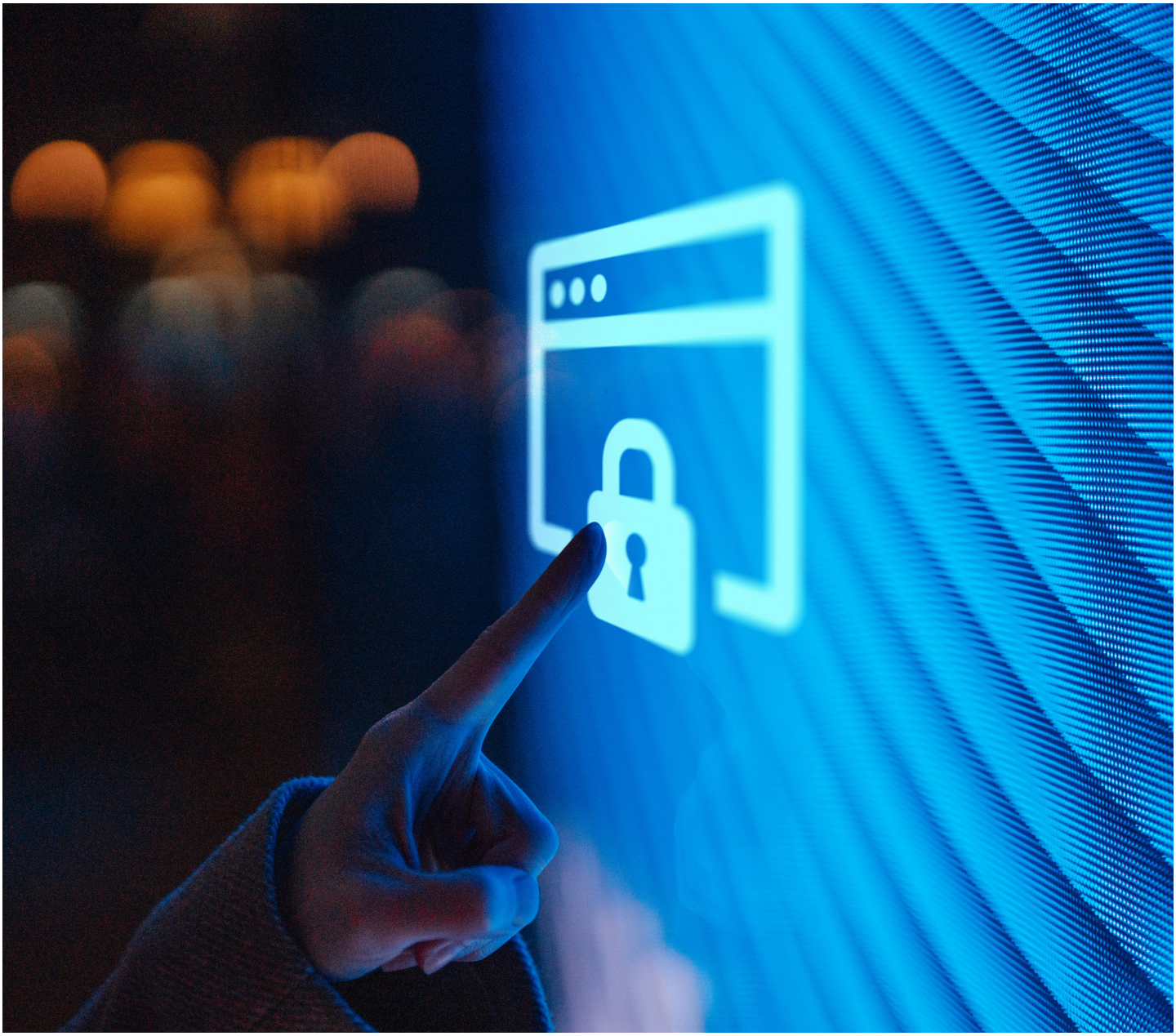
At the same time, power companies' rising adoption of cloud services and remote access capabilities is introducing greater openness and creating new potential entry-points. The overall effect is to trigger a move away from the traditional approach of blocking access and towards new methods of monitoring and detection.

3 | Build workforce-wide awareness and organisational preparedness for cyber incidents

An organisation's preparedness for cyber threats comes down to its ability to detect, manage and recover from cybersecurity incidents when they occur — as they inevitably will. A vital component here is embedding cyber awareness and readiness at all levels, from the individual employee to the organisation as a whole.

Recent EY research has found that 64% of CISOs are not satisfied with the adoption of cybersecurity best practices by their non-IT workforce, underscoring a need for better employee training. Other important elements include having clear incident response processes and procedures in place, and reporting lines for escalating issues when employees spot something amiss.

More generally, it's key to ensure that cybersecurity is regarded not as a siloed activity for the CISO's team but as everybody's problem and responsibility, including across senior teams. In this context, a valuable activity that we undertake with many clients is running crisis simulation exercises, as described in the accompanying information panel.



Crisis simulations: putting senior decision-makers through their cyber paces

For these exercises – which are increasingly popular with clients – we bring together a group of senior executives or board members and play out an as-live scenario of a cyber incident. We make the situation as realistic as possible through elements such as real-time updates and simulated news stories, and monitor the executive team's reactions and decisions. At what point do they inform the regulator? The employees? The media? Do they take services down or seek to keep them running? And in the aftermath, how do they manage remediation and guard against a recurrence? After the exercise, we provide detailed feedback on team dynamics and decision-making, and help the client act on any lessons learned – for example by developing formal documented processes or delivering cyber awareness programmes.

4 | Zero in on OT and Internet of Things (IoT) cybersecurity – integrated with IT

Historically, most operational technology used in power and utilities companies didn't require a dedicated cybersecurity capability as it wasn't connected to external systems or networks. And in cases where OT security was a potential issue, the management and monitoring of the environment was largely left to IT.

But with OT assets and devices increasingly becoming connected to the IoT, this piecemeal approach is no longer fit for purpose. The rising adoption of renewable generation infrastructure such as offshore wind farms is further blurring the boundaries between IT, IoT and OT, with the bi-directional data flows for remote monitoring and maintenance driving a substantial expansion in the organisation's overall attack surface.

All of this makes it vital to implement governance and policy-level standards specific to OT, taking account of the requirements for OT cyber compliance, including specialist training for OT cybersecurity teams. Meanwhile, activities such as security monitoring and threat detection should be an integrated joint effort between OT and IT.

Building cyber resilience for the digital era: no time to lose

For the UK power and utilities sector, the digital era is here, bringing major benefits for companies, customers and society. But without the right cybersecurity those benefits will be undermined by unnecessary risks. And with attacks on the rise, and the vulnerabilities of digital infrastructure growing, cyber incidents now pose a serious threat to national security and economic stability.

Against this background, the priority is to strengthen the resilience of both the power sector as a whole and the businesses within it. The four actions we've outlined provide a roadmap that will help to do this.

Ask yourself this simple question: Is your organisation fully prepared for the cyber threats it faces? If not, it's time to act. To find out more about how to secure your energy assets, operations and supply chain against cyber attacks, please reach out to:

Alex Campbell
UKI Industrials and Energy Cyber Leader
acampbell2@uk.ey.com

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multidisciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

EYG No. 006675-25Gbl
ED None

UKC-040404.indd (UK) 10/25.
Artwork by Creative UK.

ey.com