littlefish CYBER SERVICES GROUP | INSIGHT REPORT



HIGH STAKES SECURITY

Understanding Cyber Risk in Energy & Utilities

E&U Insights Survey by Littlefish Group in partnership with Censuswide

CENSUSWIDE

CYBER SERVICES

A note from Sean Tickle, Cyber Services Director

Energy and Utilities organisations operate at the intersection of digital dependency and public obligation. Power generation and distribution, water treatment, gas networks, and field operations depend on systems that need to remain available, trusted, and secure – often under intense regulatory and societal scrutiny.

The good news is, over recent years, cyber security maturity across the sector has improved. Investment has increased, awareness is higher, and many organisations now have stronger foundations in place. The findings in this report reflect that progress, with few leaders believing their organisation is unprepared for a cyber incident.

Confidence does not exist in isolation, though – and it's not the same as resilience.

Energy and Utilities environments are inherently complex. They blend IT and operational technology, often rely on ageing infrastructure, and must balance innovation with resilience in ways few other sectors face. In this context, preparedness is not only about tools and controls, but about how well people, processes, and systems hold together under pressure.

This report explores that complexity. It examines where confidence is well-placed, where cyber risk is felt most acutely, and which investments are delivering meaningful risk reduction. It also introduces a sector specific resilience model designed to help organisations strengthen security without slowing progress or innovation.

Kind regards,



Sean Tickle,
Cyber Services Director



CYBER SERVICES

Confidence is high, but pressure remains

One of the most striking findings in the research is the strength of confidence across the sector:

92% **of Energy & Utilities IT leaders say they feel prepared for a cyber incident.**



39% **describe themselves as "very prepared".**

This level of confidence reflects sustained and deliberate effort across cyber security, governance, and operational resilience. Over recent years, organisations across the sector have invested heavily in strengthening core controls, improving oversight, and embedding cyber risk into broader operational and regulatory decision-making. Incident response planning has matured, assurance frameworks have expanded, and cyber resilience is now more commonly understood as a business issue rather than a purely technical one.

Importantly, this confidence has not developed in a vacuum. The UK energy and utilities sector has had to respond to real-world incidents, regulatory intervention, and increasing scrutiny around the resilience of critical national infrastructure. High-profile ransomware attacks, supply-chain compromises, and near-miss events have reinforced the need for better preparation, clearer accountability, and stronger coordination between IT, operational teams, suppliers, and leadership.

However, confidence does not eliminate exposure.

When leaders are asked how cyber incidents might affect their organisations, the risks they identify reveal where pressure still sits – particularly around regulatory compliance, reputational trust, and the potential for disruption across complex, interconnected environments.

"In Energy & Utilities, cyber incidents are judged as much by regulatory and reputational impact as by their technical severity."

CYBER SERVICES

Cyber risk seen through a business lens

Rather than centring risk around technical failure alone, Energy and Utilities leaders frame cyber risk in terms of business and societal impact.

Top business risks associated with cyber incidents:



33%
Regulatory fines or compliance breaches

30%
Reputational damage and loss of trust

26%
Loss of highly-sensitive data

26%
Operational disruption or downtime

It shows that cyber risk in this sector is tightly linked to regulation, public confidence, and licence to operate. Compliance breaches can trigger scrutiny from regulators such as Ofgem and NCSC. Reputational damage can undermine trust in services that communities rely on daily. Operational disruption may not always be prolonged, but its consequences can be immediate and visible.

Cyber resilience here is therefore less about achieving perfection and more about ensuring continuity, accountability, and credible control when incidents occur.

CYBER SERVICES

Prepared – but for what, exactly?

HIGH CONFIDENCE DOES NOT AUTOMATICALLY SUGGEST COMPLACENCY – BUT IT DOES DESERVE SOME SCRUTINY.



Energy and Utilities organisations operate across mixed estates where nothing is simple by default. Cloud platforms sit alongside legacy systems that were built decades ago. IT environments are tightly intertwined with OT. Third-party suppliers play critical roles in keeping services online. Each layer adds dependency, constraint, and potential exposure.

Preparedness in this reality is rarely neat or evenly distributed.

Organisations, therefore, may feel confident in core IT controls while still accepting uneven assurance across field systems, specialist OT environments, or complex supply chains.

For me, that tension is not a weakness. It reflects a sector that understands cyber risk as something that must be managed continuously, not solved once and forgotten.

"Preparedness in complex environments is rarely absolute."

CYBER SERVICES

The OT, cloud, and hybrid reality

One factor shaping cyber risk perceptions is the growing convergence of IT and OT.

Many legacy OT systems were not designed with modern cyber threats in mind; they can lack visibility, segmentation, or the ability to patch effectively and respond to threats rapidly. At the same time, cloud adoption and SaaS platforms are expanding the digital perimeter, increasing reliance on identity, APIs, and third-party services.

This creates a layered risk profile:

OT introduces availability and safety concerns.

Cloud introduces identity-centric attack paths.

Hybrid estates increase complexity and reduce uniform control.

PREPAREDNESS HERE ISN'T ABOUT HAVING CONTROLS IN PLACE; IT'S ABOUT KNOWING WHERE RISK LIVES AND MAKING DELIBERATE CHOICES ABOUT HOW IT'S PRIORITISED AND CONTROLLED ACROSS THESE ENVIRONMENTS.



CYBER SERVICES

Where cyber investment is delivering real impact

With investment levels high across the sector, our survey asked a practical question: where is spending actually reducing risk?

Best reduction in risk per £ invested:



Endpoint Detection & Response (EDR/XDR)



Multifactor Authentication (MFA)



Security awareness and phishing training



Identity & access management (IAM)



Patch automation and vulnerability management

Notably, these are foundational IT controls rather than emerging technologies.

Their effectiveness lies in limiting attack paths, shortening detection times, and reducing exposure windows. They also apply across hybrid environments, making them particularly valuable in mixed IT/OT estates. However, OT environments have a level of criticality and complexity which means that slightly different tact is required to be effective.

Crucially, these controls deliver the most value when aligned. For example, identity without monitoring, or detection without response, limits impact.

"The biggest gains come from fundamentals implemented well, not from chasing novelty."

CYBER SERVICES

Shifting investment: from expansion to optimisation

While foundations are strong, our survey results also point to an active reassessment of value across Energy and Utilities.

We know that many organisations are reviewing penetration testing approaches in the context of the sector's evolving threat landscape – alongside identity governance tooling, overlapping endpoint and cloud security platforms, and OT-specific detection and response capabilities, as well as managed security arrangements.

This reflects a shift from expansion to optimisation.

Rather than adding more tools, leaders are asking whether existing investments are delivering measurable risk reduction, and whether complexity is being introduced faster than it can be effectively managed.

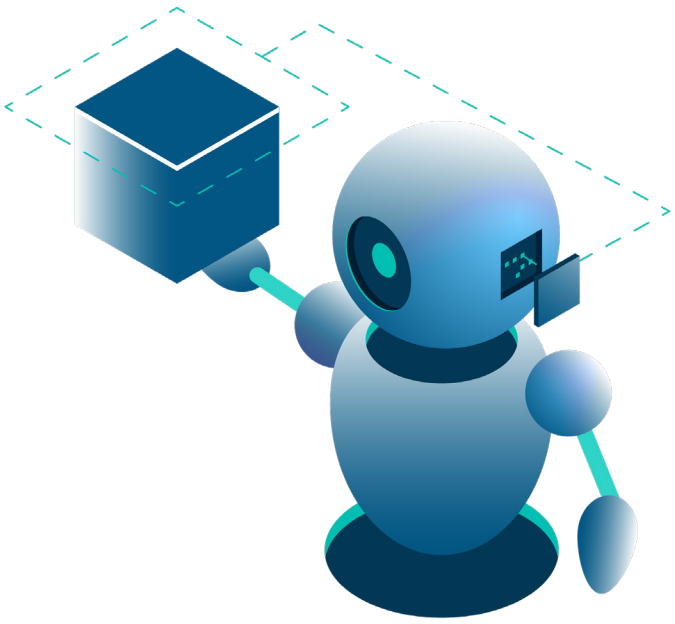
This moment of reassessment is a natural stage of maturity and a sign that cyber risk is being treated as an operational discipline, rather than a technology arms race.

AI, innovation, and emerging risk

Although not the central focus of this report, AI – as always these days – sits in the background offering both opportunity and risk. Automation, analytics, and predictive monitoring are increasingly part of Energy and Utilities operations, but they also introduce new attack surfaces, dependencies, and governance challenges.

Sector leaders appear to recognise that AI adoption must be balanced with assurance, after all, confidence in innovation is strongest where identity, data governance, and monitoring foundations are already mature.

Future resilience will depend not only on adopting new technology, but on understanding its impact on risk and accountability before it becomes business-critical.



CYBER SERVICES

A resilience model for Energy & Utilities

Taken together, the survey findings show that resilience in Energy and Utilities is not driven by any single control or investment. Instead, it emerges where strong technical foundations are supported by operational readiness and aligned with real business priorities.

The results point towards a practical resilience model built on three interconnected layers:

1. Technical foundations

Investment is delivering the strongest risk reduction where core controls are applied consistently – particularly identity, endpoint protection, patching, and monitoring. These fundamentals matter most in mixed IT, OT, cloud, and hybrid environments, where uneven coverage quickly becomes exposure.

2. Operational readiness

Confidence is shaped by more than tooling. The data reflects awareness that preparedness is tested when incidents cut across systems, suppliers, and teams under pressure. Clear ownership, rehearsed response, and decision-making defined in advance are what allow organisations to act decisively when plans meet reality.

3. Business alignment

The way leaders rank cyber risk highlights what resilience must protect: regulatory confidence, service continuity, and trust. This points to security decisions that support innovation and compliance together, rather than competing with operational priorities.

ORGANISATIONS STRONGEST ACROSS ALL THREE LAYERS ARE BEST PLACED TO ABSORB INCIDENTS WITH LIMITED DISRUPTION AND MAINTAIN CONFIDENCE UNDER SCRUTINY.



"Resilience is not achieved through tools alone, but through alignment between technology, people, and decision-making."

CYBER SERVICES

Closing reflections

This research doesn't suggest a sector unaware of risk – but one that understands just how quickly conditions can change.

It shows Energy and Utilities organisations working with pragmatic confidence: conscious of the progress they've made, clear-eyed about where exposure still exists, and increasingly focused on what genuinely strengthens resilience rather than simply adding more controls.

The real opportunity now lies in closing the gap between feeling prepared and performing well when pressure hits. That gap closes through clarity of ownership, rehearsal under realistic conditions, and regular validation through services like tabletop exercises and penetration testing – alongside alignment across people, processes, and priorities (rather than technology alone).

Preparedness, in this context, comes down to maintaining control when uncertainty becomes unavoidable.

If the themes in this report reflect conversations already happening within your organisation, you're certainly not alone. Across Energy and Utilities, leaders are reassessing what resilience means as regulatory pressure increases, threats evolve, and digital dependency deepens.

If you'd like to explore how these insights apply to your environment, or where improvements across cyber security and resilience can be made, we're always open to continuing the conversation.



littlefish GROUP

CENSUSWIDE

THE RESEARCH CONSULTANTS

The research was conducted by Censuswide, among a sample of 300n IT leaders (aged 21+) in the UK in NHS and Energy and Utilities. The data was collected between 18.02.2026 - 04.03.2026. Censuswide is a member of the Market Research Society (MRS) and the British Polling Council (BPC), and a signatory of the Global Data Quality Pledge. We adhere to the MRS Code of Conduct and ESOMAR principles.