Transforming Energy & Utilities Operations

How to Build a Secure, Compliant, and Data-Driven Future

storm
a littlefish company

littlefish
GROUP

Table of Contents

Foreword

Having spent the last 15 years working within highly regulated industries, particularly across the energy and utilities sector, Tim specialises in technology modernisation. Improving operational resilience and navigating complex regulatory and market pressures through cloud-enabled operating models, data-driven decision-making, and digital programmes that support a more efficient, customer-centric, and low-carbon future.

In this e-book, Tim examines the critical challenges currently shaping the energy and utilities landscape and outlines the technologies that can help combat these challenges. Leveraging vast industry expertise, Tim provides a comprehensive digital strategy to help organisations confidently navigate the future of the energy and utilities sector.

Tim Bayliss

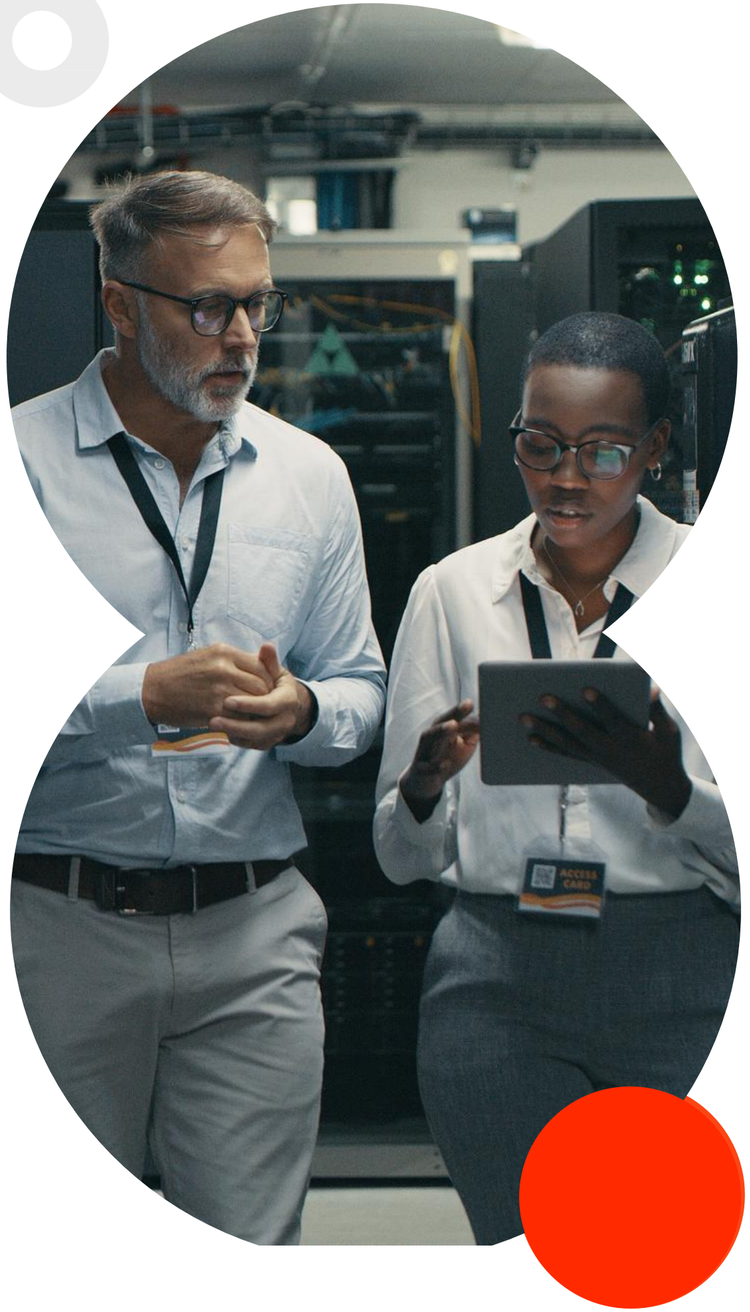
Head of Energy & Utilities
Littlefish

Navigating Complexity in the Energy & Utilities Sector

The energy and utilities sector across Irish and UK markets is undergoing a significant transformation. Driven by shifting customer expectations, technology advancements, heightened regulations, and ambitious goals to meet net zero targets, organisations are under increasing pressure to innovate and modernise operations while maintaining efficiency, security and compliance. In order to remain competitive and progress towards sustainability goals, energy providers, network operators and utilities must evolve to become data-driven, technology-enabled enterprises. However, to achieve this ambition such organisations must overcome a number of obstacles.

Legacy infrastructure remains prevalent with data often fragmented across operational technology and information technology environments. Globally, cyber threats continue to grow in sophistication and organisations storing large amounts of customer data, as in the energy and utilities sectors, make for prime targets. Meanwhile, the rise of generative artificial intelligence introduces new opportunities, but also new risks, particularly in relation to data security, governance and compliance. For organisations operating critical national infrastructure, these risks carry heightened consequences.

Technology leaders in energy and utilities must therefore adopt a pragmatic, structured approach to digital transformation. This involves not only upgrading systems, but ensuring that security, governance and compliance are embedded into the core of operations.



Challenges Facing the Energy & Utilities Sector

This eBook will explore some of the most pressing challenges facing the energy and utilities sectors today and outline how modern solutions can help organisations address them effectively, securely and at scale.

Cybersecurity Threats

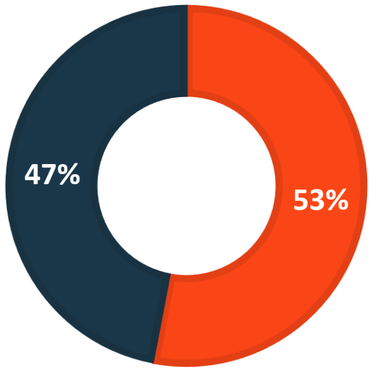
Cyber threats are becoming increasingly prevalent worldwide, with Deloitte estimating that the global cost of cybercrime will reach $10.5 trillion by the end of 2025. Energy and utilities organisations are increasingly attractive targets for cybercriminals. As critical infrastructure providers, disruptions can have widespread societal and economic impact, making security breaches particularly high-risk. The expansion of digital systems, remote monitoring, and cloud platforms has increased the attack surface, while legacy security models often struggle to keep pace with modern threats.

The rapid adoption of generative AI further amplifies these risks. While AI has the potential to optimise operations, enhance forecasting, and improve customer engagement, it also introduces new vulnerabilities. In fact, 53% of leaders say AI is creating new attack points for which they're unprepared.

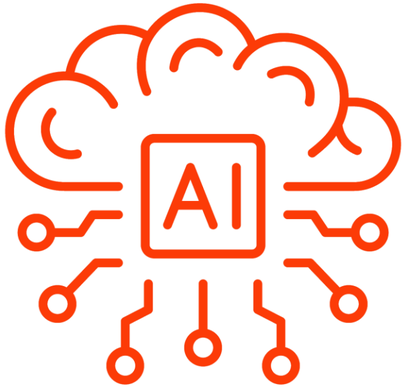
Poorly governed AI models can expose sensitive operational or customer data, while malicious actors may exploit generative AI to automate phishing attacks or probe systems at scale. Without robust oversight, organisations risk data leakage, regulatory breaches, and the erosion of stakeholder trust.

For energy and utilities providers, cybersecurity is no longer solely an IT concern. It is a board-level priority that must span people, processes and technology. Organisations need advanced threat detection, real-time visibility across environments, and a clear framework for governing AI use across the business.

The global cost of cybercrime will reach **$10.5 trillion** annually by the end of 2025.



53% of leaders say AI is creating new attack points for which they're unprepared.



Only **37%** report having processes in place to assess the security of AI tools before deployment.

Sources: Deloitte, World Economic Forum, Viking Cloud.

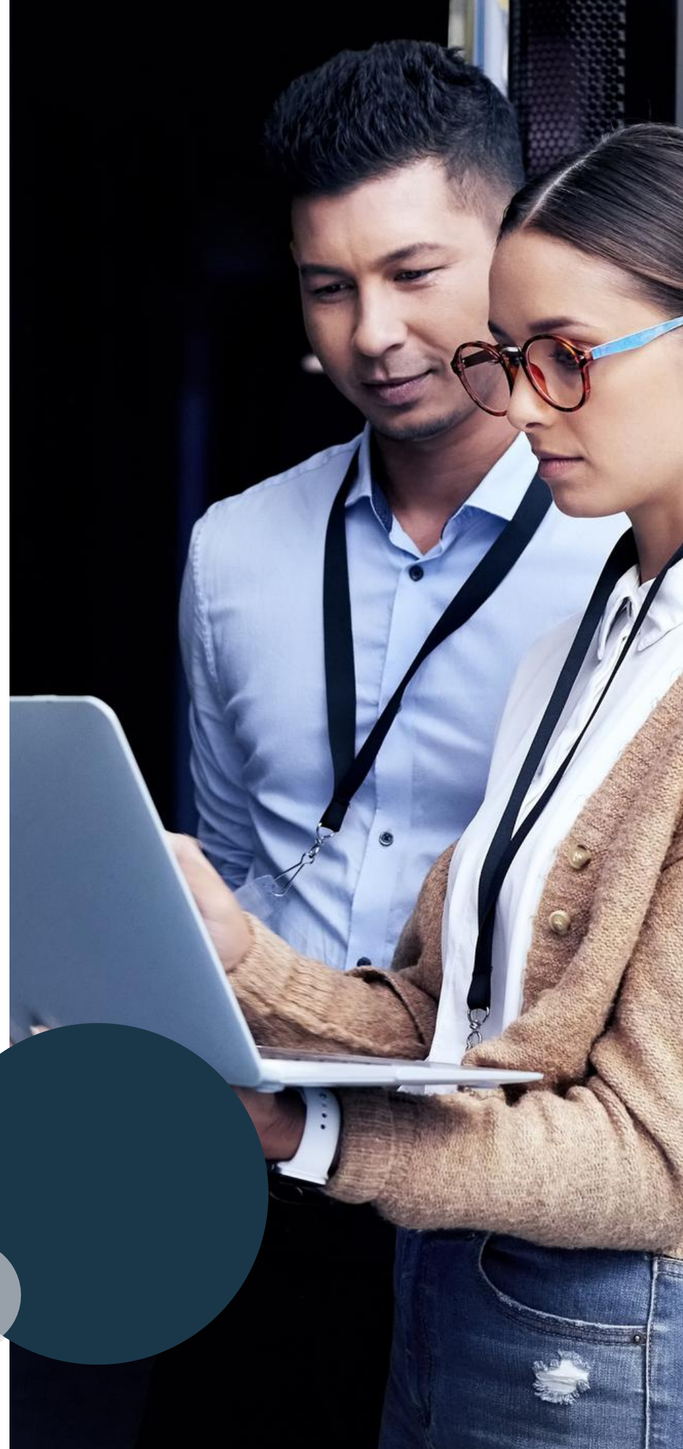
Advancing Threat Intelligence

To counter these evolving risks, organisations must prioritise investment in advanced threat intelligence and security platforms that can operate at enterprise scale. Cybersecurity solutions such as Microsoft Sentinel and Microsoft Defender provide integrated, cloud-native security capabilities that help organisations detect, investigate and respond to threats across.

Microsoft Sentinel enables security teams to aggregate data from across the organisation, correlate signals and apply machine learning and behavioural analytics to identify threats that could otherwise go unnoticed. This is particularly valuable in complex energy environments where data is generated across endpoints, networks, and cloud services. Microsoft Defender extends protection across identities, endpoints, applications, and data, helping organisations adopt a zero-trust security posture that is essential in the context of critical infrastructure.

Equally important is robust data governance, especially when considering generative AI use. Microsoft Purview supports organisations in understanding where sensitive data resides, how it is being used and how it should be protected. By classifying data, enforcing policies and monitoring access, organisations can reduce the risk of data exposure while enabling responsible AI adoption.

Technology alone, however, is not sufficient. Upskilling the workforce in AI security is a critical component of resilience. Energy and utilities organisations must ensure that employees understand how AI tools are used, where risks arise and what proper governance looks like in practice. By combining advanced security platforms with strong data governance and workforce education, organisations can harness the benefits of AI while safeguarding critical assets and maintaining regulatory confidence.

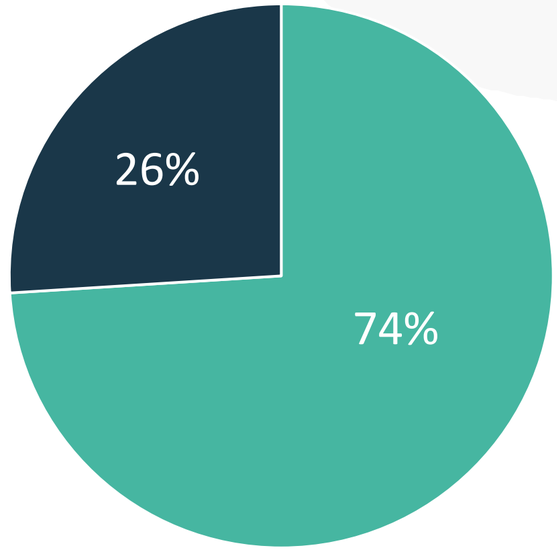


Outdated Infrastructure and Fragmented Data

Many energy and utilities organisations still rely on ageing infrastructure and a patchwork of legacy systems that have evolved over decades. Operational data may be spread across asset management systems, customer relationship management (CRM) systems and financial applications, often with limited integration between them. In fact, 74% of IT Leaders admit their data sits across a number of fragmented systems, according to Storm's 2025 Modern Workplace Report. This fragmentation makes it difficult to achieve a single, trusted view of operations and hinders the ability to respond quickly to change or unforeseen problems.

In an environment where real-time insights are increasingly essential, fragmented data can create a tangible operational risk. Workers may lack visibility into asset performance, demand patterns or network resilience, while decision-makers are forced to rely on manual processes and potentially inaccurate reports. The result is inefficiency, increased cost and reduced agility at a time when the sector must adapt rapidly to issues like changing consumption behaviours and new regulations.

Further, legacy platforms can inhibit innovation. Integrating advanced analytics, AI, or predictive maintenance capabilities becomes significantly more complex when data is siloed and inconsistent. For organisations that want to modernise, data fragmentation is often one of the most significant barriers to progress.



74% of IT Leaders say their data sits across a number of fragmented systems.

Unifying Data

Addressing these challenges requires a move towards a unified data architecture that brings together operational, financial and customer data into a single, coherent platform. Microsoft Fabric provides an end-to-end data and analytics solution that enables organisations to ingest, store, analyse and visualise data at scale.

By consolidating data into a unified data platform, energy and utilities organisations can break down siloes and establish a single source of truth. Microsoft Fabric supports real-time analytics, advanced reporting and AI-driven insights, allowing teams across the business to access consistent, trusted data. This is particularly valuable in operational environments where timely insight can improve asset reliability, reduce downtime and support proactive maintenance. Consolidating data in one system also helps simplify governance processes by allowing organisations to apply the proper access and security controls, data classification, and lifecycle management policies from one central platform.

A unified data platform also creates a strong foundation for future innovation. With clean, well-governed data in place, organisations can more easily deploy AI models, integrate new digital services and respond to regulatory or market changes. This approach does not require a complete overnight replacement of existing systems. Instead, organisations can adopt a phased modernisation strategy, integrating legacy systems into a modern data platform while progressively retiring outdated technology.

For energy and utilities providers, investing in a unified data platform is not just about efficiency; it's about building the digital backbone required to support a more resilient, flexible and sustainable energy system.

Evolving Industry Regulations & Governance

Regulatory oversight in the energy and utilities sector continues to intensify across both the UK and Ireland. Organisations must comply with a complex web of national and regional regulations covering data protection, cybersecurity, financial and ESG reporting and, of course, the use of AI. Failure to meet these obligations can result in significant financial penalties and reputational damage. Organisations are expected to demonstrate not only compliance, but control - clear audit trails, robust reporting and documented decision-making processes. Some key regulations include:

Pillar Two Rule

Requires multinational businesses to pay tax on profits in each jurisdiction it operates in, requiring businesses to provide detailed country-by-country reports.

Corporate Sustainability Reporting Directive

Requires many organisations to track and report carbon emissions categorised by 3 predefined scopes.

EU AI Act

Regulates the use of AI and requires strict AI governance protocols.

Additionally, both the UK and Ireland have set ambitious net zero targets for 2050, meaning businesses need to reduce emissions and report on their environmental impact.

For many organisations, existing systems are not well equipped to manage this level of regulatory complexity. Manual processes, disconnected reporting, and limited governance frameworks can increase the risk of non-compliance and put additional strain on teams.

Modernising ERP

Upgrading Enterprise Resource Planning (ERP) systems is a critical step in strengthening regulatory compliance. Modern ERP platforms like D365 Business Central provide integrated financial, operational and compliance capabilities, enabling organisations to standardise processes, improve data accuracy and generate auditable reports with confidence. By consolidating core business functions into a single system, organisations can reduce manual intervention and ensure that regulatory requirements are embedded into day-to-day operations. Further, users can view and report financial data in multiple currencies across different locations and update exchange rates within the system to help streamline Pillar Two reporting processes.

Business Central also provides built-in sustainability reporting features to help businesses track and manage their carbon emissions based on the categories defined by EU standards, making it much easier to remain compliant with the CSRD.

AI Governance Frameworks

Beyond ERP, organisations must establish robust internal governance frameworks for AI implementations to ensure compliance with evolving AI regulations. This includes defining clear ownership for AI systems, setting policies for data usage, and ensuring that AI outputs can be monitored and explained where required. Governance frameworks should be aligned with existing risk management and compliance structures, ensuring consistency across the organisation.

Effectively implementing strong governance frameworks will provide clarity, reduce risk and help build trust with regulators, customers and stakeholders. By combining modern ERP capabilities with disciplined AI governance, energy and utilities organisations can confidently navigate regulatory complexity without stifling innovation.

Building a Secure, Compliant, and Data-Driven Future

The energy and utilities sector across the UK and Ireland stands at a pivotal juncture, and digital transformation is the key to unlocking success. By implementing robust security and governance tools, unifying business data, and modernising systems, businesses can better navigate complex industry challenges. With the right technology and strategy in place, energy and utilities providers can not only mitigate risk, but unlock new opportunities for efficiency, innovation and sustainable growth. In doing so, they will be better positioned to deliver secure, reliable and compliant services while building a resilient foundation for the future.

Transform your Business with Littlefish Group:
UK: www.littlefish.co.uk
IRE: www.storm.ie