resill!on

Assure. Secure. Innovate.

Powering electricity's continued evolution

The three key questions that energy companies need to answer

Introduction

Electricity's role on the road to Net Zero is almost impossible to overstate. In Europe alone, up to three-quarters of final energy consumption will need to be electrified if climate neutrality is to be achieved by 2050[1]. Considering that the current figure stands at around 23%, the need for a rapid—and far-reaching—electrification programme grows clearer by the day.

The UK is no stranger to that challenge. Specific projections vary, but electricity demand here is on course to at least double by 2050[2]. Even that (fairly modest) expectation will require significant investment into critical electrical infrastructure, with transmission and distribution networks amongst the key priorities.

These events aren't playing out in a vacuum, of course. As continents and countries alike grapple with the need to supercharge their production capabilities, move to renewable generation, and unlock the potential of Distributed Energy Resources (DER), suppliers, distributors, and more are taking their own strides towards a smarter future. Distribution network operators (DNOs) in particular are investing considerable amounts into both data management and digitalisation initiatives alike[3].

Some of that spend is mandated, with Ofgem's Energy System Digitalisation programme designed to ensure that operators keep pace with innovation. Enforced or not, however, the continued transformation of the industry creates an entirely new set of challenges for energy companies to contend with. Chief amongst those is the need for an evolutionary approach to systems management.

From data to devices, now more than ever operators need to know that their technology ecosystem is fit for purpose. Moreover, they need to know that it's fit for the future, ready to support them across what promises to be a decades-long journey towards a brighter, cleaner, and more efficient horizon.

In this eBook, we're looking at what that means in practice. As they navigate these pressing digitalisation challenges, we'll look at three key questions that energy companies need to ask themselves—and why finding the right answers will help set them up for tomorrow.

[1] Net Zero? It's all about electrification – Wind Europe, 23rd October 2023
[2] Electricity Networks Strategic Framework: Enabling a secure, net zero energy system – Department for Business, Energy & Industrial Strategy / Ofgem
[3] The digital future of electricity networks – Frontier Economics

Integration issues

The days of discrete technology environments are behind us. Today, the focus is on cohesive ecosystems—connected networks in which operational technology (OT) and information technology (IT) converge to create something that's more than the sum of its parts.

The key question

How do operators bring operational and information technology systems together, without their transformation efforts grinding to a halt?

The trend towards OT/IT convergence promises a wide range of benefits, not least the fact that it's integral to the concept of grid modernisation, allowing as it does for real-time monitoring and the management of dynamic energy flows. All told, convergence paves the way for greater operational efficiency, greater reliability and resilience, the application of advanced analytics and AI, and much more.

At the same time, convergence can also create serious compatibility and integration problems. Not only is the energy industry heavily reliant on legacy OT—systems that don't tend to integrate well with modern IT—those technologies typically come parcelled with proprietary protocols and have limited connectivity capabilities too. As a result, even getting to the point which OT can be onboarded into the wider ecosystem can be a challenge.

The difficulties posed by OT/IT convergence don't end there, though. Energy companies employ a wide range of systems, devices, and data types across the generation, transmission, and distribution of electricity. Integrating those systems effectively—and ensuring that they're sufficiently interoperable—is a considerable technical challenge. That's particularly true when it comes to devices that require near-real-time operations such as smart meters.

Finally, the coming together of operational and information technology has ramifications from a security perspective, too. The security and stability of OT is a mission-critical concern for operators, and integration with IT may increase the risk of those systems being compromised.

Bringing it all together

For an ecosystem to function effectively, every component within it needs to 'play nice' with the others. If they don't, any attempt at modernisation will fall apart fast. The only way to ensure that won't happen is to put those components through their paces. It's here that the importance of conformance and interoperability testing begins to show.

This is a two-step process. Conformance testing assures a solid foundation: that individual components comply with written standards and requirements, thus avoiding wasted effort building a system that doesn't actually function. Interoperability testing, on the other hand, is primarily about validating performance and delivery of the high level use cases those standards were aiming to address. Legacy equipment—not just new components—may be included in that process.

The combination of these steps typically helps to uncover any ambiguity in written standards, and even the existence of unwritten and assumed requirements. Ultimately, that leads to significant improvements in what is an iterative and ongoing process.

Naturally, there are numerous advantages to a rigorous approach like this. As well as helping to enhance the safety and reliability of their technology ecosystems, conformance and interoperability testing can also help energy companies to improve efficiency and optimise performance. More than anything, though, conformance and interoperability testing gives them the guarantee of seamless functionality—a critical capability on the path to tomorrow.

> Utilities investing into OT/IT convergence typically see a return on investment within 12-18 months, primarily as a result of reduced downtime and greater operational efficiency.
>
> **Source:** How sustainable practices can drive inclusive growth in modern business, EY

Resillion leading the way on DSR interoperability

The UK Government's Department for Energy Security and Net Zero is running a programme to accelerate the development of interoperable demand side response (DSR) systems for the domestic electricity market. This programme has received funding from the government's £1 billion Net Zero Innovation Portfolio, which provides funding for low-carbon technologies and systems. Decreasing the costs of decarbonisation, the Portfolio will help enable the UK to end its contribution to climate change.

The Interoperable Demand Side Response programme involves a number of consortiums, including leading developers of energy flexibility platforms and manufacturers of high-consumption domestic appliances such as heat pumps, EV charge points, and battery storage systems. Each consortium is developing energy smart appliances (ESAs) and demand side response service platforms (DSRSP).

The Resillion-led consortium, also including a UK Distribution Network Operator, PNDC (Power Networks Demonstration Centre) from the University of Strathclyde, and Quality Logic, has designed and built a demonstration environment in which various combinations of ESAs and DSRSPs will undergo days of testing based on real-world-like use cases in order to verify their end-to-end interoperability.

Testing times

Today's energy companies run on software. From the ubiquitous enterprise resource management (ERP) and customer relationship management (CRM) systems to sector-specific applications for managing infrastructure and smart meters, software is the backbone of modern energy operations.

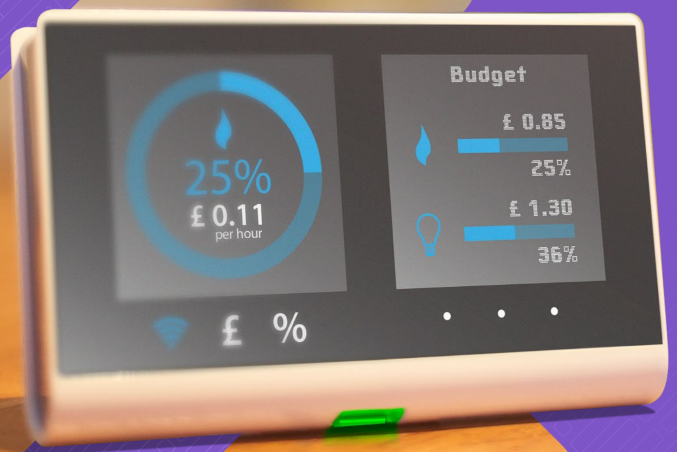
The key question

In a complex and ever-evolving software environment, how do companies guarantee the quality of their apps and services?

Managing this complex software estate is understandably difficult. Many of these systems are interconnected—meaning a minor failure in one can cascade into larger problems across the network. For instance, a bug in a billing system could lead to a host of issues—from inaccurate energy usage readings or delayed tariff updates—that impact operational efficiency and customer satisfaction.

There are challenges of speed here, too. In today's competitive energy markets, there's tremendous pressure deliver new services to market quickly—particularly in customer-facing areas such as electric vehicle (EV) integration and smart energy solutions. In the case of pricing, energy firms need to apply hundreds of tariff changes across their smart meter estate every year.

The upshot of this is that energy companies need round-the-clock assurance about the stability of their software environment—and that's something that can only be accomplished through a robust testing programme.



Automating testing for speed and accuracy

Energy companies aren't necessarily set up with software testing in mind. But the transition to digital has changed the game.

For a start, software testing is a deeply technical pursuit, requiring a great deal of specialist expertise and experience. Not only is that difficult to resource from a skills perspective, there's little sense in doing so when there are other, better testing options.

Given these resources pressures, the sheer complexity of today's systems, and the rapid pace of change within the energy sector, automated testing is only scalable approach.

Replacing slow, error-prone and manual processes, automated testing allows companies to test software continuously and at scale. This is especially critical when considering the need for hundreds, if not thousands, of tariff changes each year. Each one must be rigorously tested to ensure accuracy across the smart meter estate, billing systems and more. Manual testing simply can't keep up.

Automated testing is carried out quickly and consistently, ensuring that new tariffs, updates, and other software changes don't disrupt existing systems or lead to errors that could affect customer trust. A leading UK Distribution Network Operator, for example, has embraced automated testing and reaped significant benefits including faster release cycles, greater test accuracy, and a reduction in the costs associated with manual testing. Working with test automation specialists like Resillion, the energy giant has been able to innovate more rapidly and deliver new services to market with greater confidence.

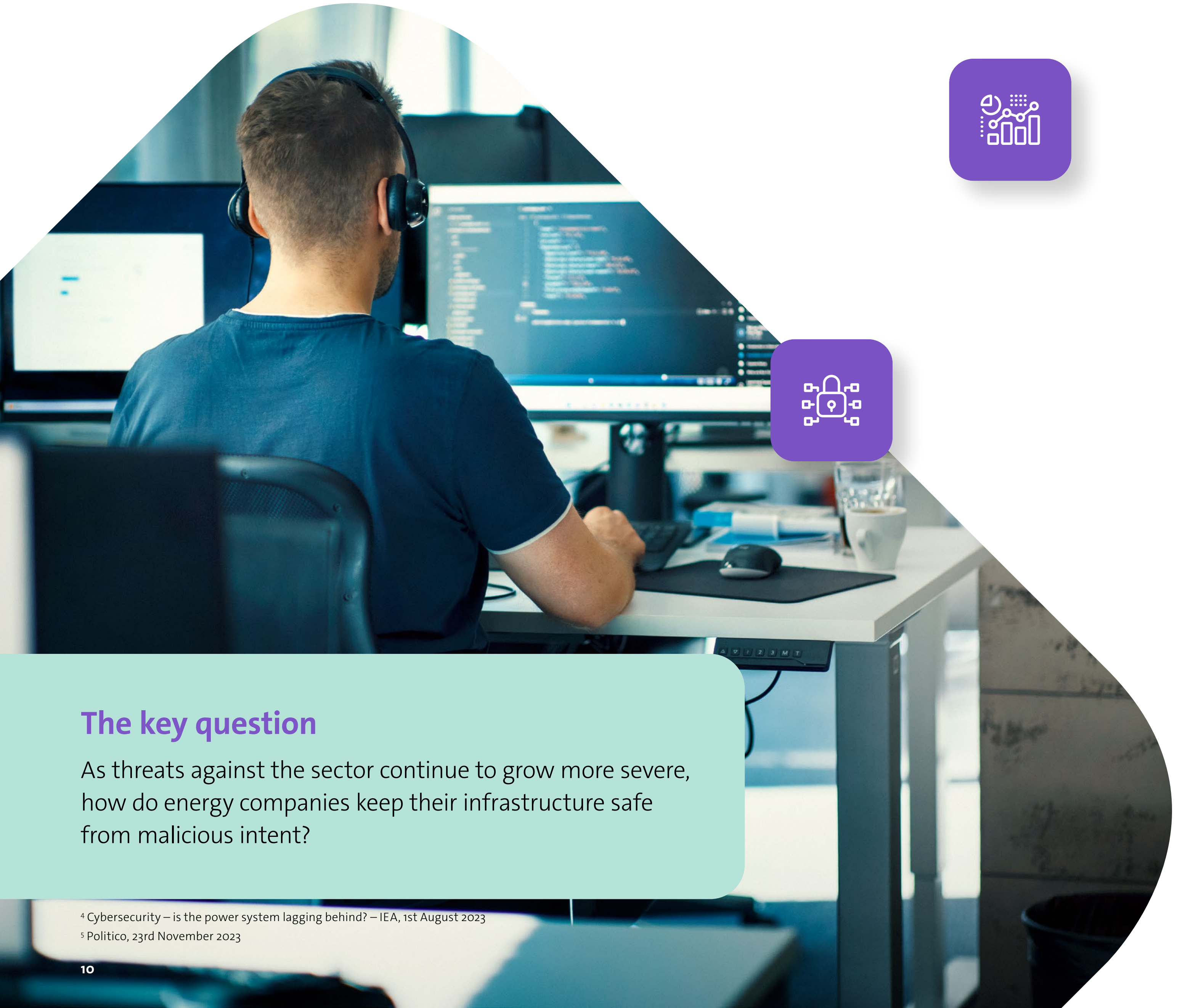
Moreover, regulatory compliance is another area where automated testing proves invaluable. With the rise of half-hourly meter readings and other regulatory requirements, energy companies must make sure their systems are always up-to-date and functioning correctly. Automated testing delivers this capability.

Plus, for added assurance, independent quality verification—carried out by third-party providers like Resillion—makes sense. By validating both automated and manual approaches, companies can be confident in the accuracy and reliability of their testing.

By automating software testing, UK Distribution Network Operators have reduced manual intervention, accelerated testing cycles, and improved accuracy—enabling faster, more reliable deployment of tariff updates across its smart meter network.

Strengthening security

A lot has changed over the past few years, not least the state of the threat landscape. Between 2020 and 2022, for example, the number of cybersecurity attacks aimed at utilities more than doubled. According to the International Energy Agency, 504 recorded incidents rose to 736 in 2021, before hitting a peak of 1,101 a year later[4]. As one media outlet puts it, "Europe's grid is under a cyberattack deluge[5]."



The key question

As threats against the sector continue to grow more severe, how do energy companies keep their infrastructure safe from malicious intent?

Fast forward to May 2023 and 22 companies forming part of Denmark's energy infrastructure were attacked—with a number having to go into island mode operation[6]. While July 2024's global Windows outage was reported to have impacted utilities, utility regulators and the U.S. Department of Energy[7]. This latter incident was more cyber-related than cyberattack—caused, as it was, by a faulty software update from security firm CrowdStrike. It certainly serves to highlight the need for both cyber-resilience and comprehensive testing.

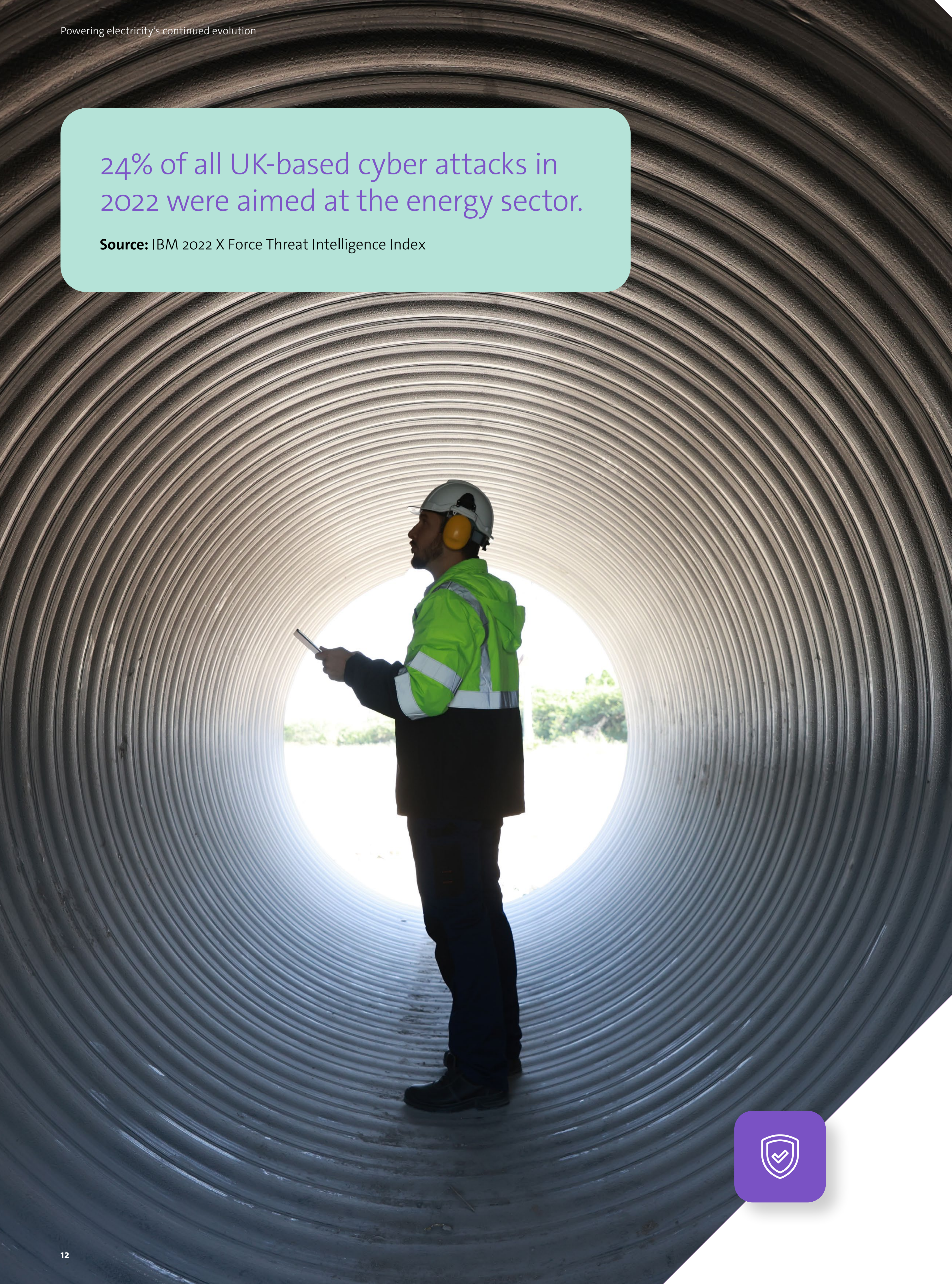
How many of those attacks were specifically aimed at energy companies is unclear. What isn't difficult to ascertain, however, is the impact that a cyber incident can have on the target. When Colombia's Empresas Públicas de Medellín was hit by a BlackCat/ALPHV ransomware attack, the company was forced to advise its 304,000 prepaid energy customers to visit a physical office in order to receive a recharge code for their meters[8].

The other certainty here is just how rapidly the "attack surface" is expanding in the energy sector. The shift towards DER has created new vulnerabilities, for instance[9], mainly because it has increased the number of potential points of entry. So too has the push towards the Internet of Things, smart grids, and the convergence of operational and information technology that we covered earlier. The industry is getting smarter, but it is becoming a bigger target as a result.

Threats themselves are becoming smarter, too. 85% of the cyberattacks witnessed by security professionals in 2024 so far have been powered by Generative AI[10]. The need for iron-clad protection has never been greater.

[4] Cybersecurity – is the power system lagging behind? – IEA, 1st August 2023
[5] Politico, 23rd November 2023

[6] The attack against Danish critical infrastructure — SektorCERT, November 2023
[7] CrowdStrike outage impacts DOE, utilities, and regulators — PowerGrid International, 19th July 2024
[8] EPM Falls Victim To Ransomware Attack – Finance Colombia, 14th December 2022
[9] The energy transition means increased attack surfaces for hackers – Power Technology, 18th July 2024
[10] The Need For AI-Powered Cybersecurity to Tackle AI-Driven Cyberattacks – ISACA, 23rd April 2024



24% of all UK-based cyber attacks in 2022 were aimed at the energy sector.

Source: IBM 2022 X Force Threat Intelligence Index

Security in a regulated world

Against this backdrop, it's little wonder that regulators are putting so much emphasis on cybersecurity. There's NIS2, the European Union's cybersecurity guidance for sectors that are "vital for our economy and society[11]". There's the UK's own NIS Regulations 2018, to which an update is expected imminently. And then there's Ofgem's comprehensive RIIO-2 Cyber Resilience Guidelines, which address a wide range of issues that from data and device management through to supply chain risks.

The other twist here, of course, is the possibility that power company directors could find themselves personally liable for cybersecurity breaches. Legal action of that kind has already been launched in the United States, and authorities in the UK may eventually choose to follow suit[12]. With that in mind, it's now in any management team's best interest to push cybersecurity even further up the agenda that it already is today.

Much like software testing, the primary issue here is the sheer scale of the challenge. As noted above, energy companies aren't just being targeted more often—they're also faced with defending a much bigger "surface" against an increasingly sophisticated set of threats. Because of that, their approach to security needs to be truly end-to-end—from regular vulnerability assessments and proactive risk management to emergency response, and more strategically-focused security engineering. This is complex stuff and support from a dedicated, vendor-agnostic third-party specialist can be of tremendous value here.

Ultimately, the only way for an energy company to be sure about the strength of its defences today is to adopt a "no-stone-unturned" policy. Every weakness, every possible point of vulnerability, needs to be identified, tested, sealed off—and then continually monitored to ensure that it can't be reopened. Compliance—and the future of the UK's critical infrastructure—depends on it.

[11] Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) – European Commission

[12] Directors face personal liability over cybersecurity failures – White & Case, 6th January 2023

Delivering assurance in energy

Today, achieving your goals means accelerating product and service time to market, seamlessly integrating IT/OT systems, implementing robust cybersecurity measures, and staying ahead of regulatory changes. But the challenges are numerous: costly infrastructure upgrades, complex technology integrations, and the pressure to balance ongoing transformation initiatives while maintaining grid resilience.

As your trusted assurance partner in energy, Resillion is here to assist. From building robust converged ecosystems and simplifying product development lifecycles to protecting critical infrastructure, we've brought together a comprehensive set of assurance services in a unique offer—giving you the capabilities you need to innovate with confidence.

Here are just some of the ways in which Resillion can help:

Integrate with assurance

Compatibility problems and integration issues in today's fast-converging OT and IT environments threaten to put the brakes on energy transformation. From smart meters to DER, our agnostic approach and specialist interoperability and conformance testing services eliminate compatibility issues to accelerate delivery of your critical national infrastructure projects.

Transform through testing

With speed and assurance key to success, our automated, repeatable testing services give you the tools to take new digital products and solutions to production faster. Now, with continuous development, testing and integration across your applications, systems and platforms, you can reduce release cycles, secure your estate and accelerate digital transformation.

Secure the future

Critical national infrastructure is under threat. Energy firms need the most robust defence. From advisory and assessment to cybersecurity testing, SecOps and expert incident response, our co-ordinated approach assures Ofgem compliance and protects your assets, data and people.

Comply with confidence

With regulations fast evolving, staying current—and compliant with Ofgem requirements—is key to protecting revenues, reputations and relationships. Our deep energy domain expertise, regulatory insights and end-to-end assurance services give you the tools you need to comply with confidence.

For more on how Resillion can help you answer the hard questions and assure your energy transformation, get in touch at hello@resillion.com

resill!on

Assure. Secure. Innovate.

www.resillion.com/energy