STRIKE THE RIGHT BALANCE

Nick Haan *reveals if the UK's Cyber Security and Resilience Bill will be enough to protect critical infrastructure*

With international tensions continuing to escalate, the threat of cyberattacks on critical infrastructure looms large. Energy networks, transport systems, and healthcare providers, among others, are increasingly under threat from state-sponsored actors seeking economic disruption or geopolitical leverage. In the wake of the latest crisis in Iran, the NCSC issued warnings of increased cyber risk, specifically highlighting critical national infrastructure (CNI) operators.

Many governments have responded by strengthening cybersecurity regulations specifically designed to protect essential services. In the EU, the NIS2 Directive introduced stricter reporting requirements, broader sector coverage and greater accountability for leadership teams responsible for managing cyber risk. The UK is following suit with its proposed Cyber Security and Resilience Bill, which aims to update the country's existing regulatory framework and expand protections for infrastructure providers.

Policymakers and CNI operators alike must ask if the UK can afford a softer resilience regime at a time when attacks on infrastructure are becoming more frequent and more disruptive. The growing urgency around infrastructure cybersecurity is closely tied to the technologies that now underpin modern essential services. Energy grids, transportation networks, manufacturing plants and healthcare systems rely heavily on cyber-physical systems (CPS) – environments in which digital networks directly control physical equipment and operational processes.

Because these operations have a foot in both the digital and physical worlds, they provide threat actors with a unique opportunity. Compromising digital networks connected to CPS can shut down transportation grids, cause blackouts and leave hospitals without access to critical systems.

Last year's colossal power blackout in Spain and Portugal is a prime example of the impact energy infrastructure disruption can have

Most infrastructure operators also operate within increasingly complex digital ecosystems. Supply chains now involve large networks of partners, contractors and service providers that require some level of access to operational systems. These sprawling supply chains provide attackers with even more opportunities to infiltrate network environments. Claroty's research found that 46 percent of organisations have experienced a breach caused by third-party access in the last 12 months, while 49 percent say changes in supply chains driven by geopolitical or economic pressures are increasing cyber-physical security risks. Together, these factors are making infrastructure one of the most attractive and strategically valuable targets in the cyber threat landscape.

Against this increasingly hostile and unpredictable threat landscape, the UK's proposed Cyber Security and Resilience (CSR) Bill is intended to strengthen the country's ability to protect essential services from cyber threats. Building on the existing Network and Information Systems (NIS) regulations, the legislation aims to expand regulatory oversight, improve incident reporting and ensure organisations responsible for critical services take cybersecurity much more seriously.

After several delays, the CSR Bill is currently making its way through the governmental process and continues to evolve, most recently making more provisions for data centres as CNI. In its current form, it's a good foundation and certainly a welcome update to the rapidly ageing NIS regulations from 2018. However, it is grappling with the same challenges we always see with technology-based legislation.

Many regulatory frameworks are written at a high level to remain flexible as technology evolves. Too much specificity around specific technology can quickly leave a law or regulation irrelevant or restrictive when tech moves on. But while this flexibility can be helpful, it can also create uncertainty about what organisations are actually expected to do in practice. At the moment, there is still limited detail about how the UK's new legislation will translate into concrete operational requirements for infrastructure operators.

Without clear expectations, organisations may struggle to determine what compliance actually requires. This can lead to regulatory compliance becoming a procedural exercise rather than a driver of genuine resilience.

Accountability is another critical factor. Declaring stronger defences in legislation is one thing, but ensuring organisations are held accountable when those defences fail is another. As we've seen many times, regulations must have teeth if they are to deliver real change, and this is especially important when we're talking about protecting critical infrastructure. With economic stability and public safety on the line, the UK cannot afford for its long-awaited bill to end up as little more than a compliance checklist.

Delays to the UK's CSR Bill have put the country even further behind its continental neighbours. The EU has moved ahead at a faster pace, with the NIS2 Directive coming into effect at the end of 2024. Replacing the EU's original Network and Information Systems legislation, NIS2 significantly expanded both the scope and the enforcement of cybersecurity obligations for organisations operating essential services.

The Directive brings a wider range of critical sectors into scope and introduces stricter requirements around incident reporting, supply chain risk management and governance. One of the most significant changes is the emphasis on leadership accountability. Responsibility for cybersecurity resilience sits at the board level of organisations, rather than being treated purely as a technical issue handled by security teams.

The UK may eventually incorporate some of these principles into its own legislation, and elements of NIS2 are likely to influence the final shape of the Cyber Security and Resilience Bill. There is still uncertainty about how closely the UK will align with the European framework and whether enforcement mechanisms will be as robust. However, while the

GOVERNMENTS CAN HELP SUPPORT CRITICAL OPERATORS WITH MORE SPECIFIC GUIDANCE

EU is at least two years ahead of the UK in terms of getting regulations through, the adherence to NIS2 among member nations has been patchy to say the least. Some countries, like Germany, stand out as strong examples, particularly through existing frameworks like KRITIS and the BSI cybersecurity authority. But many others are lagging behind and have already missed their initial compliance deadlines. The UK's singular governmental status should be an advantage compared with this piecemeal progress, but it must learn from Europe's stronger examples and enact meaningful change.

Both NIS2 and the forthcoming UK CSR Bill have expanded the scope of cyber best practice around supply chains. However, this remains one of the most persistent weaknesses in infrastructure security and is still under-addressed.

Modern critical infrastructure relies on a complex ecosystem of vendors, contractors and service providers who require varying levels of access to operational environments. Over time, infrastructure environments often accumulate multiple remote access tools, vendor accounts and maintenance channels introduced by different suppliers or operational teams. The full extent of these connections is rarely understood until organisations take specific action to map them. This creates a complicated access landscape that is difficult to monitor and secure. It's a vulnerability that is well understood by threat actors, and compromising poorly secured suppliers and remote access pathways is a primary attack tactic for reaching operational systems.

As mentioned, our own research found that nearly half of organisations have experienced cybersecurity breaches linked to third-party vendor access in the past year. As a result, 73 percent are currently reassessing how remote access to cyber-physical systems is managed. As infrastructure supply chains become more digital and interconnected, managing these

Picture credit: AdobeStock

external access relationships is a central element of building cyber resilience.

OT environments are typically designed for reliability and longevity rather than security. Many industrial systems remain in service for decades and cannot easily be replaced or upgraded. Many assets currently in operation were built for very different threats and even predate the digital revolution

DELAYS TO THE UK'S CSR BILL HAVE PUT THE COUNTRY EVEN FURTHER BEHIND ITS NEIGHBOURS

entirely. This creates unique security constraints. OT environments tend to have a high proportion of proprietary systems that are not compatible with standard IT management and security tools. Strategies and tool stacks designed around traditional will encounter significant blind spots in OT environments, leaving gaps for threat actors to slip in.

Patching software vulnerabilities, which is routine in IT environments, may not always be possible where downtime could interrupt critical services. In many cases, taking operational systems offline for maintenance simply is not an option.

Operators must ensure their tools and processes include specialist capabilities that can see and engage with OT systems. This is critical for understanding what assets exist within their environments, how they are connected and how they support operational processes. Without that visibility, prioritising risk and responding to threats becomes extremely difficult.

Compliance alone is rarely enough to ensure that critical infrastructure is genuinely resilient. To make a difference, regulations on securing critical infrastructure need to focus on establishing a genuine understanding of risk. This begins with a simple question: what systems would cause the greatest disruption if they stopped working?

Security programmes should begin by identifying which systems would have the most significant operational, environmental or safety consequences if compromised. Once those systems are understood, organisations can begin mapping the dependencies that support them and prioritising protections accordingly.

This impact-driven approach allows infrastructure operators to focus security investments where they matter most. Instead of attempting to address every vulnerability equally, organisations can concentrate on protecting the systems whose disruption would have the greatest real-world consequences. Getting to this point doesn't require regulations to focus on, or even acknowledge, specific technical systems.

For example, much as it's essential to understand the difference between IT and OT, that distinction matters far less than the impact the system has on operations, safety or the environment. If a system affects the continuity of a business, the well-being of people or the safety of infrastructure, it needs to be protected – regardless of its classification.

Governments and other bodies can help support critical operators with more specific guidance, but keeping the regulatory focus on visibility, understanding and accountability keeps it relevant and timely, regardless of specific environments and changing technology.

As threats evolve, governments must ensure regulatory frameworks keep pace with modern infrastructure risks. The UK's Cyber Security and Resilience Bill represents an important acknowledgement that stronger protections are needed for essential services. However, legislation alone will not guarantee that infrastructure is adequately protected.

The real measure of success will be whether frameworks drive meaningful improvements in how organisations manage risk across their cyber-physical environments. That requires clear expectations, stronger accountability and a focus on protecting the systems whose disruption would have the greatest societal impact. Ensuring their security demands a strategic approach that recognises cybersecurity as a core component of national resilience. Without that shift in perspective, the UK risks building a regulatory framework that appears robust on paper while leaving the systems it is meant to protect increasingly exposed ●

Nick Haan is Field CTO at Claroty.

Infrastructure is one of the most attractive and strategically valuable targets in the cyber threat landscape

Picture credit: Crown Copyright