Five key takeaways from the UK's new Cyber Security & Resilience Bill

BY ED PARSONS · APRIL 7, 2026 · LAST UPDATED ON APRIL 22, 2026

What You Will Learn

- What the UK Cyber Security & Resilience Bill covers
- Which organizations and sectors will be affected
- New incident reporting and regulatory requirements
- How to prepare your organization for compliance

The content of the Cyber Security & Resilience Bill (CSRB) recently introduced to Parliament contained few surprises. Having spent a significant amount of time working with European cyber-security frameworks, particularly NIS2, I see the Bill as both a continuation of the trend towards common approaches, and a signal of how seriously governments now take cyber risk. From my perspective, there are five key takeaways that matter most for organizations trying to understand what this Bill really means in practice.

The Bill is part of a global convergence in cybersecurity regulation

The first and most important point is that the CSRB shouldn't be viewed in isolation. Arguably, we're living through a "golden age" of cyber regulation: where lawmakers around the world have made cyber security a priority area, resulting in a noticeable convergence of approaches across countries and regions.

The proposed new UK legislation clearly draws on the same thinking that underpins NIS2 in the EU. It isn't a copy-and-paste exercise, but the underlying principles are strikingly similar:

- Resilience over prevention
- Accountability at organizational leadership level; and
- Increased transparency through reporting obligations.

This harmonization will be welcomed by organizations that operate internationally. It allows companies to design security and compliance programs that work across borders rather than reinventing the wheel for each jurisdiction. Regulation is trending towards being more outcomes-based and accompanied by technical guidance, but where they are specific, it tends to be about the same things. For example, incident reporting timelines.

From a policy perspective, the convergence also suggests a growing maturity: regulators are no longer experimenting in isolation but are settling on shared norms about what "good" looks like when it comes to cyber resilience. The CSRB fits squarely within that trend.

A dramatic expansion of who/what is considered “in scope”

The second key takeaway is the sheer expansion of scope. One of the most consequential features of both NIS2 across Europe and the CSRB in the UK is how many more organizations they bring into the regulatory net. This happens in two ways: by broadening the definition of what counts as a critical or important service, and by introducing tiered classifications that capture thousands of additional entities.

Historically, cyber regulation has been focused on ‘traditional’ critical national infrastructure: energy, utilities, telecoms. Nowadays digital services and infrastructure are also essential. The designation of data centers as critical national infrastructure in the UK is a good illustration of this shift, with similar moves happening across Europe.

The Bill mirrors the NIS2 model by distinguishing between “essential” and “important” entities. Essential entities face more stringent oversight, but important entities are still subject to meaningful obligations. As evidenced by the experience of Belgium and other EU member states, this can increase the number of regulated organizations by an order of magnitude. The CSRB signals that many organizations which may not consider themselves part of national cyber resilience will now need to do so.

Incident reporting as a central pillar of the Bill

The third takeaway is the emphasis on incident reporting. This is one of the most concrete and easily understood aspects of the Bill, and it is also where we see the strongest convergence with EU regulation.

The staged reporting model will be familiar to anyone operating under NIS2: early warning within 24 hours, formal notification within 72 hours, and a detailed report within one month. The intention is clearly to improve transparency, allow national authorities to coordinate responses, and build a more accurate picture of systemic cyber risk.

That said, reporting is not without challenges. The concept of a “significant” incident, defined in terms of operational disruption, financial loss, or material damage, still leaves room for interpretation. There’s a genuine risk of over-reporting, particularly if organizations fear penalties for under-reporting; we’ve seen this play out before elsewhere, notably in the US. Nonetheless, these obligations are a meaningful step forward. Done well, they will encourage maturity, accountability, and shared learning across sectors.

Stronger regulatory powers and meaningful penalties

The fourth key point is the strengthening of regulatory authority. A substantial portion of the CSRB is about providing regulators with more power: to inspect, to direct, and to penalize. Even for organizations classified as “important” rather than “essential,” the potential fines are significant, certainly large enough to be material for medium-sized businesses. The bill also gives the UK Government power to step in during a national security incident.

This reflects a broader political reality. Cyber-attacks on critical services are no longer hypothetical risks; they are happening, and they are causing real economic and societal harm. Strengthening the arm of government is a deliberate response to that reality.

At the same time, experiences in Europe show that enforcement need not be purely punitive. Some governments have paired obligations with education, online portals, and practical resources to help organizations understand and meet their requirements. The CSRB, at this stage, leans heavily into powers and penalties. While that might be expected for the Bill in its early stages, it does mean that practical support and guidance will need to follow.

The Bill sets the framework, but much of the technical detail is still to come

The final takeaway is that the CSRB is, at heart, a structural piece of legislation. It provides clarity around organizations in scope – although designation will be left to the regulators, how incidents must be reported, and what powers regulators will have. What it does not (yet) do is spell out, in detail, the specific requirements organizations will be subject to.

Details will emerge later, likely through secondary legislation and good practice guidance, leveraging existing frameworks like the UK's Cyber Assessment Framework. Belgium developed the Cyber Fundamentals framework (CyFun) to describe the organizational and technical controls require to comply with NIS2. For example, it includes guidance on Coordinated Vulnerability Disclosure (CVD), a formal requirement for all essential and important entities.

But currently for organizations, there's enough clarity to know that action is required, but not yet enough detail to know exactly what "good" looks like in every area. The upside of harmonization is that organizations already aligned with recognized standards and best practices are likely to be in a strong position when that guidance arrives.

Conclusion

In its totality, the Cyber Security & Resilience Bill is both predictable and significant. It reflects a mature, internationally aligned approach to cyber regulation; it expands the scope of who is responsible for national cyber resilience; it standardizes incident reporting; and it strengthens regulatory enforcement. And, while there is clearly more work to be done, particularly in providing technical guidance, the Bill sends a clear message. That message is that cybersecurity is critical for building resilience in critical services. It is a core component of national resilience, economic stability, and trust in digital services.

AUTHOR

Ed Parsons

Ed Parsons is Chief Operating Officer for Intigriti. Before joining Intigriti, Ed was Vice President of the world's largest member association for cyber professionals and led an international cybersecurity consultancy, renowned for research and technical expertise. As a cybersecurity professional, Ed spent several years helping organizations investigate and respond to cyber threats from nation-states and organized crime groups. He is a Certified Information Systems Security Professional (CISSP) and a UK Chartered Cyber Security Professional.

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com