The Cyber Security and Resilience Bill: what it means for businesses and how to get ahead

BY ANNA HAMMOND · JULY 31, 2024 · LAST UPDATED ON APRIL 1, 2025

Cybersecurity and resilience have always been key priorities for information security experts, but recently, they've captured the attention of the public as well. The recent wave of cyber-attacks on the UK's critical sectors—including the Ministry of Defence, Royal Mail, the British Library, and London hospitals—has thrust these issues into the spotlight. These incidents have highlighted the urgent need for change, and in a bid to keep pace with the EU, the King introduced the new Cyber Security and Resilience Bill in his speech on 17th July, 2024.

In this article, we'll take an in-depth look at what is being proposed within the Cyber Security and Resilience Bill, examining the key principles it sets out to address and the potential impact on businesses.

What is the Cyber Security and Resilience Bill?

The Cyber Security and Resilience Bill is a significant piece of legislation being proposed that aims to transform how cybersecurity is handled in the UK. By broadening the coverage of existing cyber regulations, strengthening regulatory powers, and enhancing reporting obligations, the bill will ensure that critical national services can continue to be delivered in the face of a cyber incident.

"This legislative initiative is a significant step in the UK government's commitment to protect the country from cyber threats", says Marilyn Vandermarliere, Intigriti's General Counsel. She continues: "It will raise the bar for cybersecurity and resilience, which is essential to keep up with the ever-evolving threat landscape."

What will the Cyber Security and Resilience Bill do?

The Cyber Security and Resilience Bill will bolster the country's cybersecurity defences and increase the resilience of critical sectors. The current proposal remains quite general, and a more detailed draft of the bill is anticipated for further clarity. However, as it stands, the newly proposed bill aims to update the UK's existing framework by:

- **Broadening the scope of regulation** to include additional digital services and supply chains, which are becoming increasingly targeted by cyber attackers.
- **Strengthening the position of regulators** to ensure that essential cybersecurity measures are in place, which includes the introduction of possible cost recovery mechanisms and granting the authority to proactively investigate vulnerabilities.
- **Requiring more comprehensive reporting of incidents** to provide the government with better data on cyber-attacks, including instances of ransom attacks.

The bill will apply UK-wide.

How the bill correlates with EU laws

As stated in the King's Speech background briefing, 'the existing UK regulations reflect law inherited from the EU and are the UK's only cross-sector cyber security legislation. They have now been superseded in the EU and require urgent update in the UK to ensure that our infrastructure and economy is not comparably more vulnerable.'

The European Union has been at the forefront of cybersecurity legislation, actively developing technical standards and frameworks for mitigating and responding to cyber threats. The NIS Directive is being updated to the NIS 2 Directive, which officially came into effect on 16th January of the previous year, with a deadline for EU Member States to incorporate it into national law by October 17th, 2024.

The NIS 2 Directive introduces extensive modifications to the EU's cybersecurity framework for networks and information systems, applicable to operators of essential services and key digital service providers, such as search engines, cloud computing services and online marketplaces. Digital products, on the other hand, will become subject to increased security requirements under the Cyber Resilience Act.

Impact on businesses: What you need to know

The Cyber Security and Resilience Bill marks a new era in the UK's approach to cybersecurity for businesses. Seeing earlier similar legislative initiatives in the EU and USA, businesses are increasingly being encouraged to view cybersecurity as a strategic investment, essential for the protection of their operations and the data of their customers, and for the preservation of public trust.

The legislation also underscores the importance of supply chain security. Organizations must recognize that their cybersecurity is only as strong as the weakest link in their supply chain. They must ensure that their suppliers and third-party vendors are following strong cybersecurity practices. This approach extends beyond direct business partners and includes the entire supply chain ecosystem. By working together, organizations can create a collective defense against cyber threats that goes beyond the boundaries of any one organization.

A failure to meet the new and higher cybersecurity standards imposed by recent legislative initiatives, such as the NIS 2 Directive, the Cyber Resilience Act and the Cyber Security and Resilience Bill, may have serious consequences. For example, significant fines, reputational damage, and even legal liabilities. It is imperative for businesses to take a proactive approach, allocate sufficient resources, and establish a culture of cybersecurity awareness within their organizations.

How businesses can prepare for the Cyber Security and Resilience Bill

Depending on the details, it is probable that businesses, especially those in technology and critical service sectors, will have to comply with and possibly invest in enhanced cybersecurity protocols. All companies will need to assess their supply chain interactions to ascertain if they are, even indirectly, affected by the new, more stringent cybersecurity regulations.

While a more detailed draft is anticipated, here are some steps businesses can take already to strengthen cybersecurity and increase resilience:

1. Conduct comprehensive risk assessments

Businesses are advised to undertake thorough risk assessments (such as penetration testing) to pinpoint, analyse, and prioritise cyber risks that are pertinent to their activities. These evaluations should encompass all facets of the organization's IT infrastructure, data assets, and information systems. By identifying vulnerabilities, businesses can allocate their efforts and resources to tackle the most pressing risks.

2. Embrace vulnerability disclosure

Fostering a culture that embraces vulnerability disclosures is essential for enhancing resilience. Creating a transparent environment, such as a vulnerability disclosure program (VDP), where security researchers and users can report vulnerabilities without fear is crucial. Additionally, implementing internal processes to handle these disclosures efficiently ensures that vulnerabilities are addressed promptly and effectively. This not only strengthens security postures but also builds trust with customers and stakeholders, demonstrating a commitment to protecting their data and privacy.

3. Implement robust security measures

Businesses should implement robust security measures to mitigate potential cyber threats. This includes employing secure authentication mechanisms, deploying firewalls and intrusion detection systems, encrypting sensitive data, and regularly updating software and systems to address known vulnerabilities. Additionally, businesses should establish and maintain comprehensive vulnerability management programs to identify and promptly patch any security weaknesses.

4. Develop incident response plans

Discussing the new legislation, Jon Ellison, NCSC Director of National Resilience, reflected, "regulation alone cannot fortify the security of our critical systems, nor can we anticipate it to prevent every incident. However, our shared goal should be to significantly challenge our adversaries' efforts to succeed and ensure robust response and recovery mechanisms when breaches occur."

Proactive planning is essential for effective cyber incident management. Businesses should develop comprehensive incident response plans that outline the steps to be taken in a cyber-attack or data breach. These plans should include procedures for detecting, containing, eradicating, and recovering from cyber incidents, as well as clear roles and responsibilities for all relevant personnel. Regular security testing and updating of incident response plans ensure that businesses are prepared for responding swiftly and effectively to cyber threats.

5. Provide employee training and awareness

Human error can be your biggest weakness in cybersecurity, yet your employees can also be your biggest strength. Conducting frequent training and awareness programs to equip employees with the knowledge to spot and respond to cyber threats is vital. These programs should encompass a broad range of topics,

from phishing scams to the importance of promptly reporting any suspicious activities. By doing so, businesses can markedly decrease their susceptibility to attacks.

6. Continuously monitor and review cybersecurity measures

Cybersecurity is an ever-growing and rapidly changing field. Businesses must be vigilant in monitoring and reviewing their cybersecurity measures to proactively address emerging threats. Regular security audits and assessments, such as bug bounty programs, are essential to identify any vulnerabilities in the organization's cybersecurity posture. Staying abreast of the latest cyber threat intelligence and industry best practices is crucial to maintaining robust and effective cybersecurity measures.

How Intigriti can help businesses prepare for the bill

Intigriti empowers the world's largest organizations to proactively identify and address vulnerabilities before they're exploited by cybercriminals. Harnessing the expertise of our 100,000+ researchers, businesses can detect vulnerabilities as soon as they surface, avoiding the costly damage of security breaches. Intigriti is honoured to be the preferred bug bounty platform for top industry players like Coca-Cola, Microsoft, and Intel, helping to protect their digital environments against the constantly changing threat landscape.

We enable organizations to:

- **Transition to proactive security testing:** Since 2016, we have launched over 400 bug bounty programs, hybrid pentests, and vulnerability disclosure programs.
- **Drive security assurance:** Through our meticulous triaging process, commitment to legal compliance, and unparalleled customer service, we ensure the highest level of reliability for our clients.
- **Speed up vulnerability response:** Our platform enables security teams to quickly identify and prioritize vulnerabilities, facilitated by our efficient triaging and an unrivalled communication system.
- **Stay informed**: We are proud to be a CVE Numbering Authority (CNA) under the CVE Program, which catalogues publicly disclosed cybersecurity vulnerabilities.

Our goal is to ensure that businesses are supported in navigating the bill's complexities through our platform and services, effectively improving their cybersecurity and resilience. To learn more, speak to one of our advisors today.