Telecoms Security Bill

The biggest change to the telco regulatory environment in a generation

Digital Intelligence

BAE SYSTEMS

In the last 30 years the UK telecommunications market has transitioned from state owned monopoly, to major enabler for digital growth, to provider of critical national infrastructure (CNI). The importance of this sector to the UK economy is clear for all to see, yet the regulations in place during this tumultuous period has been relative static. That's about to change with the arrival of the Telecoms Security Bill, the single biggest change to the regulatory environment in a generation. In a world where cyber threats continue to proliferate it's easy to see why many would conclude that this change is long overdue.

The legislation has far reaching implications for telco operators, not least due to the potential for huge fines from Ofcom, but also the reputational damage and business disruption any breach of compliance would cause. So why hare these more specific obligations being enforced on this sector now, and what are the implications on them and on UK Plc?

Firstly, the telecoms sector is all pervasive by which I mean it influences not only our daily lives, but our whole economy. As we move towards a fully digital economy the need for a resilient and reliable telecommunications backbone becomes even more critical. The pandemic has taught us to expect the unexpected and brought to light how reliant we are on this sector for our prosperity and wellbeing. If we ever took our broadband and telecoms infrastructure for granted we do so far less now. CNI is so defined because it holds a key strategic importance to the nation, particularly during times of national emergency.

Secondly, the cyber threat is increasing at a substantial rate. Research by BAE Systems Digital Intelligence for the UK Cabinet Office estimated that UK firms lose approximate £27 billion every year through cyber incidents. Globally, some have estimated the figure could be as high as $6 trillion or, roughly $16 billion lost every single day to cyber security breaches (Source: Cobalt). To put this into context that's greater than the combined GDP of the whole of Europe.

"The legislation has far reaching implications for telco operators, not least due to the potential for **huge fines** from Ofcom..."

"Our research showed that circa **78 per cent** of CSPs have not proactively sought to work out where their cyber vulnerabilities are..."

Think of the economic growth that could be made in minimising this impact even by a few percentage points. Our research showed that circa 78 per cent of CSPs have not proactively sought to work out where their cyber vulnerabilities are or what they would do to minimise them or how contingency planning could help in the event of an attack.

Thirdly, globalisation has significantly increased supply chains, making us more reliant on remote organisations who have access and transact through our networks. Whilst smooth unrestricted access is essential for economic growth, restricting or even blocking access from untrusted sources has become a pressing and real concern. The legislation has at its inception a focus on a number of perceived high risk vendors but if you look deeper into the legislation you'll see a set of cyber security policies that should have been implemented many years ago.

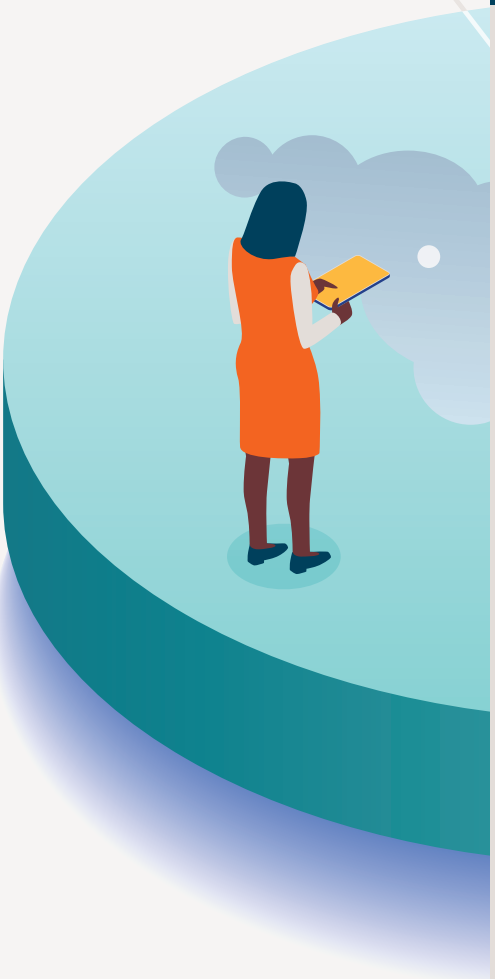
The environment summarised above puts greater onus on organisations to understand emerging threats and technology risks. Having a range of partners to navigate this landscape is key. Step forward BAE Systems who have a deep routed experience in protecting enterprises and nation states from cyber threat. With a portfolio of mature cyber offerings we are exceptionally well placed to de-risk the implications of the legislation for the operators. These products, services and capabilities include, Threat Intelligence, Cyber Threat & Risk Assessment, Critical Incident Response, SOC Optimisation, Governance and Policy Framework and Disclosure Solutions.

Whilst products and services are key, it's absolutely essential to work with organisations that have the skilled staff to implement solutions. With over 4,000 consultants and engineers working across the high trust sector in the UK, BAE Systems Digital Intelligence is well placed to mitigate the risk and optimise the opportunities presented by TSB.

If you need to speak to a BAE Systems representative please contact learn@baesystems.com

We are Digital Intelligence

BAE Systems Digital Intelligence is home to 4,800 digital, cyber and intelligence experts. We work collaboratively across 16 countries to collect, connect and understand complex data, so that governments, nation states, armed forces and commercial businesses can unlock digital advantage in the most demanding environments. Launched in 2022, Digital Intelligence is part of BAE Systems, and has a rich heritage in helping to defend nations and businesses around the world from advanced threats.



BAE Systems Digital Intelligence
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom
T: +44 (0) 1483 816000

BAE Systems Digital Intelligence
8000 Towers Crescent Drive
13th Floor
Vienna, VA 22182
USA
T: +1 720 696 9830

BAE Systems Digital Intelligence
Malta Office Park
ul. Abpa A. Baraniaka 88
Poznan
61-131
Poland
T: +44 (0) 330 158 3627

BAE Systems Digital Intelligence
Level 2
14 Childers St
Canberra
ACT 2601
Australia
T: +61 (0) 2 9053 9330

BAE Systems Digital Intelligence
Level 28, Menara Binjai
2 Jalan Binjai
Kuala Lumpur
50450
Malaysia
T: +60 327 309 390

BAE Systems, Surrey
Research Park, Guildford,
Surrey, GU2 7RQ, UK

E: learn@baesystems.com

W: baesystems.com/digital

linkedin.com/company/baesystemsdigital

twitter.com/BAES_digital

BAE SYSTEMS