NTT DATA

Transforming security across the UK communications industry

How the UK Telecommunications (Security) Bill is forcing a new security culture

uk.nttdata.com

素晴らしいガイド

GUIDING GREATNESS

The UK government takes action on communications security

The UK communications sector is undergoing the deepest regulatory-driven change since the introduction of the General Data Protection Regulation (GDPR) a few years ago and even arguably since BT's 1984 privatisation. That's because public telecoms providers are facing one of the world's toughest legislative cybersecurity regimes deriving from the Telecommunications (Security) Bill.

The Bill advances the UK government's findings within its Telecoms Supply Chain Review Report to establish an enhanced legislative framework for telecoms security. It also provides the government with the powers to act on the use of high-risk vendors on national security grounds.

The changes come in response to the UK's growing dependency on fixed and mobile broadband, driven by new working patterns and 5G ultimately becoming essential for autonomous vehicles and all sorts of safety dependant use cases. Everyone in the UK telecommunications industry, not just security and regulatory compliance specialists, will be impacted.

Remembering that 5G covers both mobile and fixed/broadband networks, future UK economic performance is intertwined not only with how well 5G technology and supply chain risks are tackled, but also how vulnerabilities around "national capability to operate networks" are addressed.

As such, although connectivity such as Wi-Fi and 5G and the ever-growing number of Internet of Things (IoT) devices create new business models and lifestyle advantages, they have vulnerabilities that threaten the availability of services and make them juicy targets for hackers. The deployment of open 5G networks based on software driven, virtualised technology are all creating new vulnerabilities. Some threats affect network availability, while others risk data loss and theft.

What the Bill says

The Telecommunications (Security) Bill amends the Communications Act 2003 by placing strengthened telecoms security duties on public telecoms providers, providing new powers for the government to set out specific security requirements and issue codes of practice, and giving Ofcom new tools and responsibilities to ensure industry compliance.

Additional controls are being imposed on high-risk vendors posing a material security risk to network resilience. Although media reporting tends to focus on the procurement aspect of this Framework, it is significant that its scope extends into the design, build and operate phases of the technology lifecycle.

The Framework ensures that network management functions and tasks cannot be achieved from corporate administrative networks. The Bill covers the diversity of supply chains, the quality and security of equipment and managed service providers.

It also addresses the government's concerns about global telco operators making decisions for reasons that may not be in the UK's interests. Global operators that may have allowed commercial benefits, accrued at a multi-national level, to drive offshoring instead of considering infrastructure risk at a national op-co level might be a case in point.

The time has come for everyone in the communications industry to elevate their thinking about the risks to critical national infrastructure as they go about their day-to-day work.

Telecom Security Requirements mark a transformational change

The Telecommunications (Security) Bill enhances the legislative framework governing communications providers by levelling up the industry's security response and transforming good practice into common practice across the sector.

Ultimately, the effect will be transformational and communications players will be forced to look and behave differently. Transformational change is never easy, particularly as fixed deadlines are an integral part of the mix. Execution will need to be multi-disciplinary, properly designed and well planned.

Although technology aspects are the most frequently written about, the real challenge could be how culture is redefined and business and operating model change is achieved. Some functions may need to be brought back onshore in addition – although certainty in this area does not yet exist. Risk-driven thinking must become a natural part of people's day-to-day work.

What does transformation mean in reality?

Transformation is a much over-used word. It is often attached to projects that are merely big or relatively complex. Vendors often apply the term to make their offers sound more compelling.

Real transformation is about responding successfully over a short, constrained time to an existential threat. It impacts the entire organisation and when completed, the business will be seen as acting differently by its various stakeholders – including customers and regulators. Transformation is about companies re-engineering their modus operandi while continuing to move forward in terms of their structures, the evolving market and its demands.

An approach adapted from John Kotter's work describes the transformation as a series of intertwined, not necessarily linear steps:

- Create a sense of urgency about the need for a change of culture.
- Create the vision for the end state – if you are thinking mainly about technology change you may be missing some of the point.
- Align the leadership team around a common cross-functional/cultural vision for what the post-transformation organisation will look like.
- Remove the barriers to change.
- Get some early delivery going.
- Mobilise the programme in its full structure.
- Keep the delivery going by focussing on the future need to track, report and evidence compliance. Envisage the information requests that will be coming and design your changes from that point inwards.

Five priorities for communications players

To achieve the transformational change called for by the Telecom Security Framework. NTT DATA recommends communications companies focus on five key priorities.

1

Get the right people in place

People will be needed for gap analysis, operating model design, programme delivery, commercial re-negotiations and re-shoring. New competencies will need to be developed.

2

Plan to avoid legacy issues

The telecommunications industry is one of multi-generational networks. Although dodgy IoT devices present an ever-present danger, there are other issues such as legacy signalling protocols that may be around for a long time yet. Dealing with legacy needs to be an integral part of planning.

3

Design with the end in mind

Failing to disclose evidence could result in a £10m fine. The new supervisory regime will be active with demands for large amounts of data expected. It's essential to build traceability and the ability to share information into your programme and future security-driven operating model.

4

Make the culture change

We are all used to working in a global context with global supply chains and operator structures. The Telecoms Security Bill is, however, a UK requirement. This calls for the development of a culture of UK-oriented risk awareness, even though it is likely that many other nations' regulators will develop some sort of framework that may not be exactly like the UK's but will have the same objectives.

5

Put the customer first

Consider the TSRs as a catalyst for change that will enable the organisation to perform better and be more open and transparent with regard to its network, supply chain and ultimately, paying customers. Safe connectivity and protected data are then inherent parts of a customer promise and from which commercial benefits will follow.

How NTT DATA can help

Security is the responsibility of every executive and employee: it is not the domain of the security organisation alone. Any complex change initiative that touches everyone in the business is of course going to be resource and expertise heavy. Companies may not have the necessary in-house resources meet the demands of the TSF compliance journey. This is particularly relevant when considered alongside the demands of keeping existing change portfolios on track.

In a global environment where security resource and core competence is in high demand and limited availability, all companies will need to find partners with the right competencies and resources to support the bell curve of change. With a strong telco heritage and deep know-how in telco security, NTT DATA offers a proven 'assess, deliver, manage' approach to dealing with the challenges of regulatory driven change and the Telecom Security Framework in particular.

Contact us to find out more about how NTT DATA can help you with your security needs and the challenges of the Telecom Security Framework.

Ken Jones

+44 7875 561221

Ken.Jones@nttdata.com

GRC Director, Security Consulting Practice -
NTT DATA UK

Warren O'Driscoll

+44 7387 525 159

Warren.O'Driscoll@nttdata.com

Head of Security Consulting -
NTT DATA UK

Matt Kearney

+44 7811 838095

Matthew.Kearney@nttdata.com

Vice President, Advisory Telco Media -
NTT DATA UK

NTT DATA UK
1 Royal Exchange
London
EC3V 3DG
020 7220 9200

NTT DATA is a leading consulting and IT services provider, combining global reach with local expertise in over 50 countries. Whether it's business transformation, enabled by digital, data and technologies, safeguarding against security breaches, improving operational efficiency or driving new revenue streams, our vision as the Trusted Global Innovator can help organisations navigate the ever-changing digital landscape and deliver outstanding results.

NTT DATA offers a portfolio of best-in-class consulting services and innovative enterprise solutions tailored to suit the entire life cycle of IT investment. Supported by our international Centres of Excellence, our team of local experts can deliver on a wide range of services from transformation to agile development and intelligent automation for industries across manufacturing / automotive, banking, insurance, telecommunications, media and public services.

For more information about NTT DATA please visit **uk.nttdata.com**