DigitalXRAID
CYBER SECURITY EXPERTS

TELECOMMUNICATIONS

Navigating the UK Telecommunications Security Act: A Guide for Providers and Suppliers

Threats are becoming more sophisticated and their potential impact cannot be ignored

The UK Telecommunications Security Act (TSA) was introduced in October 2022, in response to growing cyber threats and the need for a reliable and resilient telecoms infrastructure.

As digital connectivity becomes increasingly integrated into our daily lives, the risk of cyber threats has grown exponentially. Telecommunications companies are attractive targets for cybercriminals, nation-state actors, and hacktivists due to their critical role in supporting various industries and the vast amount of sensitive data they manage.

The TSA sets new security requirements for public telecom providers and is crucial for ensuring the continuity of vital services in sectors such as energy, transport, and healthcare.

This ebook aims to simplify the TSA, helping providers and vendors understand their obligations and the benefits of achieving compliance proactively. And why it's essential for providers and vendors to take action now.

The Growing Cyber Threats Facing Telecommunications Companies

Cyber threats have evolved significantly over the years, with attackers employing new tactics, techniques, and procedures (TTPs) to target critical national infrastructure, including telecommunications.

Some of the key potential vulnerabilities and threats that have emerged include:

Advanced Persistent Threats (APTs)

APTs are often state-sponsored or well-resourced cybercriminal groups that conduct long-term, targeted attacks.

They aim to infiltrate and maintain a foothold in an organisation's network, exfiltrating sensitive data or causing damage over time.

Ransomware Attacks

Ransomware attacks involve the encryption of a victim's data, rendering it inaccessible until a ransom is paid.

Telecommunications providers, with their vast amounts of customer data and reliance on uninterrupted services, can be particularly attractive targets for ransomware attackers.

Supply Chain Attacks

As seen in the SolarWinds incident, attackers can compromise a trusted supplier's software or hardware, subsequently infiltrating the networks of multiple organisations.

This type of attack can be particularly damaging, given the complex and interconnected nature of the telecoms supply chain.

Distributed Denial of Service (DDoS) Attacks

This attack involves overwhelming a network or system with excessive traffic to render it inaccessible.

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

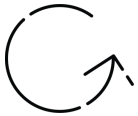
Exploited assets can include computers and other networked resources.

Increased Interconnectivity & Vulnerabilities

The rapid growth of IoT devices, 5G networks, and cloud-based services has increased interconnectivity within the telecommunications sector.

While this offers numerous benefits, it also exposes providers to a wider range of vulnerabilities and potential attack vectors.

Furthermore, the reliance on third-party vendors and suppliers for various services introduces additional risks.



Impact on Critical Infrastructure and Services

The telecoms infrastructure is deeply intertwined with other critical sectors, such as energy, transport, and healthcare.

A successful cyberattack on a telecommunications provider could have severe consequences, disrupting vital services and potentially endangering public safety.

This makes securing the telecommunications infrastructure even more crucial.

Consequences of Cyberattacks on Telecommunications Companies

The potential consequences of a successful cyberattack on a telecommunications company are far-reaching, including:

Service disruptions: Interruptions to essential services, such as emergency response communications, energy distribution, and transportation systems.

Financial losses: Direct costs from ransom payments, system repairs, and loss of business due to reputational damage.

Data breaches: Unauthorised access to sensitive customer and company data, leading to identity theft, fraud, and intellectual property theft.

Regulatory fines: Penalties imposed by regulators for non-compliance with data protection and privacy regulations..

Ransomware attacks on businesses have increased by 485%

The Role of the UK Telecommunications Security Act (TSA)

The TSA Code of Practice was published by the Department for Digital, Culture, Media and Sport (DCMS) in October 2022. Since then, DCMS has become the Department for Science, Innovation and Technology (DSIT).

The TSA provides 258 technical guidance measures for providers. It covers critical areas of operations like network management, monitoring and analysis, supply chain, and more.

The main goal is to achieve the desired outcomes, and providers can demonstrate their compliance to Ofcom without necessarily following the recommended protocols to the letter.

The Act aims to:

- Establish minimum security standards: Ensuring that providers maintain robust network security, risk management, and incident response capabilities.
- Strengthen supply chain security: Encouraging providers to scrutinize and manage the security of their suppliers and partners.
- Facilitate information sharing: Enabling providers to share threat intelligence and best practices with one another and government agencies.
- Enhance regulatory oversight: Empowering Ofcom to monitor compliance and take enforcement actions against non-compliant providers.

By adhering to the TSA, telecommunications companies can proactively address cyber threats, minimise potential consequences, and contribute to a more reliable and resilient telecoms infrastructure that supports vital services in sectors like energy, transport, and healthcare.

Public telecoms providers that fail to comply with the regulations could face fines of up to ten per cent of turnover or, in the case of a continuing contravention, £100,000 per day.

Understanding the obligations and benefits of achieving TSA compliance is crucial for providers and suppliers in navigating the evolving cybersecurity landscape.

Compliance Deadlines

The TSA sets different deadlines for Tier 1, Tier 2, and Tier 3 providers based on their annual revenues.

These deadlines affect not only providers but also their suppliers. Tier 1 and Tier 2 providers must ensure their supply chain complies with the requirements set by the TSA, and suppliers should be aware of the ticking clock.

The Benefits of Compliance

Compliance with the TSA offers several benefits, including impetus for modernisation, simplified procurement, and a competitive edge.

By aligning with the TSA requirements, providers and suppliers can improve their market position and build business resilience.

Five Steps to Achieve TSA Compliance

Start planning now:

Start working on a roadmap and milestones so you don't fall behind with compliance requirements.

Complete an asset inventory:

If not already in place, an asset directory will give a clear understanding of every asset in your organisation which needs to be included in the scope of requirements

Scope your requirements:

Identify the systems and operations in your organisation that will be subject to the regulation. This will give you steer on how and when to take steps in your roadmap and tackle compliance in stages.

Third parties and supply chain:

Develop a system for verifying and managing your suppliers in line with the Code of Practice measures.

Expert partner:

Collaborate with a partner that can bring expertise to interpret the regulations, help you to understand what needs to be included in your scope, and develop a roadmap with you for improvement that can be managed more effectively.

Why Procrastination is a Mistake

While some providers may be tempted to procrastinate due to the complexity of the regulation, this approach is risky. The regulation is already in effect, and providers should start working on compliance as soon as possible.

The UK Telecommunications (Security) Act is a vital piece of legislation aimed at securing our increasingly connected society.

By understanding the requirements, deadlines, and benefits, providers and suppliers can turn compliance into a competitive advantage and contribute to a more resilient telecoms infrastructure for all.

Achieving compliance with the TSA can be a complex undertaking, but working with a cybersecurity partner can significantly ease this process.

A knowledgeable cybersecurity partner can provide the expertise and resources necessary to navigate the regulatory landscape, ensuring that your organization meets the necessary requirements in a timely manner.

It's essential to stay informed about cybersecurity trends and to be proactive in identifying and addressing vulnerabilities

DigitalXRAID
CYBER SECURITY EXPERTS

How can we help?

Expertise:
A cybersecurity partner possesses the necessary knowledge and experience to help you understand and interpret the TSA's requirements. They can provide valuable insights into best practices and effective strategies for achieving compliance.

Resource optimisation:
Many organisations, particularly smaller ones, may lack the internal resources to dedicate to achieving TSA compliance. By working with a cybersecurity partner, you can leverage their expertise and resources, allowing your organization to focus on its core business objectives.

Risk mitigation:
A cybersecurity partner can help you identify and prioritize potential risks, ensuring that you address the most critical vulnerabilities first. This proactive approach to risk management can significantly reduce the likelihood of a successful cyberattack.

Ongoing support:
Compliance is not a one-time event. A cybersecurity partner can offer ongoing support, ensuring that your organization remains up-to-date with evolving regulations and cybersecurity best practices.

With over 25 years' experience in the industry, DigitalXRAID has the expertise to protect your business and provide comprehensive security solutions.

We take a proactive approach to cybersecurity. Rather than simply responding to attacks after they occur, we help you to stay a step ahead of cybercriminals, preventing attacks and other cybersecurity threats before they happen.

By partnering with DigitalXRAID, you can confidently take proactive measures in protecting your systems and data and ensure TSA compliance.

Ultimately, this collaborative approach will contribute to building a more robust and resilient telecoms infrastructure for the benefit of all.

DigitalXRAID

CYBER SECURITY EXPERTS

Need the Best Defence Against Cyber Threats?

Call us now on 0800 090 3734

info@digitalxraid.com digitalxraid.com

ISO 27001 INFORMATION SECURITY MANAGEMENT

ISO 9001 QUALITY MANAGEMENT

CYBER ESSENTIALS CERTIFIED PLUS

IASME CONSORTIUM

CREST

Assured Service Provider

in association with National Cyber Security Centre

CHECK Penetration Testing