NEW REGULATIONS PUT TELECOMMUNICATIONS CYBERSECURITY UNDER SCRUTINY

In an interconnected world, cybersecurity and national security are often deeply entwined. As both private sector organizations such as banks and intergovernmental bodies such as NATO and the World Bank conduct business and transactions across borders, they need to be confident that each telecommunications network they touch is fully protected from threats. Within nations, telecommunication networks play an essential role in critical services such as defense, healthcare, and public safety. To protect their national interest and the wellbeing of their people, governments must ensure the security of physical infrastructure, systems, and personnel across the entire supply chain of software and services. Simply put, if a nation can't rely on the security of its telecommunications, it can't participate fully in the gigabit society.

To ensure the trustworthiness of its national telecommunications networks, the government of the U.K. recently conducted a thorough security review of the sector—and found much work to be done. In response to the risks surfaced in the findings, the U.K. is working hand-in-hand with communications service providers (CSPs) to enable a better security framework, culminating in the Telecommunications (Security) Act (TSA) 2021, which came into force on October 1, 2022. The Telecommunications Security Code of Practice introduced by the TSA encompasses the entire telecommunications ecosystem of companies, partners, and suppliers, all of whom must now maintain a high level of governance in how they work together. Strict enforcement provisions include fines of up to 10 percent of their annual revenue, or £100,000 per day for a repeated infraction.

The introduction of the TSA isn't an insolated case, but rather part of a global trend. In Australia, the Security of Critical Infrastructure Act 2018 focuses on managing "the complex and evolving national

security risks of sabotage, espionage and coercion posed by foreign involvement in Australia's critical infrastructure," including communications among other vital sectors. Legislation has been introduced in the U.S. to promote secure information and communications technology infrastructure around the world. A 2021 survey by EY found that privacy, security, and trust are now viewed as the second-greatest risk in telecommunications, citing a 75 percent rise in cyberattacks during the previous year.

In this blog, we'll discuss key security challenges CSPs now face in light of growing regulation and rising threats, and how they can be addressed using BMC solutions for service management, operational management, observability, and orchestration.

The scale and speed of the telecom security threat

As in many industries, telecommunications companies often face difficult tradeoffs between cybersecurity and competitiveness. The demand of customers for new types of services makes time to market a top priority for the next big product. While security is a consideration, it's rarely given the same level of attention.

A rapidly changing regulatory landscape and threat environment has now reshaped these priorities. With new threats flooding the environment, including intensifying activity by state actors in global conflicts, regulators are raising the stakes for the protection of critical infrastructure. In fact, telecommunications companies were cited for GDPR violations 69 times in 2020—more than four times the number of sanctions imposed on technology companies—for a total of €62,400,000 in penalties.

Within the U.K., CSPs now have until March 2025 to adhere to the new code of practice, including timely information-sharing with Ofcom, the U.K.'s communications regulator. While the provisions of the TSA and its code of practice are extensive, the overarching goal is simple: ensuring that critical elements of the nation's day-to-day life won't be brought down by a security breach of its telecoms networks.

To respond to this mandate, CSPs must move quickly to upgrade their cybersecurity capabilities—for example, meeting a new requirement to remediate known vulnerabilities within 14 days of discovery. In an industry where such gaps typically linger for months before being addressed, this is a major shift.

Ensuring a trusted network for global telecommunications

While national security is a key driver for new telecommunications security regulations, market dynamics come into play as well. As CSPs around the world race to monetize new investments in 5G licenses and infrastructure, they often share spectrum with partners across the global industry. If telecoms networks aren't viewed as trustworthy, other companies will be reluctant to enter into these partnerships. This can leave the nation at a disadvantage in the rollout of next-generation infrastructure, slowing the extension of cost-effective connectivity to historically underserved customers and the introduction of the edge computing services made possible by 5G-based systems.

Here again, maintaining its status as a first-class digital nation depends on the U.K.'s ability to ensure the trustworthiness of its telecoms industry. And the same holds for other nations as well, as they move quickly to establish standards to reassure the global community that their critical

infrastructure is secure.

Key challenges for CSP cybersecurity

To achieve and maintain compliance with the U.K.'s TSA and similar regulations to follow around the world, CSPs need to meet a wide range of demanding technical requirements, including:

- Discovering assets throughout their business and operations environments, including third-party resources
- Understand the relationships among these assets and the business and network services they support
- Manage identities, authentication, and authorization for the internal and partner personnel who access the network
- Identify vulnerabilities anywhere in the network, understand their potential impacts, and remediate them within established timelines
- Leverage data in a streamlined scalable way for stakeholder reporting meeting specific deadlines

A common theme across these requirements is the importance of visibility and observability. CSPs need to be able to access the right information at the right time, with the context to translate raw data into an understanding of which vulnerabilities pose the greatest risk to services and infrastructure. A modern telecoms network might have hundreds of thousands of existing vulnerabilities, some critical, many less so—with a backlog that grows every day. This problem can't be solved by throwing personnel at it. CSPs will need to automate their identification and response processes to fix the most urgent problems first.

With data distributed across OSS and BSS environments, IT networks, and systems from the network edge to the core, data protection has become a major challenge as well. On one end, data within the data center might be locked down and backed up to ensure resiliency—but on the other end, business and consumer customers, field personnel with mobile devices, and other users all represent points of potential vulnerability. People, devices, and the network itself must all be seen as assets to be protected.

How BMC helps CSPs ensure secure telecoms

Given the reliance of CSPs on solutions for service management and digital business automation, the telecoms industry has long been one of BMC's largest and most important markets. BMC Helix provides a common platform across service management, discovery, application and data workflow orchestration, and vulnerability management for a unified approach encompassing people, process, and technologies across their IT and operating network environments. A common data layer provides a single source of information, with a shared data lake that can be accessed by all BMC solutions as well as integrated with non-BMC solutions.

BMC Helix Discovery – You can't secure what you don't know about. BMC Helix Discovery enables CSPs to identify assets, business services, and the relationships among them across on-prem and cloud environments. Dynamic service modelling provides a clear understanding of the connections and dependencies between assets and the services they support, allowing a service-oriented view of the environment. Ingesting and analyzing data and events beyond the scale of human processing, Discovery quickly identifies which part of the infrastructure is being affected by a given issue and

the resulting impact on specific business services.

Working with BMC Helix Service Management, Discovery also makes it possible to analyze the impact of change to anticipate and avert potential problems. As new patches are released, Discovery uses artificial intelligence to model the impact of the respective vulnerabilities, identify those most relevant to the CSP's business, and then prioritize and automate patch deployment to reduce time to remediation.

Control-M Saas – As CSPs service internal and external users, they need to be able to maintain a consistent governance model across people, processes, and technologies. At the same time, technologies such as fiber-to-the-home (FTTH) involve high volumes of data and files as well as disparate applications and systems requiring fine-tuned data operations orchestration. Due to its ever-changing nature, this data grows obsolete quickly and loses value over time.

Control-M Saas enables enterprise orchestration to meet the complex demands of modern data operations while managing which people and services can manage which resources, with which credentials, for what length of time. In this way, the solution allows the autonomy and productivity needed by business users while maintaining control and meeting security requirements.

With data feeds from hundreds of systems to coordinate, inefficient processes can quickly introduce delays that make it impossible to provide timely and accurate data to regulators or ensure that right internal teams have the right data at the right time. Control-M Saas Data workflow orchestration facilitates information-sharing with Ofcom, a key element of compliance to avoid fines for missed deadlines. AI built into the Helix platform enables automated correlation of incidents and data to provide IT personnel and network engineers with the context and actionable insight to remediate problems more quickly and effectively. With a Control-M Saas subscription, the customer not only gets access to the full capabilities and innovation of the platform, but also onboarding services, subscription education resources and a dedicated customer success specialist facilitate adoption of automation initiatives and maximize the value of the service.

BMC is already working closely with major U.K. telecoms to build solutions that enhance our core capabilities to address specific requirements. As trusted advisors to the industry, BMC can help CSPs meet the requirement of the TSA code of practice and other telecoms cybersecurity regulations around the world.