Baringa

A tipping point for Telco cyber security

Reframing cyber security

As network operators embark on ambitious and technology-led organisational transformation, they become increasingly exposed to a wider set of sophisticated and motivated threat actors that find ever more innovative ways to cause harm. The net effect is an increased risk to unprepared operators, to their customers and to the resilience of critical national infrastructure. The stark reality is many cyber security functions are struggling to keep pace with the business, and current ways of working, security technologies and operational teams are not sufficiently equipped to enable the business to transform securely.

Digital and technology transformation is creating an opportunity for business leaders to re-imagine themselves through the lens of a digital technology business. However, if security functions are unprepared to evolve at the same pace as the wider business, they will continue to create friction that causes more harm than good.

We have observed many business leaders question the efficacy of security processes, particularly when it comes to delivering effective business change and the commensurate value security functions provide. Ultimately, this is limiting the ability of operators to compete with digital-native businesses where highly efficient ways of working, such as those presented by Agile and DevOps, are baked into their DNA.

Some of the archetypal cyber threats such as state-level espionage and widespread network disruption are fundamental risks to the communications arteries that network operators supply and support. It is therefore not surprising that the UK's National Cyber Security Centre (NCSC) has raised the stakes for UK operators with the introduction of the Telecommunications (Security) Bill[1], giving regulators heightened powers to raise the level of security across networks operators and remove the threat of high-risk vendors. Similarly, the European Union had announced some significant changes to the Network and Information Systems Directive (NISD)[2], first introduced in 2017. The changes expand the scope of the directive to a larger set of 'Essential' and 'Important' entities and enforce a more granular set of regulatory requirements. With several regulators enforcing a range of cyber security requirements, network operators are having to navigate an increasingly complex and multi-national regulatory landscape, whilst also navigating major organisational change. The upper limits for penalties and fines can devastate the bottom lines of most operators and while historically regulators have been restrained in dealing out the most severe penalties, these grace periods have, or are about to, expire.

[1] Telecommunications (Security) Bill - Parliamentary Bills - UK Parliament
[2] Proposal for directive on measures for high common level of cybersecurity across the Union | Shaping Europe's digital future (europa.eu)

4 priorities
for security leaders

As network operators digitally transform, the expertise and technical capability that they are building is creating opportunities that can significantly benefit the security function. Security leaders risk falling behind their peers if they don't apply this capability effectively.

For network operators to succeed in this complex and high-risk environment, we have outlined what we believe are four priority areas for security leaders to consider.

PRIORITY 1: GET THE RIGHT BALANCE BETWEEN RISK & COMPLIANCE

Network operators need to significantly enhance their cyber risk management capabilities, both in the boardroom and within the security team and functional areas. 'Risk-based security' is the gold-standard. It enables leaders to make pragmatic and effective budget and resourcing decisions that drive the biggest Return on Investment (ROI) and carefully balance potential benefit and loss mitigation. Regulators are enforcing similar requirements, with tick-box compliance being replaced with less prescriptive standards that require operators to implement a governance structure and a set of practices to continually evaluate and mitigate cyber risk in a manner far more acute and quantifiable than in previous years.

Supply chain breaches are one of the most prevalent and damaging sources of incidents. In recent years, the SolarWinds and NotPetya attacks were supply chain driven and had far reaching global impacts for several of the most mature organisations across financial services, technology, and government sectors. The scale and complexity of the supply chain in network operators is growing as operators are relying more on their strategic suppliers for business-critical services. Prioritising around risk is a necessity. Automating low-risk supplier assurance processes and making (re)procurement decisions that consider quantified cyber risk will deliver significant savings for operators, both in direct resource savings and in identifying and avoiding potential cyber incidents.

CLIENT EXAMPLE

A major utility provider developed a supply-chain risk management approach which delivered an entirely automated and risk-driven response for evaluating over 80% of third parties. This gave their third-party assurance team the availability to target the biggest risks across their suppliers by eliminating laborious tasks like chasing low risk suppliers for responses.

PRIORITY 2: ESTABLISH A CYBER RESILIENCE CAPABILITY

Cyber resilience focuses on the ability to continue important business services and operations while responding to and recovering from cyber related incidents, rather than preventing them outright. Adopting the principles of resilience into cyber security capability means developing increased knowledge regarding loss thresholds, knowing what is acceptable and what isn't, and adjusting cyber capability accordingly. This requires a much more in-depth knowledge of credible loss events that are likely to occur and modelling their effects.

The NCSC has outlined clear objectives to build resilience into the UK's networks and to avoid any over-reliance on High-Risk Vendors (HRVs) like Huawei in delivering core components, which is a major driver behind the Telecommunications (Security) Bill outlined in November 2020. For network operators where availability and integrity of systems is paramount, cyber resilience should be considered a top priority. The technology estates that most operators support are a complex mix of new software-defined and cloud infrastructure alongside large estates of legacy infrastructure and devices which are often in varying states of decommission. By focusing attention on business outcomes and the underlying 'Important Business Services', security teams can unpick complex IT ecosystems and mitigate the risks that matter most.

CLIENT EXAMPLE

A global insurance business embedded cyber resilience within their organisation as part of a programme of operational resilience. This process outlined the core processes that the business considered critical, and stress tested the ability to sustain them in disaster scenarios. The holistic and business-centric approach outlined significant cyber risks that were either under-represented or entirely absent in previous risk registers.

PRIORITY 3: BUILD INTELLIGENCE & AUTOMATION CAPABILITY

As the volume of data grows, the maturity of data science and the ability to harness data is becoming a key differentiator and a core strategic objective for network operators. Many operators are already employing sizable and skilled teams to deliver data-driven insights across their business operations. Operators should also use this expertise to develop data and insight-driven use-cases for cyber security, such as richer cyber dashboarding for security leaders to better pre-empt security events and make proactive risk-based decisions. By employing data science and machine learning it will drive efficiency across security activities and ultimately improve maturity and enhance risk management capability.

Security Orchestration, Automation and Response (SOAR) refers to a set of technologies and processes that are growing in prominence. It enables security teams to better integrate their security toolsets and automate playbook responses. However, implementing the principles and technology of SOAR has its challenges. Within a legacy-controls environment SOAR may not initially produce tangible benefits whilst increasing complexity. Security operations teams also often lack the expertise to define and implement SOAR effectively. Where businesses have invested in developing the right capabilities, SOAR delivers consistent and effective security activities and releases time for skilled security teams to deliver value elsewhere, alleviating the capacity constraints on the function. Removing laborious and repetitive work also drives better employee retention in an industry with increasing skills shortage.

Spanning both automation and prioritisation is 'Compliance-as-code', which is the principle of automating the monitoring compliance with pre-defined, coded compliance statements. Driving these principles into new controls and retrofitting them where possible to existing controls will remove the resource-intensive assurance processes and replace them with real-time data-driven insights and reporting.

CLIENT EXAMPLE

A global Financial Services business established architectural principles that required all services to align and report on compliance-as-code security standards. The move required upskilling their Governance, Risk and Compliance (GRC) team and establishing the relevant tooling and processes across the business. The transition has enabled significant reduction in the effort to develop management reporting and has been used by product delivery teams to establish feedback loops into the DevOps pipeline.

PRIORITY 4: WORK COLLABORATIVELY WITH THE WIDER BUSINESS

We have seen acknowledgement in recent years from security functions that they cannot deliver and monitor a comprehensive set of capabilities as a silo. There needs to be some reliance on the broader business to own, manage and tap into security controls and services. This devolution of responsibility has not been an easy transition for many security functions. It involves a repositioning of the security operating model and the effort to establish the guardrails that will support and guide the business, which can be a significant upfront investment of time and resources. As a result, the status quo is often considered preferable even if it has been acknowledged as unsustainable in a rapidly changing business.

In this transition, network operators are in an advantageous position given the highly critical nature of their operations, the increasing regulatory scrutiny, and the technical nature of their business. This has resulted in the workforce being far more security conscious than in many other industries. Additional training will, in most cases, still be necessary as operators embrace new digital technologies. Security champions or advocates across the business will need to be upskilled in the security implications of the domains in which they operate but they start from a higher baseline of awareness and will be supported by a culture which is less opposed to secure practices.

Absolute and uncompromising trust isn't the end state here. Establishing guardrails and support structures for the business should ensure the right checks and balances are installed, which can then be supported by the security champions and reinforced with data-driven metrics.

Future-proofing cyber security

Security teams need to support the business by optimising cyber capability and risk management. They need to establish strategies and roadmaps that deliver change effectively and efficiently, in a way that allows the business to adapt at pace with the wider industry. The challenge is in maintaining a strategy and roadmap of change as business objectives shift and augment. To deliver future-proof and efficient cyber security, security leaders should implement the following three steps:

STEP 1: BUILD A CYBER STRATEGY THAT ENABLES THE WIDER BUSINESS TO ADAPT

- Enabling the pace of business change requires security teams to be adaptable. Establish mechanisms to enable the flexibility to revisit the strategy and underlying objectives as the business and external landscape shifts. Developing 'living' components within your strategy will allow you to adapt objectives based on the latest relevant insights from threat intelligence and the business.
- Set out clear objectives within the strategy that are adaptable, focused on response times and on user experience. Ensure that this agenda is understood across leadership.
- Enable continuous monitoring and reporting against the strategy by employing technologies which can deliver this, incorporating data insights where possible. Embed agile methods into your approach to security. Move away from PowerPoint to more dynamic reporting where leaders can interrogate the data more regularly.

STEP 2: ESTABLISH AN OPERATING MODEL THAT MINIMISES COLLABORATIVE FRICTION

- Devolve responsibility to the business to deliver and operate security controls where appropriate to do so. Invest in developing the guardrails to support the business and monitor the on-going efficacy of controls through a more robust and automated assurance model.
- Deliver using a service-orientated model. Enable the business to utilise services like vulnerability scanning, project support and supplier assessments in a pay-as-you-go model. Underpin this with clearly defined expectations, monitoring and reporting on risky business areas.
- Draw down on expertise from across the business. Establish working groups with relevant stakeholders across the business to collaborate on opportunities. Use data science expertise to elevate the efficacy of metrics and reporting.

STEP 3: DELIVER QUANTIFIABLE VALUE

- Develop mechanisms for monitoring the value of risk reduction and avoidance. Upskill security teams and the business on quantified risk management principles. Establish clear and quantified risk reporting that articulates ROI for budget relative to risk reduction.
- Work with the business to develop opportunities for value creation. Where capabilities are mature, consider expanding them as commercial services for both B2B and B2C customers. Consider segregating or spinning up separate services to ensure that internal security is not compromised.

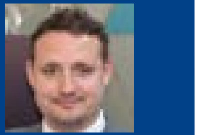
The risk and complexity of unpicking the current landscape of regulation and technology is growing for network operators. Security leaders must act now to stabilise the security of operations today and build a cyber strategy for the future, or risk facing huge penalties, brand impacts and being left behind.

DAN NICHOLSON

PARTNER
Dan.Nicholson@baringa.com

DAVID PRINCE

DIRECTOR
David.Prince@baringa.com



JAMES DAVIDSON

SENIOR MANAGER
James.Davidson@baringa.com

Baringa is one of the world's leading independent management consultancies, with 21 years' experience advising governments and industry on business change and cyber security. Baringa have been involved in defining some of the most material legal and regulatory cyber security framework changes across Europe, America, and the UK. Our teams have deep understanding of cyber regulations and extensive experience in adapting our clients' businesses to the needs of the regulation. Our consultants are experienced in engaging C-Suite and their teams to prioritise risk management decisions, build resiliency across their organisations, and protect critical assets. We have supported organisations in establishing effective security capability and have worked with clients in establishing successful business propositions around cyber security that have driven revenue whilst uplifting internal security capabilities.

Our team is passionate about helping operators to optimise their cyber strategy and operations to set up for success. We would welcome your thoughts on the topics we've discussed in this article, and how you see these challenges impacting your organisation.

www.baringa.com