White Paper

HardenStance

Partnering Government for Better Telco Security

By Patrick Donegan, Principal Analyst, HardenStance

Sponsored by

MOBILEUM

September 2018

Executive Summary

- Telco security professionals should look for the opportunities arising from greater engagement by governments around the world in cyber-security and telco security.
- Upper management and the Board of Directors in an operator often need more than generic, non-binding, industry-wide guidelines to sign off on security spending.
- Working with industry associations, national cyber-security agencies can be key in helping telco security professionals achieve their goals.
- An example of national cyber-security agencies making a powerful contribution is in making the case for investment in signalling firewalls.

It's become a mundane fact of life that there is a growing threat to privacy and business continuity - and ultimately to public order and human life – posed by three widespread abuses of Information and Communications Technology (ICT). These abuses consist of the unauthorized use of private customer data; the use of technology in support of physical-world criminal and terrorist activity; and global cybercrime.

National cyber-security agencies can be key in helping telco security professionals secure their goals.

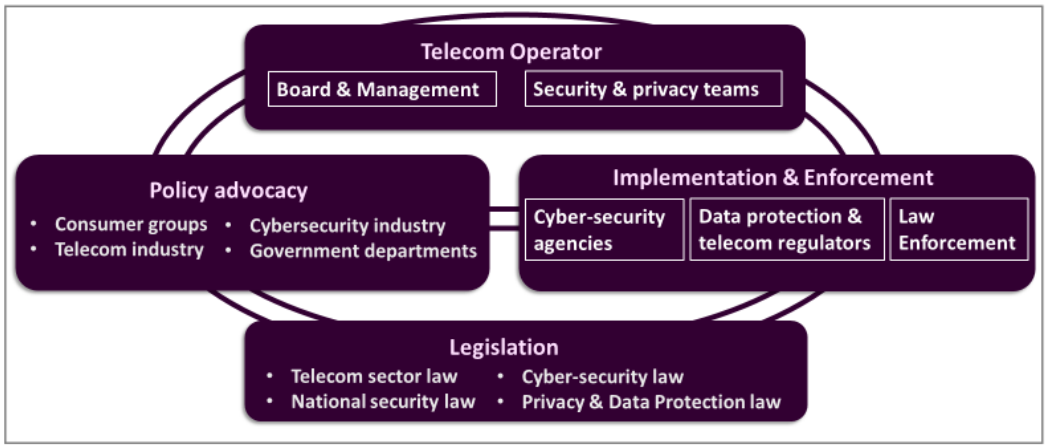
A wave of new legislation all over the world

Driven by heightened fears, governments and legislatures throughout the world are scrambling to protect their citizens and businesses against these abuses. Inevitably, telecom operators are among the organizations that governments turn to first in designing and enforcing an enhanced cyber-security and privacy framework for the businesses, consumers and government departments they serve.

Whether it be through legislation on data protection, law enforcement, cyber-security or the telecom sector itself, a huge number of countries including Australia, Brazil, Chile, Germany, Ghana, the Netherlands, Nigeria, the UK, Saudi Arabia, South Africa and Singapore have all passed new laws in at least one of these areas in the last couple of years. New legislation is also ongoing as far afield as India and Thailand. The EU's General Data Protection Regulation (GDPR) also came into effect this year. New laws are also making their way through many other parliaments around the world. Each of these laws impacts one or more aspects of how telcos protect their infrastructure and revenues; how they protect customer data at rest, in use or in transit; or indeed how telcos are required to expose customer data to law enforcement.

As shown in **Figure 1** an operator arrives at its security posture via a combination of its obligations as set out by government as well as its own priorities. Within the operator, investment decisions arise from the Management team and the Board scrutinizing how much the security team wants to spend – and on what.

Figure 1: The security policy framework for the telecom sector



Source: HardenStance

Management then decides, taking into account the company's business goals, its appetite for business risk, and other competing spending priorities. The way telecom operators interact with these three layers of policy advocacy, legislation, and implementation and enforcement that drive government policy in these areas has been largely unchanged for decades. But these relationships - and the outcomes arising from them – are starting to change now. This paper explains these changes and how telco security professionals can leverage them to their advantage.

Government functions are being restructured

Within the Executive branch of government, change is being introduced in the staffing, structure and powers of cyber-security agencies that support implementation and enforcement of policy. Traditional 'national security' remits are being expanded to allow broader, more open, engagement with citizens and businesses. As shown in **Figure 2**, legislation is often driving the creation of entirely new national cyber-security agencies.

The traditional remits of cyber-security agencies are being expanded to allow broader, more open, engagement.

Figure 2: New National Cyber-Security Agencies are being formed

Country	Formed	New agency	Agency's mission
Malaysia	2017	National Cyber Security Agency (NACSA)	A stable, safe and resilient cyber environment to protect Malaysia
Poland	2016	National Cyber Security Centre (NC Cyber)	Coordinate government and industry efforts in cybersecurity
Saudi Arabia	2017	National Authority for Cyber Security (NACS)	Boost the state's cyber-security & protect sensitive infrastructure
Singapore	2015	Cyber Security Agency of Singapore (CSA)	Oversee national cyber-security strategy, ecosystem and outreach
UK	2016	National Cyber Security Centre (NCSC)	Make the UK the safest place to live and do business on-line

Source: HardenStance

The ways that these agencies engage with the telecom sector is evolving in line with these changes. In the case of Lawful Intercept (LI), there are one or two cases of national cyber-security agencies being given enhanced powers over telcos. For example:

- **France's Agence Nationale de la Sécurité des Systèmes D'information (ANSSI)** now enjoys formal powers to overrule and reject a French operator's choice of networking equipment used in providing Lawful Interception (LI).
- **Under New Zealand's Telecommunications (Interception Capability and Security) ACT (TICSA)** of 2013, telecom operators are now formally required to gain the approval of the Government Communications Security Bureau (GCSB) before carrying out any significant changes to their networks.

In both these cases, informal collaboration between government agencies and telecom operators in this area goes back many years. In both cases, mandating such influence over an operator's security posture by government agencies in law marks a change. It has potential to alter the way security strategy is formulated and implemented.

Government agencies can be supportive allies

Among western and western-leaning countries, cases of government agencies being given stiff new powers to direct telecom security strategy are still the exception rather than the rule. A more common model which is emerging is one in which government agencies are engaging as partners with the security teams in the telecom operator. Here they are investigating specific vulnerabilities and helping telco security professionals build the business case for investing in new protections.

One example is how national cyber-security agencies in Norway, the UK and the US are helping build the case for signaling firewalls in mobile networks. The GSMA's Fraud and Security Group (FASG) is already well established in this area, providing detailed technical recommendations and advocacy. The European Union Agency for Network and Information Security (ENISA) added its weight to this case with its March 2018 report "Signaling Security in Telecom SS7/Diameter/5G". This calls on the EU to "consider revising the current legal landscape so that signaling security is covered." The report embraces emerging 5G standardization and the first 5G network build-outs.

At the national level where the actual implementation of telecom security gets done, support from national government agencies in the implementation and enforcement layer can be very helpful to telco security teams. The latter often recognize the need for signaling firewalls, but they need additional compelling validation to convince the operator's upper management or Board to invest. Three case studies follow below.

Since government recommendations were issued, mobile operators in Norway have invested in SS7 firewalling.

Case study #1: NKOM (Norway)

NKOM is Norway's Communications Authority. The country has direct experience of a network outage triggered by SS7 vulnerabilities. In February 2015 more than a million of Telenor's customers went several hours without service arising from what proved to be the benign signaling vulnerability testing of one of its roaming partners.

In 2016 NKOM, together with the telecom regulators in the three other Nordic countries, issued joint recommendations to mobile operators in their markets around closing off SS7 vulnerabilities. HardenStance has validated with NKOM that the operators in Norway have since invested in SS7 firewalling capabilities. NKOM has subsequently asked the mobile operators in Norway for a status update with respect to Diameter security. A potential next step which NKOM is considering is an independent third-party test to potentially verify the security status across both protocols.

Case study #2: CSRIC (US)

The Communications Security Reliability and Interoperability Council (CSRIC) is a department within the US Federal Communications Commission (FCC). In March 2017 CSRIC published its report on "Legacy Systems Risk Reductions" focused on SS7 and Diameter. CSRIC concluded that "the probability that bad actors will exploit this community of trust has increased." It "recommends and endorses the GSMA security best practices and guidelines to secure signaling interconnection for SS7 and Diameter." And it recommended that mobile operators in the U.S "need to be measured as they implement steps and solutions in order to avoid collateral network impacts."

Case study #3: The NCSC (UK)

The UK's National Cyber Security Centre (NCSC), is the country's authority on cyber-security. It is part of Government Communications Headquarters (GCHQ) and was created as a separate entity in November 2016. NCSC is a model for how a national cyber-security agency should engage with industry in general and the telecom sector in particular. At this year's ETSI Security Week in Nice in June, for example, there were more participants from NCSC than any other national cyber-security agency.

Signaling security is just one of the areas that NCSC has engaged in heavily with telecom operators. HardenStance has validated with the relevant UK government authorities that substantially all of the UK's operators have now completed extensive independent tests on their SS7 infrastructure, carried out for NCSC by an independent third party. During the first half of 2018, NCSC has communicated the exact risks posed by current vulnerabilities in the UK's SS7 infrastructure to the UK government. It is now helping the operators' security teams make the case for implementing the GSMA's guidelines.

Figure 3: Government agencies are helping make the case for SS7 firewalls

Country	Government Agency	Work done on signaling security	Outcome
Norway	NKOM	Recommendations issued to local operators	Operators are investing in line with Recommendations
UK	NCSC	Testing undertaken on all UK networks	Working with UK operators to implement GSMA guidance
USA	CSRIC	Report endorses GSMA guidelines	Enhanced technical case for investment by US operators

Source: HardenStance

GDPR's reach could extend to signaling vulnerabilities

Whereas their record in protecting the confidentiality of customer data in transit is generally excellent, when it comes to data at rest telcos have been just about as vulnerable to serious data breaches as any other sector of industry. GDPR in Europe and some GDPR-like regulations coming to the fore in other countries will impose the same privacy-oriented regulatory regime across all organizations. There's a dimension to this that blurs security and privacy from a telco perspective, though. Given that some signaling vulnerabilities can lead to private customer data being exposed, failing to fix them could leave operators open to penalties under GDPR.

On their own, industry associations often don't carry enough weight to drive a decision in favour of investment.

Making best use of the security policy framework

As they consider the impact of key government actors responding rapidly – and wanting to be seen to respond quickly - to the new cyber-security and privacy landscapes, telco security professionals needs to recognize that there is both opportunity and risk in this.

There is certainly a risk of the executive branch being given too much power. Inappropriate or inflexible government mandates can be unhelpful. The same is true of decisions or implementations that have to be delayed in order to align with bureaucratic timescales or overtly political agendas.

There is a lot of opportunity too, though. Telco security professionals should recognize that they need help securing the budgets they need from their upper management – and that national cyber-security agencies can be very helpful to them.

Industry associations and standards bodies do enormously important work in making the case – and specifying the solutions – for fixing security vulnerabilities. But the truth is that at the level of upper management and in the Boardroom, industry associations often don't carry enough weight to drive a decision in favour of investment.

Getting the business case over the line

Industry associations are often seen as advancing generic, non-binding, guidelines for dozens or hundreds of organizations world-wide and which may not be relevant to a company's unique marketplace. In the absence of compelling evidence of a security threat that poses a clear risk, the typical default position of management and the Board in the operator is to defer investment. Clear evidence and specific guidance from a national cyber-security agency, or other regulator representing the government in the operator's home market, is often a lot more persuasive.

Where there is an opportunity to leverage them as allies, telco security professionals and industry associations should therefore welcome government and government agencies engaging more deeply in the cyber-security and telco security space. With the right partnership approach, they can achieve common goals■

About Mobileum

Mobileum delivers analytics solutions that generate revenues, reduce costs and accelerate digital transformation for more than 600 communications service providers across 150 countries. Mobileum's solutions help to grow and protect existing CSP revenue streams, as well as drive new revenues through business model innovation. We focus on specific domains including roaming, counter fraud and security, data monetization and digital transformation. Mobileum's success is built on its unique Active Intelligence platform which combines analytics and engagement technology with deep network and CSP systems integration to deliver end to end solutions.

Mobileum is based in California's Silicon Valley, with offices in Argentina, Dubai, Hong Kong, India, Ireland, Jordan, Singapore and Uruguay. To learn more, visit www.mobileum.com and follow @MobileumInc on Twitter.

About HardenStance

HardenStance is a leading independent industry analyst firm delivering trusted research, analysis and insight in IT and telecom security. www.hardenstance.com