White Paper

HardenStance

Supply Chain Security for Telecom Operators

By Patrick Donegan, Principal Analyst, HardenStance

Sponsored by

July 2021

Executive Summary

- Faced with a perfect storm of new supply chain risks, telcos should expect a lot more of themselves and their suppliers with respect to investing in transparency as well as security automation, testing and monitoring throughout the supply chain.
- The fact that telcos are among the victims of the SolarWinds attack reaffirms how critical it is to get security right with the transformation of the software development life cycle (SDLC) that underpins 5G.
- Geopolitical tensions and the pandemic are creating chipset supply constraints. Telcos can mitigate this risk by reaching back into the supply chain to strike new deals with their vendors' chip suppliers as well as with their vendors.

A Revolution in Telco Supply Chain Management

The telecom sector likes to think and act in terms of evolutions rather than revolutions. As far as possible, telcos like to undertake large scale vendor rip and replacements with zero service interruption. They like to leave legacy services uninterrupted when new ones are rolled out. The telecom sector generally doesn't like revolutions.

The supply chain disruptions that have been heaped on over the last three or four years leave little doubt that telco supply chain management is undergoing a revolution.

Going back three or four years, telco supply chain management leaders could clearly foresee that a major change in best practices was upcoming. 5G being a cloud native network necessarily implies far greater automation of a telco's development environment, including greater automation in the way new software is sourced, secured, integrated and released. One could certainly argue the contrary, but three or four years ago, supply chain leaders could plausibly present this as evolution rather than revolution.

As captured in **Figure 1**, four major new supply chain disruptions have erupted over the last three or four years. These are driving what is more usefully thought of now as a revolution in telco supply chain management. These four drivers are described below:

Geopolitical tensions are raising barriers to trade in ICT products. Telcos in countries that are allied to the United States now face restrictions or outright bans on buying 5G network products from Huawei, the world's largest networking vendor. U.S. semiconductor vendors also face restrictions or outright bans on selling to Huawei and other Chinese vendors. With the U.S. and China seemingly set on a new path of creating separate and competing ICT ecosystems, the imposition of these new trade barriers is creating new supply chain risk for telcos and throughout the ICT ecosystem.

The SolarWinds breach points to heightened cyber risk to supply chains. Businesses have been dealing with cyber attacks that exploit software vulnerabilities in their supply chain for many years. For example, Singtel was among the many victims of such an attack arising from exploits discovered in the file transfer software of Accellion, an enterprise software vendor. Odd as it may sound, though, the cyber security industry does not define these as 'supply chain attacks'. That term refers to very specific attacks like the one on SolarWinds that are more difficult to prevent and also tend to impact a lot more victims. That's because, as defined by the cyber security industry, a 'supply chain attack' like the one on SolarWinds arises from the unauthorized insertion of a

Figure 1: Threats and Disruptions to the Telco Supply Chain

Source: HardenStance

vulnerability, usually into popular business or consumer software *prior to* that software being deployed (which is what makes it hard to detect). This potentially gives the threat actor – typically an Advanced Persistent Threat (APT) group – access to all that software vendors' customer environments (which is why the scale of the impact is so extensive).

In one of its first blogs after the discovery of the breach, FireEye, a leading Incident Response company, stated that "telecom entities" are among the victims of the SolarWinds attack. Although the names of affected telcos haven't been publicly disclosed, it's reasonable to assume that the impact in terms of compromised data is likely to be on par with those suffered by other SolarWinds victims.

In one of its first blogs after its discovery of the breach, FireEye, a leading Incident Response company, stated that "telecom entities" are among the victims of the SolarWinds attack.

Moving Laterally from Enterprise IT into Telco Operations

Unless the initial breach is either prevented or quickly detected and mitigated, APT groups can establish an initial foothold in enterprise IT infrastructure and then move laterally within a telco organization to gain access to telco operations. Imagine also how attractive a SolarWinds-style insertion of malicious code directly into a big telecom vendor's software looks to a nation state threat actor targeting the telecom sector.

An Executive Order signed by President Biden in May this year mandates that any company selling software to the U.S. federal government must supply a Software Bill of Materials (SBOM) that provides transparency into all of the software components used in building the application. This is a direction of travel that the telecom industry may find itself having to comply with in the coming years.

The pandemic has triggered semiconductor demand volatility: By triggering major changes in consumer behaviours, the pandemic has created new volatility in chipset demand. Specifically, the shift to remote working drove a surge in demand for home entertainment products like high end computers, games consuls and flat screen TVs as well as streaming services like Netflix.

The Telecom Market Requires Better Incentives to Improve Security

This White Paper provides guidance on best practise supply chain security for telcos in the context of the new global market environment they find themselves operating in. Whether or not they have the resources – and above all the incentives – to apply those principles in full is a different matter.

This question of incentives is one that was well articulated by the UK Department of Digital, Culture, Media and Sport (DCMS) in its July 2019 report entitled "UK Telecoms Supply Chain Review". This noted key failings in the incentives that telcos have to improve cyber security. The report pointed to:

- insufficient clarity on the cyber standards and practices that are expected of industry;
- insufficient incentives to internalise the costs and benefits of security. Commercial players are not exposed to the full costs and consequences of security failures; security risks are borne by government, and not industry alone;
- a lack of commercial drivers because consumers of telecoms services do not tend to place a high value on security compared to other factors such as cost and quality; and
- complexity of delivering, monitoring and enforcing contractual arrangements in relation to security.

Whilst the DCMS report only addressed the UK market, those same shortcomings will sound familiar to telcos and telco regulators all over the world. The above point serves as an important reminder that without supporting adjustments in incentives, many telcos will struggle to rigorously implement at least some of the supply chain security enhancements recommended in this White Paper.

Notably the automotive industry over-estimated the extent to which demand for cars would fall during the pandemic and slashed its orders accordingly. When it found demand holding up a lot better than expected, automotive manufacturers found chip suppliers unable to fulfil their new orders because they were unable to even keep up with demand from more dependable customers in the consumer electronics and networking markets.

Climate change is disrupting chip production: The vast majority of the world's chip manufacturing capacity is concentrated in Taiwan, Korea, China, Japan and other parts of the world that are among the most vulnerable to extreme weather events driven by climate change. This is making chip production increasingly vulnerable to major disruption. In March this year, power shortages arising from severe storms forced Samsung to halt production at its chip factory in Austin, Texas, where it manufactures for customers like Intel and Qualcomm.

The rest of this White Paper explains how telcos must adapt to mitigate the new risk that is being introduced into their supply chains. The paper describes the techniques telcos must embrace to assure availability of supply of the hardware and software components they need; ensure that they can have a high degree of trust in the integrity of those components to allow full-blown commercial release; and be able to detect, respond and minimize the impact of any breaches that do occur in live operations.

Assuring Diversity of 5G Network Suppliers

Telco security operations professionals typically prefer fewer public cloud partners to allow mastering of a provider's unique tooling environment.

In many western countries, the imposition of government restrictions or outright bans on buying Huawei's 5G network products is presenting a major disruption to supply chains. In many cases, extracting and writing down investments in Huawei products will take years. Telcos and national security agencies are also uncomfortable with the risk this creates of becoming 'locked-in' to a 5G vendor duopoly of Ericsson and Nokia.

Samsung is the main credible contender to be a third trusted end-to-end 5G system supplier for telcos that are barred from using Huawei. Key wins with NTT DoCoMo, Singtel, Verizon and Vodafone suggest Samsung is 'going big' in 5G networks, but it must still show it's ready to go beyond 'cherry-picking' from among the biggest accounts.

The market in 5G core network software is pretty healthy. Alternatives to the end to end 5G system suppliers are available from Cisco, Microsoft, Oracle and NetNumber. The bigger challenge in terms of ensuring supplier diversity is with 5G Radio Access Network (RAN) products. Efforts here are focused on trying to build an OpenRAN ecosystem that could allow multiple trusted providers of specialist RAN hardware and software components to thrive in a more open RAN ecosystem.

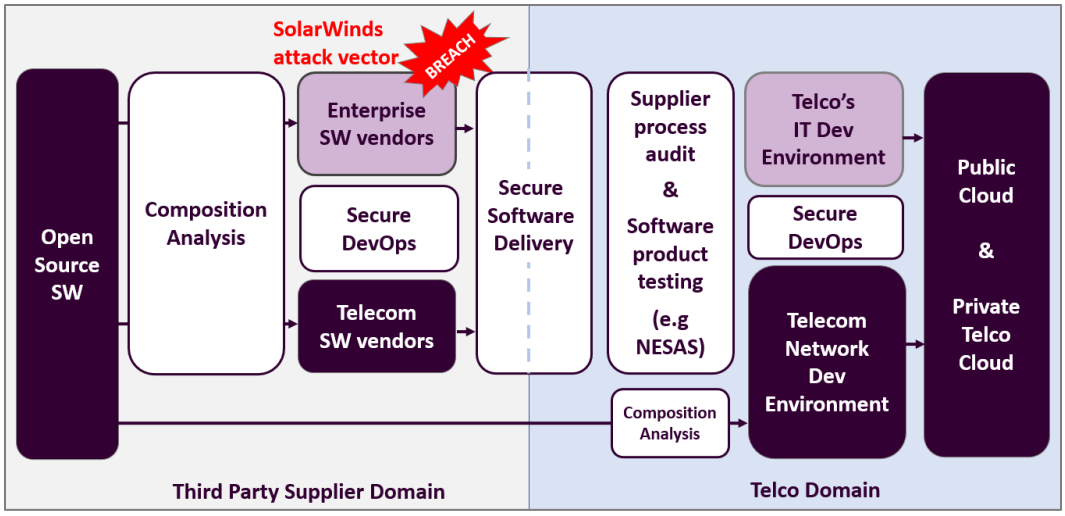
Telco strategy with respect to public cloud partnerships also poses questions – as well as potential trade-offs – between diversity of supply and security. Telco security operations professionals typically prefer fewer public cloud partners to allow mastering of a provider's unique tooling environment. Supplier diversity considerations object to the risk of a single point of failure that arises from restricting the number of partnerships with cloud partners (not to mention denying choice to enterprise customers).

Software Vulnerabilities & Exploits

The stunning successes achieved by Russian cyber threat actors via the SolarWinds attack (and other attacks like Codecov) make it likely that APT groups are focusing more attention on the supply chain attack vector. In the UK government's "Telecoms Supply Chain Review" cited on the previous page, it references the country's National Cyber Security Centre (NCSC) as assessing the risk of disruption or data compromise to UK networks via a vendor's administrative access to the telco's network as "high".

Telcos are going to have to raise their game here and expect more from themselves and their suppliers in terms of investing in transparency and in security verification and

Figure 2: Managing Software Vulnerabilities in the Supply Chain



Source: HardenStance

testing throughout the supply chain. The UK's NCSC advises thinking of requirements in terms of four core principles of understanding the risks; establishing control; checking your arrangements; and targeting continuous improvement. A multi-layered approach to security checks throughout the supply chain is needed, leveraging automation wherever feasible.

As shown in **Figure 2**, the management of software vulnerabilities spans the whole telco supply chain, covering the domains of third party IT and telecom software vendors as well as the telco's own enterprise IT and telecom domains. As part of that, telcos need to ensure that investments are aligned with heightened risk in the following key areas:

Telcos should be auditing the security practices of third party vendors throughout their software development lifecycle.

- analysis of open source software vulnerabilities;
- auditing the security practices of third party vendors throughout their software development lifecycle (SDLC);
- best practise security verification and testing of third party software at the point the telco itself takes delivery of it;
- transforming the telco's own lifecycle management of software across both development and operations for private and public cloud environments.

Analysis of Open Source Software Vulnerabilities

Telecom vendors, not to mention telcos themselves in many cases, are making increased use of open source software. Software composition analysis tools should be used to scan these open source software packages, evaluate the risk of exposure that may arise from those vulnerabilities, and ensure compliance with licencing guidelines.

When it comes to dealing with a vendors' use of open source software, telcos face a choice. Either the telco limits itself to whatever versions of open source components the vendor itself supports, together with a comprehensive SLA. Alternatively they buy the vendor's proprietary software and potentially integrate the very latest supporting open source components themselves. In this scenario, the vendor SLA is likely to be less comprehensive and the telco has to proactively manage security issues itself.

Auditing The Security Practices of Third Party Vendors

It's been common practice for years for telcos to require their vendors to share their secure software development and life cycle (SDLC) policies as a part of the procurement process. Increasing cyber threats to the supply chain now require that telcos up their game here by adopting the core cyber security principle that you 'trust but verify'.

This is captured in the 'Prague Principles' that emerged from a 2019 cyber security conference in the Czech capital attended by government officials from 32 countries, the EU and NATO. Among these principles are that 5G vendors must demonstrate a secure software development process. The EU incorporated these principles into its 'EU Toolbox on 5G Cyber Security', released in January 2020.

Telcos should now be requiring an independent audit and certification that verifies in detail that the process described is indeed observed in the vendor's day to day operations. While the GSM Association's (GSMA) Network Equipment Security Assurance Scheme (NESAS) is sometimes associated only with a test suite for testing mobile network software, NESAS also serves as a standard for this kind of independent security assessment of vendor SDLC policies. All of the big end to end 5G system vendors have now passed NESAS-certified development audits for at least one part of their portfolio. Telcos should be pushing this requirement onto their other vendors as well.

It should be mandatory for all developers to download from that trusted internal repository rather than be permitted to download open source software independently themselves.

It's Not Enough Just to Vet Open Source Software

One important aspect of a secure SDLC policy is how a vendor actually uses open source software internally. It's not enough for a vendor to do all the right things in terms of doing software composition analysis and clearing a given software package for internal use. Those vetted packages also need to be hosted securely in internal repositories. It should also be mandatory for all developers to download from that trusted internal repository rather than be permitted to download open source software independently themselves. Where a telco integrates open source software itself, the same applies to its own development environment.

Another important aspect of reducing risk in the SDLC is the release and update management tools that vendors use to deliver their software to telco customer sites. Particularly in the context of 5G software and the decomposition of monolithic Network Functions (NFs) into microservices, telcos should be demanding release and update management tools that reduce the risk of the kind of malicious intrusion that occurred with the SolarWinds attack. Among the key capabilities that count here are:

- a secure, interface between the vendor's premises and remote telco customer sites, complete with integrity protection. This should monitor and verify that the software package received at the customer site has not been altered in transit.
- a high level of automation to reduce the number of manual interventions.
- customized delivery so that a given telco customer only gets precisely those software updates it needs (and no more). This reduces the potential attack surface.
- securing of received software updates at rest at customer sites.

Testing Vendor Software

As well as applying the 'trust but verify' principle to gain transparency into a vendor's SDLC policies, it's just as important that telcos apply it to their actual consumption or ingestion of vendor software.

Best practise security requires telcos to do their own testing of vendor software packages for vulnerabilities prior to operationalizing it. Some national security agencies have advanced telecom software testing requirements – leveraging their own test suites – which local telcos and their vendors must comply with. NESAS is also building a test suite with independent certification that vendors can use as proof-points with mobile operators anywhere in the world.

Greater risk in the threat landscape requires that telcos also invest in penetration testing. This is needed to assess the potential of new software to trigger security events arising from the specific architecture and configurations within an individual telco's own unique environment.

Security in Development and Operations

In the migration to agile development based on 5G microservices, many telcos are still not where they need to be in terms of understanding, let alone operationalizing, security across their development and operations environment.

The principle of driving security into the early part of the development process rather than making it a gating process at the end – often referred to as 'shifting left' – is essential to removing flaws as early as possible and automating security as code. But moving security to the right into operations is also important for generating a feedback loop on attacks seen in the network. These can then be fed back into development.

Like most other aspects of cyber security, supply chain security isn't a technical problem to be solved, it's a business risk to be managed. This requires security teams to learn the interpersonal skills to train, persuade and inspire development and operations teams to work with them as partners and allies. In practise, that means security teams thinking of themselves as 'servant-leaders' who view development and operations leaders as their customers. This is key to operationalizing security so as to maintain the chosen trade-off between fast time to market and low risk to the business.

Security operations has to focus on detecting threats that get through – as some inevitably will – as well as minimizing the impact or 'blast radius'. This relies on effective network zoning as well as detecting and responding to threats as soon as possible when they first appear in the environment. Once attackers obtain administrative credentials, it's easier for them to hide and start manipulating logs or switch off logging altogether. Hence automated monitoring and analysis of logs is an extremely important aspect of detection and response capabilities.

Like most other aspects of cyber security, supply chain security isn't a technical problem to be solved, it's a business risk to be managed.

Adapting to Greater Volatility in Chipset Supply

The ICT market, of which the telecom sector forms a key part, accounts for roughly half of global semiconductor consumption. It hasn't suffered the same problems as the automotive sector in adjusting to new supply and demand volatility, but it has been negatively affected as demonstrated by the examples below:

- Qualcomm, Cisco and Nokia have all guided investors to expect continued shortages throughout 2021. In April, Nokia's CEO, Pekka Lundmark, told Reuters that "it would be naïve for anyone to say that this would not be a serious shortage, and most likely it will continue for another year or even two years."
- In comments to the FCC earlier this year, the U.S Telecommunications Industry Association (TIA) predicted that silicon wafers will be in short supply until 2023, predicting that "in 2022 demand will be around 150% of existing fab capacity."
- In May, AT&T's CEO, John Stankey was cited in Light Reading as stating that he was "a little skittish" about supply shortages. In June, the CTO of Rakuten Mobile, Tariq Amin, told Light Reading "the situation is much worse than I had anticipated" and that "everyone I talk to tells me this will be an uphill battle for the next 24 months."

It's not just availability that's at stake. There's also a risk of exposure to rising prices, which risks being exacerbated by vendors stockpiling supply. The coincidence of so many disruptive factors converging to impacting global chip supply – together with the fact that most of them will play out over many years - means telcos must reach further back into the supply chain than they're used to and engage with the semiconductor industry. As depicted in **Figure 3**, there are four specific things they can do here:

1 Invest in 'Supplier of the supplier' deals with chip suppliers;

2 Maintain and audit dedicated chip inventory;

3 Inspect and verify the chipset content of vendor products;

4 Negotiate local or regional manufacturing (with network vendors and chip vendors).

Invest in 'Supplier of the Supplier' Deals with Chipset Suppliers

The first invokes the 'trust but verify' principle again. In today's marketplace, telcos can't have the same confidence as they could in the past that a network vendor partner can fulfil its orders. That requires greater transparency into a vendor partner's supply agreements with its chipset vendors. Specifically, telcos should be considering requiring independent verification from chipset suppliers of the terms of their supply agreements with network vendors, and potentially doing deals directly with those chip suppliers to assure supply is dedicated to meeting their own specific orders. This may also require telcos agreeing to some more stringent contractual terms with their network vendors

Maintain and Audit Dedicated Product Inventory

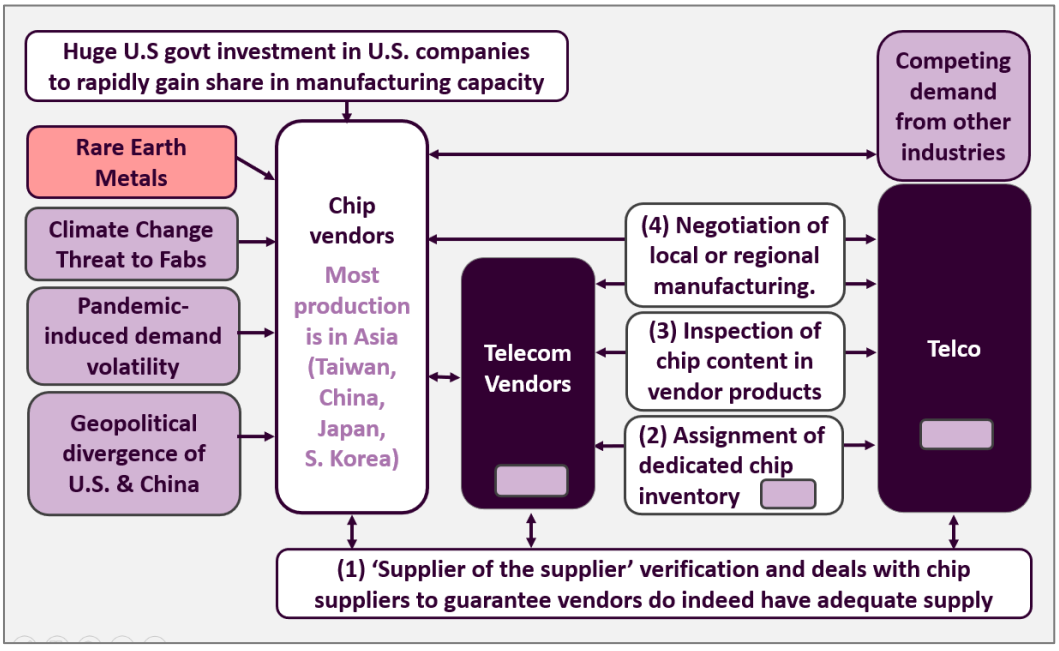
Maintaining access to dedicated product inventory as well as spare parts has always formed part of good telecom supply chain management but it's becoming more critical now. Larger telcos have the bargaining power to require that vendors dedicate a part of their inventory to them on their own premises. Smaller telcos may find they need to increase their own inventory holding capacity.

In affected markets, telcos must implement new procedures for systematically inspecting vendor products for banned chipset content prior to deployment.

Inspect and Verify Chipset Content of Vendor Products

In affected markets, telcos must implement new procedures for systematically inspecting vendor products for banned chipset content prior to deployment. As regulated entities, deploying networking products that feature banned components is a greater risk to the telco operating a service off those products than it is to the vendor shipping the product. In the case of some of the bans already in force, there are layers of ban dependency between the hardware itself, design software and the use of machines used in certain types of manufacturing processes. These are very early days in terms of telcos and their vendors having to adjust to these new government-imposed component restrictions. Telcos must guard against deploying vendor products that are non-compliant with some of these new government bans.

Figure 3: Engaging in The Supply Chain to Secure Long Term Chipset Supplies



Source: HardenStance

Negotiate Investment in Local or Regional Manufacturing Capacity

In a global market which is fragmenting along political lines, telcos throughout the Americas and EMEA should recognise the increased risk posed to their supply chain by the dependency of their network vendors on Asian chipset vendors and the concentration of global chipset manufacturing capacity in Asia. Reducing risk here requires taking steps to develop manufacturing capacity in-region, closer to local telco operations.

There's not much point in building local chip capacity without also investing in local manufacturing of network routers, base stations, transport equipment or other heavily chip-dependent products.

There are a couple of key things to note about this. The first is that telcos are generally not big enough to drive those kinds of large scale, multi-year, capital-intensive investments in manufacturing capacity by themselves. Even several telcos working together at a national or regional level must still coordinate extensively with the vendors themselves as well as with governments, banks and other ICT stakeholders.

The second thing to note is the importance of having a 'joined up' approach with respect to investing in local manufacturing capacity, whether it be in chipsets or networking products. Specifically, there's not much point in building local chip capacity without also investing in local manufacturing of network routers, base stations, transport equipment or other heavily chip-dependent products - and vice versa.

Telcos should work with one another and their network vendors to recognize that a more uncertain outlook for global chipset supply is a risk to both sides of industry and to work together to de-risk their positions. It's also important to consider the timelines for such projects. As an example, Taiwan Semiconductor Manufacturing Company (TSMC) announced a $12 billion investment in a fab in Arizona in the Spring of 2020. This won't actually come on-line until 2024 at the earliest. ■

More Information

- HardenStance White Paper: A Blueprint for a Cloud Native Telco (February 2020)

About the Sponsors

The sponsors of this White Paper are NetNumber and Deutsche Telekom Security.

About NetNumber

NetNumber, Inc. brings 20 years of experience delivering platforms that power global telecom and enterprise networks. Our software-based signaling-control solutions accelerate delivery of new services like Private LTE and IoT/M2M solutions across multi-gen networks, dramatically simplifying the core and reducing opex.

These solutions span a range of network types from 2G-3G-4G-5G to future G delivered on the industry's most robust signaling platform called TITAN. NetNumber Data Services are essential for global inter-carrier routing, roaming, voice and messaging. Data powers fraud detection and prevention solutions and enables enterprise B2B and B2C communications platforms. NetNumber multi-protocol signaling firewall, fraud-detection, and robocalling solutions help secure networks against current/emerging threats. For more information visit www.netnumber.com.

About Deutsche Telekom Security

Deutsche Telekom is one of the world's leading integrated telecommunications companies, with some 242 million mobile customers, 27 million fixed-network lines, and 22 million broadband lines. Deutsche Telekom is present in more than 50 countries. With a staff of some 226,300 (Dec 31, 2020) employees throughout the world, we generated revenue of 101 billion Euros in the 2020 financial year, about 66 percent of it outside Germany (All figures taken from the 2020 Annual Report).

As a leading telco provider, Deutsche Telekom has shaped the networking of our society for over 20 years – and knows that universal connectivity requires equally

comprehensive security measures. The most effective weapon against cyberattacks is not even technology itself – but the people who work for Telekom. Their expertise about vital security architecture, its configuration and customization for customer infrastructure is what counts most. Boosting and sharing this know-how is a top priority for Telekom. In this way, it can offer future-oriented security in a connected world.

Therefore, Telekom Security was founded as a business unit within T-Systems in early 2017 – and transformed into a separate legal entity within DTAG group on July 1, 2020 (Deutsche Telekom Security GmbH or Telekom Security for short). With over 250 million euros of revenue, Telekom Security is the market leader in Germany and one of Europe's top cybersecurity providers. For more information www.t-systems.com/security

About HardenStance

HardenStance provides trusted research, analysis and insight in IT and telecom security. HardenStance is a well-known voice in telecom and enterprise security, a leader in custom cyber security research, and a leading publisher of cyber security reports and White Papers. HardenStance is also a strong advocate of industry collaboration in cyber security. HardenStance openly supports the work of key industry associations, organizations and SDOs including NetSecOPEN, AMTSO, MEF, OASIS, The Cyber Threat Alliance, The GSM Association and ETSI. To learn more visit www.hardenstance.com