National Cyber Security Centre
a part of GCHQ

Security analysis for the UK telecoms sector

Summary of findings

January 2020

Contents

1. Introduction

Since the initiation of the DCMS Supply Chain Review in September 2018, the NCSC has performed an extensive and detailed analysis of the security of the telecommunications (telecoms) sector. The outcomes of that analysis are now being provided through a blog by the NCSC's Technical Director [1], our formal advice on the use of High Risk Vendors (HRVs) [2], and through this document, a summary of the NCSC's security analysis for the UK telecoms sector. Specifically, this document summarises the NCSC's technical recommendations for improving the security of the UK's telecoms sector, alongside a description of our technical security analysis that we used to derive these recommendations.

The security of the UK's telecoms networks is of paramount importance. The government intends to bring gigabit capable broadband to every home and business across the UK by 2025. The potential economic and social benefits of 5G and full-fibre digital connectivity can only be realised if we have confidence in the security and resilience of the underpinning infrastructure. As technologies grow and evolve, we must have a security framework that is fit for purpose and ensures the UK's Critical National Telecoms Infrastructure remains online and secure both now and in the future.

The findings of the DCMS Supply Chain Review [6] show that there is much work to be done. The review recommended the establishment of a new, robust security framework for the UK telecoms sector, with a set of new Telecoms Security Requirements (TSRs) at its heart. These TSRs will provide clarity to telecoms operators. Their implementation will ensure that operators operate secure and resilient networks and manage their supply chains appropriately.

As part of the DCMS Supply Chain Review, and as part of defining a new security framework, the NCSC analysed the cyber risk towards the telecoms sector. This document summarises the NCSC's analysis, including the methodology (Section 2), the collation of attack vectors through attack trees (Section 3), the assessment of risk due to the attack vectors (Section 4) and the significant areas of risk identified through this analysis (Section 5).

From Section 6 onwards, we set out the measures that the NCSC recommends to mitigate the risks identified in Section 5. These recommendations fall into five categories:

- TSRs, detailing how operators should reduce their most significant cyber risks
- advice to government and industry on the management of High Risk Vendors (HRVs)
- diversification of the infrastructure market
- the establishment of a National Telecoms Lab to perform a broad range of testing of the UK's telecoms networks and equipment
- continued regular and detailed threat-driven security testing of operators' networks, as performed under Ofcom's TBEST scheme

Through implementation of these recommendations, the security of the UK's telecoms sector will be significantly improved, ensuring the UK's digital economy has a solid foundation.

2. Methodology

The core of the NCSC's analysis was to enumerate the risks and threats faced by the UK telecoms sector. To achieve this, the NCSC drew on several sources.

- Details of previous attacks on the UK telecoms networks, both successful and unsuccessful.
- Our knowledge of global attacks on telecoms systems, regardless of the attacker, mainly from classified sources.
- Our knowledge of telecoms systems and security gained through our industry relationships with operators and vendors. This includes our understanding how telecoms systems are built, operated, and managed in the real world.
- Our knowledge of global standards and their security properties.
- Our world-class vulnerability research capability.
- Reports and analysis produced by the Huawei Cyber Security Evaluation Centre (HCSEC).

Pulling these threads together gives us a broad spectrum of knowledge about the ways in which actors could attack a telecoms system in the real world and how to defend against such attacks. It also allows us to anticipate and consider attacks that could be mounted over the coming years.

This array of attacks was pulled together into 'attack trees' or 'threat trees' (Section 3). These attack trees were then considered in the context of specific telecoms networks and their relative risk assessed (Section 4). From the risk assessment, the NCSC identified the most significant areas of risk (Section 5). The NCSC aimed to mitigate the most significant risks arising from this process (Section 6 onwards). By linking the mitigations to the motivating threats, the potential impact of not implementing a mitigating control is clear to government, the regulator and to industry.

The NCSC has a long history of working closely with the major UK operators, major suppliers and standards bodies and we have relied on this experience to make recommendations that will work in the UK. Our assumption is that government, through the NCSC and Ofcom, will continue to work closely with industry to ensure that network designs, operations and security mitigations are appropriate for the UK.

3. Attack trees

3.1 Overview

Attack tree analysis was used to identify cyber risks to telecoms networks. This involves identifying higher-level impacts or outcomes, and linking these to lower-level methods or exploitation routes that could contribute to such events occurring. Each individual path down the attack tree is a potential attack vector. The methodology is shown in Figure 3.1-1.

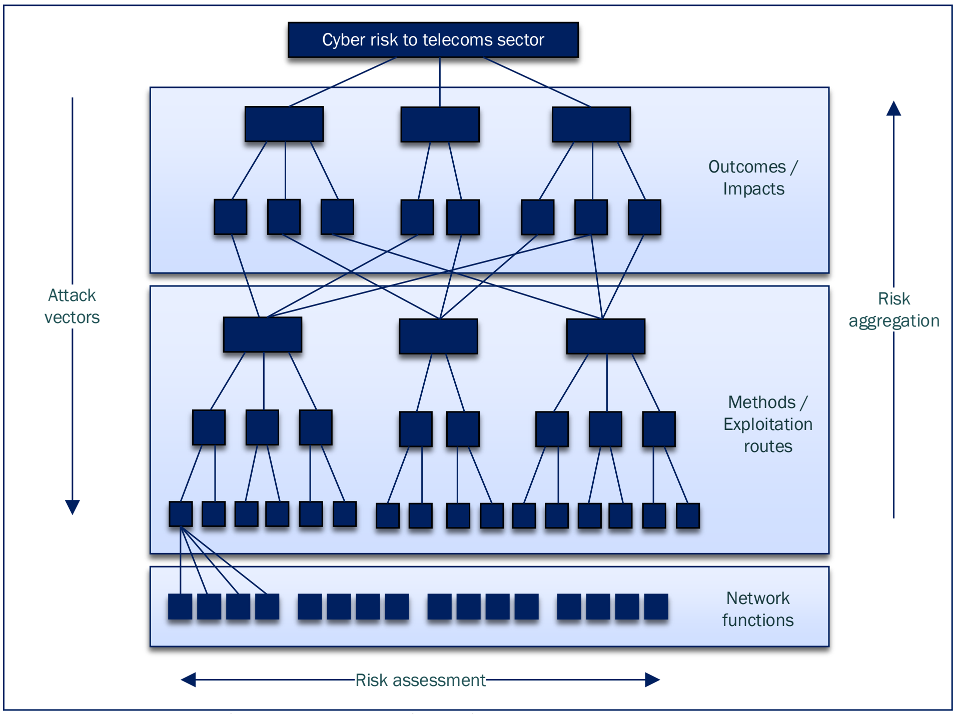

Figure 3.1-1: Using attack trees to assess cyber risk

Building attack trees allows a significant number of potential risks to be explored, creating a natural grouping of risks into 'themes' or particular areas of concern. It also enables them to be presented in a digestible way for risk owners.

Leading on from this, the risk associated with an attack is assessed based on a range of factors such as likelihood/cost/repeatability etc. By aggregating risk up the tree, the risk due to a particular area of concern can be assessed, allowing mitigations to be identified.

3.2 Impacts or Outcomes

The threats were broken down into four overarching negative outcomes:

- disruption of networks: impacting the operation of services or equipment within the UK's telecoms networks
- network espionage: the malicious acquisition, modification or use of data within the UK's telecoms networks
- network pre-positioning: attackers gaining administrative access or presence within the UK's telecoms networks to enable future exploitation
- national-scale supplier dependence: dependence on an external service for effective operation of the UK's telecoms services

Under each of these, specific outcomes can be listed and the impact, whether damage or loss of data, assessed.

Outcomes may or may not be intentional. For example, equipment may be disabled through intentional cyber attack or through the unintentional failure to renew a software licence. The outcome, in this case network outage, is the same either way.

3.3 Exploitation methods

Exploitation methods are 'how' an outcome is achieved. An exploitation method provides a means to gain access or capability within the network and may be used to achieve multiple outcomes.

The exploitation routes towards a general telecoms network are shown in Figure 3.3-1.

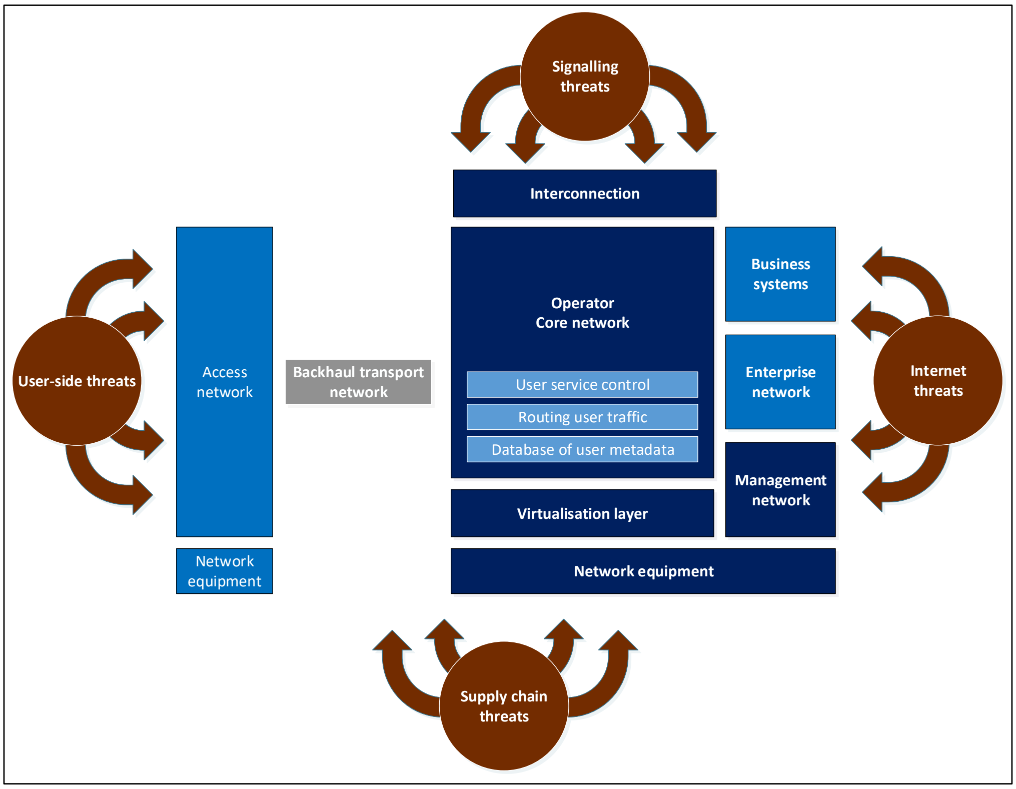

Figure 3.3-1: Attack vectors against a generalised telecoms network

Beneath these exploitation routes, the tree was expanded so that specific attack vectors were able to be explored, such as: 'Exploit equipment vulnerability over signalling plane'. This process was repeated to define a comprehensive set of attack vectors.

The first step in dealing effectively with an incident involves identifying it. That is, how can you detect that an incident has occurred (or is still happening)?

4. Threat application, impact and network sensitivity

4.1 Threat application and verification

The attack trees described in Section 3 were created as generalised attack vectors applicable towards all telecoms networks, whether they are mobile (2G, 3G, 4G or 5G) or fixed (xDSL, FTTx). Classes of attack against networks are grouped together and considered as a single kind of attack. For example, almost every type of telecoms network has its own signalling protocol. However, regardless of the specific properties of the protocol, an attacker with disruptive intent, sufficient access and the capability, could send a corrupt message into the network. Ultimately, the use of generalised attack vectors is effective; telecoms networks have been structurally consistent for at least 20 years, and this underlying structure is likely to remain.

However, such an approach can never be comprehensive. There is some variation in risk across telecoms technologies and functions, and our generalised analysis might miss significant attacks that exploit an unusual property of one network type.

To avoid this, the next stage in the process was to consider the attack trees against existing network types. Threat analysis was performed against three network types: a 4G network, a 5G network and a FTTP network. These were chosen as they are likely to be the most significant types of telecoms network over the next 10 years. Applying the attack trees in this way allowed us to refine our attack vectors and assess the risk associated with the vector.

4.2 Example: The 5G network

As an example, 5G network functions are placed onto the general model of a telecoms network (see Figure 4.2-1).

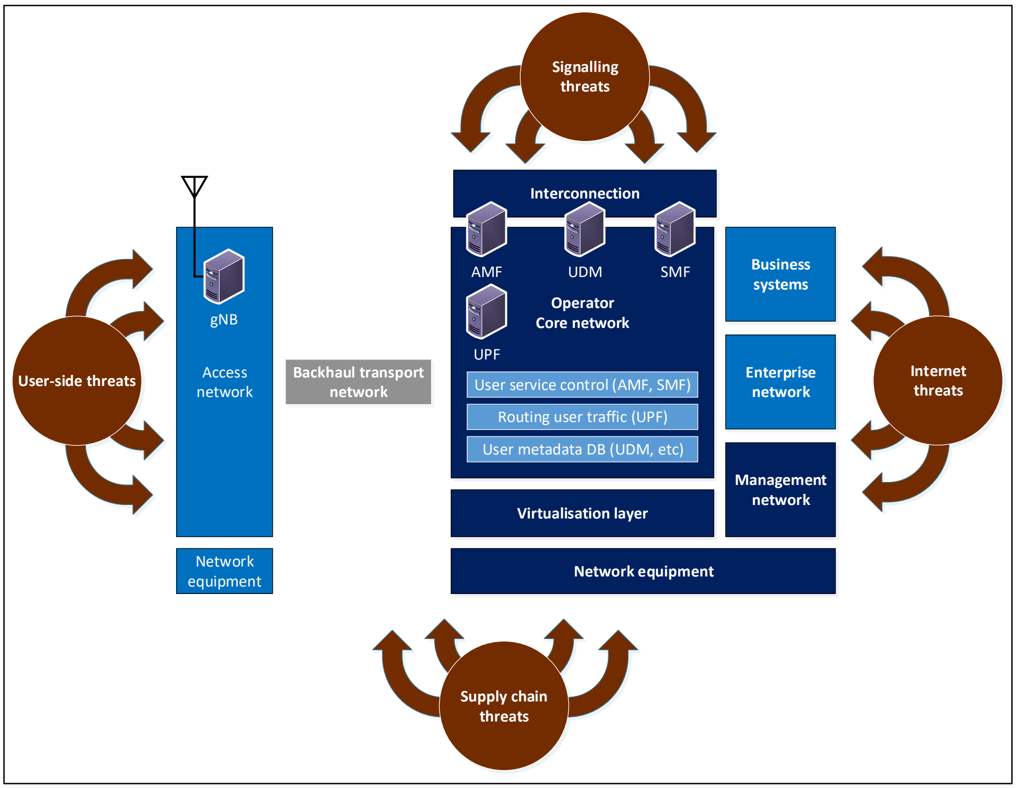

Figure 4.2-1: Attack vectors against a 5G telecoms network

Compared with a 4G network, the nationally-significant attack vectors towards a 5G network are almost identical. There are only a few differences.

- 5G networks fully split the signalling plane and user plane. Consequently, network functions processing user traffic are not addressable from the international signalling network, and this provides some additional protection.

- The 5G core network uses a service-based architecture, utilising a broader range of data and services. This approach will have an increased attack surface over signalling networks and network APIs.
- 5G networks use commonly used web protocols, so attackers and defenders will have a broader suite of existing tools at their disposal.
- 5G networks have some additional security features for air interface protection.

In addition, while virtualisation technologies are not unique or necessary for 5G networks, these networks are more likely to use virtualised infrastructure. In this case, the attack vectors and mitigations applicable to virtualised networks would also apply.

Finally, the risk due to every attack vector may increase over time, particularly for 5G networks, as the criticality of telecoms networks increases with the nation's digitalisation.

4.3 Threat impact and network function sensitivity

Scoring the risk due to an attack vector requires considering the likelihood of the vector (cost, complexity, reputational impact, repeatability), and the impact of the attack vector (damage or data loss).

While an attack vector may be general, the impact is determined by both the outcome and the capabilities of the network function that is under attack. Clearly some functions are more sensitive than others. The network impact from disrupting or exploiting a single network element in the access network, such as a base station, is clearly lower than the impact of disrupting or exploiting core equipment. The former may impact a local area, the latter could impact services across the entire country.

Hence scoring the attack vectors requires establishing the 'sensitivity' of classes of network functions and considering the worst case. 'Sensitivity' is established based upon the following three impacts:

- availability impact: the damage to the network of the equipment going offline
- integrity impact: the disruption caused by changing the data over which the equipment has control
- confidentiality impact: the cost of compromise of data within the network equipment

Table 4.3-1 shows the high-level outcome of this analysis.

Table 4.3-1: The sensitivity of network functions

	Critically sensitive	High and moderate sensitivity
Access functions		User-aware access functions. Such as: • 4G RAN (eNBs) • 5G centralised access (RAN-CU) User-independent access functions. Such as: • 5G distributed access (RAN-DU, RAN-RU) • Fixed aggregation: OLTs / MSAN / DSLAM • Fixed edge: CPEs / ONTs / ONUs
Core functions	• Virtualisation infrastructure, orchestrators and controllers • Internet gateways and monitoring functions • Core network equipment, including database functions and access control functions • IP core (routing and switching of traffic)	
Transport & transmission functions		• Backhaul transport and transmission equipment
Internet exchanges	• Equipment used for network interconnection.	
Management systems & supporting services	• OSS, management and AAA systems • Security enforcing functions or security critical functions	

The sensitivity of certain functions is highly variable and needs to be determined on a case-by-case basis, depending on operator architecture and operation models. This includes business support systems (such as billing), voice systems, logging and backup systems, and border network gateways (BNG/BRAS).

This analysis supports the scoring of attack vectors and also supports the process of determining appropriate mitigations. The more sensitive a network function, the more important that the function is protected.

4.4 Scoring

With a complete attack tree, each attack vector was assessed (scored) to categorise how damaging it might be to the operation of a telecoms network.

Each attack vector has a cost to develop, complexity to deploy, a risk of discovery and the attack may or may not be repeatable. Depending on the outcome, the attack vector will have an associated impact. Combining these factors allowed the relative risk of each attack vector to be assessed, and the risk traced back up the tree to identify the most significant areas of risk.

This information led us to define mitigations for the most significant areas of risk and the attack vectors within those areas of risk. These areas are covered in more detail below.

5. High-risk areas

5.1 Introduction

Upon completing the threat analysis, the majority of the highest scoring attack vectors fitted into one of the following five categories:

- exploitation via the operators' management plane
- exploitation via the international signalling plane
- exploitation of virtualised networks
- exploitation via the supply chain
- loss of the national capability to operate and secure our networks (dependency)

In the following subsections, these high-risk areas are described in greater depth. Within Section 5 intrinsic risks are described. These are risks that occur absent any mitigating actions by operators or governments. Recommended mitigating actions are described from Section 6 onwards.

5.2 Management plane

The management plane of a network is where administrative activity takes place. It is the most powerful part of the network infrastructure; whether used for provisioning and configuration of new equipment, or making changes to existing infrastructure or services. This also makes the management plane the primary target for any malicious attack intending to disrupt or otherwise compromise the operation of a network. Exploitation of the management plane could have a long-term impact on the availability and confidentiality of the operator's services, including critical services.

Historic management of telecoms networks has relied heavily upon standard corporate devices 'doubling up' as administrative workstations. Consequently, the laptops that perform standard 'office' type functionality such as email, web access and productivity tool use are also defining the operation of the network. This can lead to several 'commodity' classes of attack being performed with relative ease on administrative users and these can achieve a significant impact.

Attacks of this type may also not always be easily detected, as there may be no overt impact on the network. The compromise may be maintained for years, growing in scale and complexity over time.

5.3 Signalling plane

All public telecoms networks connect to each other over signalling networks. These signalling networks allow operator networks to connect to each other, reach each other's services and ultimately allow users to communicate with each other.

Traditionally, and to a degree currently, telecoms standards have been built on an assumption that all signalling from other telecoms networks can be trusted. However, that assumption is no longer valid as these international networks can be exploited by attackers to conduct attacks. Operators must today consider that any inbound signalling may be malicious and treat it appropriately.

Without the implementation of appropriate mitigations by operators, malicious inbound signalling could impact the availability of core network nodes, extract network or user metadata, or reroute user calls or data.

As an example, within the last five years a major telecoms network was accidentally remotely disabled for a number of hours due to the failure of a critical core node to process an unusual, internationally-routed signalling message. While this failure was an accident, it highlights a potential vulnerability that could be intentionally abused unless mitigated. Furthermore, signalling networks have been shown to allow the leaking of subscriber and network data, sometimes in support of criminal activity.

In many ways the situation is no different to IP data received from external sources, such as the internet. The data received by the operator could be malicious, and if it is, it could have a negative network impact. Networks need to appropriately protect themselves against receipt of malicious data to mitigate this risk.

5.4 Virtualisation plane

Virtualisation provides a method to separate workloads and is a widely used technique to utilise the resources available on a host in the most efficient and secure manner. Compromise of the virtualisation fabric could result in an impact to the network availability, or full compromise of the operator's core and all workloads running within it.

A successful 'virtual function to physical host' attack could enable an attacker to bypass the hypervisor's enforced separation, allowing the attacker to influence and control any workloads running on the impacted host. As such it is critical that security mitigations are in place to help prevent successful attacks against the hypervisor, and to prevent lateral movement between hosts to limit the impact and compromise of this type of attack.

The successful exploitation of the virtualisation's fabric, orchestration, and management functions could enable an attacker to influence and control the entire virtualisation fabric, including all hosts and virtual workloads, potentially achieving a total compromise of the network. Consequently, the orchestration and management functions must be locked down to prevent malicious access from compromised hosts.

However, while network virtualisation presents risk, it also allows advanced and flexible network protections. For this reason, a well-built virtualised network can be more secure and resilient than an equivalent network built on dedicated hardware.

5.5 Supply chain

5.5.1 Risk overview

No operator can perform all of the activities required to design, manufacture, install and run an operational telecoms network, and some are not equipped or staffed to operate all the supporting functions that the underlying business requires. Every operator therefore has a supply chain, which can involve the provision of hardware, software, and managed services.

Supply chain risk breaks down into four risk components shown in Figure 5.5.1-1:

- risks due to national dependence, supply disruption and sanction
- risks due to equipment supply (including software)
- risks due to supplier network access and support
- risks to operator data including SIM supply

These risks are directly linked, in that mitigating one risk will likely increase another. Consequently, minimising the risk to the UK requires balancing the risk across each risk component.

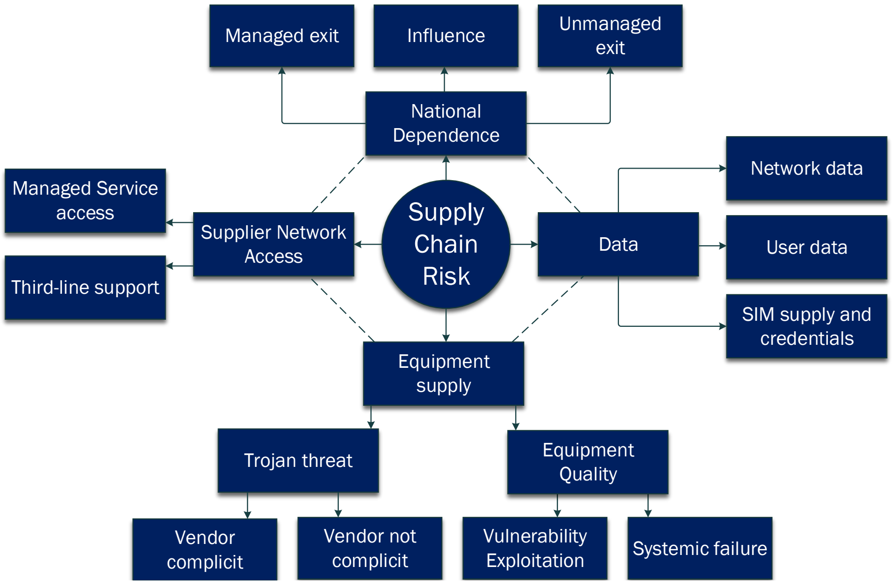

Figure 5.5.1-1: A breakdown of supply chain risk

The extent of supply chain risk depends significantly on the sensitivity of the equipment supplied or accessed. Assuming a properly managed network (for example, one which complies with the TSRs), the supplier can only directly alter the behaviour of equipment it supplies or supports. Hence the risk of supply is intimately coupled to equipment sensitivity (described in Section 4.3).

The intrinsic risks due to the supply chain are described in the following sections. These are risks that occur absent any mitigating actions by operators or governments. Recommended mitigating actions are described from Section 6 onwards.

5.5.2 National dependence

The risk of 'national dependence' is the risk that a supplier's continued supply or support is required to maintain the resilience of the UK's telecoms services. This potential dependence on a supplier arises from the operator's ongoing need to access support services from the supplier to maintain their networks. If all telecoms services in a particular region of the UK rely upon a single supplier, that would create a national dependency on access to the supplier's support services. Furthermore, without that support, UK networks would likely be disrupted over an extended period, potentially years.

Should the UK become nationally dependent on any individual supplier, this would present a significant risk to the UK. Any national dependence on a high risk vendor would present a significant national security risk.

National dependence would reduce our ability to hold the supplier to an appropriate standard of behaviour and security. Furthermore, if the supplier were caused to exit the UK market for any reason, this would have a disruptive impact on the UK. It may also create a proxy dependence on the supplier's own supply chain dependencies, including dependencies on other nation states.

It is important to avoid the situation in which the UK becomes nationally dependent on a particular supplier. Once established, a dependence will take time to correct, potentially years, assuming viable alternatives exist. As market diversity reduces, the risk of national dependence increases.

Without government intervention, the NCSC considers there to be a realistic likelihood that due to commercial factors the UK would become 'nationally dependent' on Huawei within three years.

5.5.3 Administrative access and managed services

As described in Section 5.2, administrative access presents a significant cyber risk to telecoms networks. Operators provide administrative access to Third-Party Administrators (3PAs) for a variety of reasons. Operators provide administrative access to Managed Service Providers (MSPs) as part of a managed service contract, to an operator group function (when centralising administration across the operating companies of a group), or to an equipment vendor as part of a third-line support function.

Due to their nature, 3PAs gain access to multiple telecoms networks. This means that a single set of administrators, and administrative systems can negatively impact multiple networks. 3PA access to multiple clients' networks also makes them particularly attractive to attackers. Should 3PA systems be exploited, or a 3PA administrator be malicious, multiple UK networks could be exploited or disrupted simultaneously.

As an example, on 20 December 2018, HMG attributed a cyber attack targeting several global managed service providers (MSPs) to China-linked group APT10. Through compromise of these MSPs, APT10 had managed to exploit multiple customers of those MSPs and exfiltrate a high volume of data. The overall scale of the compromise was unprecedented, and had gone undetected since at least 2016. Using an MSP in this way, as a platform to attack multiple further targets, demonstrates why this risk is of concern.

While both managed service access and third-line support can present a risk to UK networks, the risk due to managed service access is particularly significant due to increased scope and frequency of network access, and increased scope and frequency of data access. The use of 3PAs by UK networks almost certainly increases the overall threat of cyber attack, requiring careful risk management by industry.

The use of 3PAs also creates a risk due to the dependence of the operator on the 3PA for the continued operation of networks. Should the 3PA be no longer able to provide the service, this is likely to have a service impact.

5.5.4 Supply risk due to product quality and security

There are two primary risks due to equipment quality and security:

- systemic failure due to software or firmware fault
- equipment vulnerability exploited by an attacker

If there are product quality issues, be it from legacy build environments, poor software development processes or poor vulnerability management, a flaw in one or more products could potentially result in widespread equipment failure or be turned into an exploitable vulnerability by an attacker, allowing the attacker to gain control of network equipment.

From our work with telecoms vendors, we believe that the security maturity of products in this sector lags behind industry good practice, driven by market drivers that disincentivise security improvement. While there are some vendors who are better at security than others, this is true of all vendors and a variety of measures to drive and enforce better standards are needed across the sector to sustainably remediate the problem. This is particularly true when compared to the security approaches of commodity end user devices and mature public cloud offerings. The move to virtualised infrastructure in telecoms will provide opportunities to leverage these enhanced security approaches within the telecoms sector.

The 2018 and 2019 HCSEC Oversight Board reports highlighted serious quality and security issues with Huawei's engineering. While the NCSC does not believe that the issues are due to malicious intent, they increase the risk to the UK regardless, and require mitigation through the recommendations described in this document.

As with the other supply chain risks, the risk to the UK is determined by the type and quantity of equipment supplied. Equipment that is less exposed to attack, and that plays a less critical role in the UK, causes a lower impact and hence presents a lower risk due to equipment quality and security issues.

5.5.5 Supply risks due to equipment trojans

This threat covers malicious functionality added to equipment either intentionally by the vendor or covertly by a hostile actor who has access to the vendor's hardware design or manufacture, software development systems, or to the equipment in transit.

The benefit for an attacker of compromising a telecoms vendor is high given the data that could be gained from such embedded accesses or the disruption that could be caused by an embedded access. Due to the significant lack of vendor diversity available to telecoms providers, the return on investment from a hostile actor embedding malign functionality into a product would be significant as the product is guaranteed to be deployed into many operators across the world.

However, embedding trojan functionality remains a costly and complex attack. Any covert changes require a deep understanding of the equipment and the undetected modification of code or build chains. Any intentional malicious change is performed while shouldering significant business and reputational risks should it be discovered.

5.5.6 Data risk due to network and user data

As part of an operator's interactions with suppliers, it may be necessary to share user or network data, or the supplier may come into contact with this data incidentally. As a consequence, without proper controls, this data could be more vulnerable to compromise by a threat actor, either due to the insider threat within the supplier, or due to a network compromise of the supplier's systems.

5.5.7 Data risk due to supply of user access credentials

User access credentials, such as SIM cards provide users with access to the network. A UICC (Universal Integrated Circuit Card) contains credentials of the SIM/USIM (Subscriber Identity Module), which is used to authenticate subscribers' access to the telecoms network. Historically these were for mobile devices but are increasingly being used for fixed access as well. Increasingly UICCs are being embedded in mobile and IoT devices (eUICC or eSIM), meaning that card replacement will not be feasible. In the case of IoT devices with removable UICC, the cost of physically accessing the device to change the SIM card would not be financially viable at scale.

Should a SIM fail to allow access to the network, the subscriber or device will be unable to gain connectivity beyond the default emergency service access. In this case the device could be anything from a light switch to a 'lift-cable monitor', to a mobile phone. In some cases, without connectivity, the device will become inoperable. Consequently, at-scale disruption of SIM cards or SIM card infrastructure is a national security concern.

Disrupting traditional SIM cards requires access to credentials held by the UICC supplier and network operator. Hence the protection of these credentials is essential, as is the careful choice of UICC supplier.

Similarly, there is a risk that the recently-defined eSIM functionality could be misused to perform disruption at scale. As eSIM gains traction in the industry, mitigations need to be implemented to prevent corruption of the credential, inhibiting access to the network, or an unauthorised service transfer.

5.6 National dependency for design and operation of telecoms services

The trend in the telecoms industry is increasingly to outsource and/or centralise functions, into international locations. This approach may be applied to business decisions, technical decisions, management processes and security processes. Business decisions, such as procurement decisions, are increasingly taken within an operator group HQ.

The most significant risks due to this trend are that business decisions may be taken without an understanding of the local threat environment and without full consideration of the local context or local risks.

One business decision is to operate UK networks from outside the UK. Networks are increasingly designed, operated, maintained and secured from lower cost international 'hub' locations. This presents network availability concerns should there be an international connectivity issue, and increases the complexity of securing the network.

Mitigating this risk does not mean that network operations cannot be globally distributed provided appropriate protections are in place, but sufficient knowledge, capability and data should reside locally to ensure the security and resilience of the network.

6. Mitigating telecoms risk

Based on risk analysis described in this paper, the NCSC set out to define the technical recommendations and mitigations that could reduce the identified risks and support the creation of a robust new security framework for the UK telecoms sector.

These recommendations and mitigations fall into five categories:

- Technical Security Requirements (TSRs) detailing how the NCSC recommends that operators reduce their cyber risk in the highest risk areas (Section 7)
- recommendations on the management of High Risk Vendors (Section 8)
- diversification of the infrastructure market
- the establishment of a National Telecoms Lab to perform a broad range of testing of the UK's telecoms networks and equipment (Section 10)
- continued regular and detailed threat-driven security testing of operator's networks as performed under Ofcom's TBEST scheme (Section 11)

The following sections describe the NCSC's technical security recommendations and mitigations.

7. Telecoms Security Requirements

7.1 Overview

7.1.1 Background

The DCMS Supply Chain Review [6] recommended the establishment of a new, robust security framework for the UK telecoms sector, with new TSRs at its heart.

No system can be 100% secure or available. The intent of the TSRs is to set realistic standards for the protection of our national telecoms networks and to clarify the security offer from operators to their stakeholders, whether they be users, government, the regulator or other operators. Through practical controls, we want to make it hard for an attacker to compromise a UK network, make it likely that any such compromise will be noticed quickly and the harm and impact limited, and make remediation as simple as possible. These are commercial networks, and security of those networks has to be judged in the context of commercial realities. This is all independent of any given threat actor; our aim is to protect equally from them all.

Consequently, the TSRs define an achievable baseline of security controls to protect operator networks from realistic and nationally significant cyber attacks. The TSRs are presented within a broader framework that describes the risk that motivates the requirement, and guidance on the implementation and testing of the requirement.

The TSRs have been built around mitigating the five main areas of significant risk:

- management plane
- signalling plane
- virtualisation plane
- supply chain
- loss of national capability to operate UK networks

The requirements aim to provide a consistent, measurable, and achievable list of security controls and procedures that will help improve the security of all UK telecoms networks when applied together.

The TSRs set out all recommended security controls, even the most basic. Security controls are not consistent across the industry and including even the most basic controls in the TSRs ensures an essential control is not missed. Adopting the TSRs will improve the security of the UK’s national telecommunication sector, building confidence in the security and resilience of our telecoms services.

7.1.2 Components of the security framework

Within the TSRs, each risk area is broken down into the following components:

- Summary of risk: why the framework focuses on this area.
- Security principles: the security intents that the framework seeks to achieve to mitigate the area of risk. They are intended to be high-level long-lasting aims.
- Security Requirements – the heart of the framework, and the baseline security elements for telecoms networks in the UK.
- Security Tests: the type of test that should be performed to evaluate compliance against the TSRs. The test descriptions are high-level and should be supported by detailed test plans.
- Implementation Guidance: provides a best-practice example of how the TSRs could be implemented and elaborates further on the intent of the TSRs.

7.1.3 Evolution of the framework

Cyber risks continue to change and evolve, and so cyber defence cannot be static. It is intended that the framework will be subject to regular periodic review to both evaluate the framework’s success and enhance the framework. The framework will likely also need to evolve, to reflect advancing best practice, and to respond to new attack vectors and new technologies.

7.2 Management plane

The primary intent of the TSRs relating to the management plane is to segregate critical management functionality from networks with direct access to the internet. Additionally, they contain principles to ensure that management is performed securely, e.g., by using well secured protocols and tightly controlling the network traffic permitted between management endpoints and equipment.

The TSRs propose a Privileged Access Workstation (PAW) model [3]. This enables a set of workstations to be "known good" within the same level of trust as the equipment being managed, and as such able to perform management activities without introducing significant risk. This model also enables 'tiering' of access, such that more critical services can be subject to tighter access control.

Due to this segregation from other business functionality, the supporting information also details methods by which access can be gained in a safe way so as to minimise inconvenience for administrative staff, alongside more robust data transfer procedures.

7.3 Signalling plane

The intent of the TSRs with respect to signalling networks is to increase the network's resilience to disruptive attacks from external signalling networks, and to inhibit the leaking of subscriber or network data over external signalling networks.

7.4 Virtualisation plane

The TSR mitigations for virtualisation are broken down into multiple areas.

The hardware requirements detail the mitigations CPU manufacturers have implemented to better protect and separate virtualised workloads. These mitigations cover both CPU and UEFI security considerations.

The software requirements detail the mitigations that the hypervisor operating system and software should implement. These mitigations focus on helping prevent known exploitation vectors from being available.

The architectural requirements detail the mitigations that the operator should follow to securely architect their virtualised infrastructure. These mitigations focus on highlighting best practice architectural patterns around micro segmentation, secure administration, and patching.

Combining these mitigations with a secure management plane (as defined in Section 2) will help an operator build and maintain a secure virtualisation fabric to support their network functions.

7.5 Supply chain

7.5.1 Overview

The intent of the TSRs in this section are to mitigate the following supply chain risks:

- risks due to equipment quality and security issues
- risks due to supplier network access and support
- risks to operator data, including SIM supply

The remaining risks identified in Section 5.5 are:

- national dependence and supply disruption
- equipment trojans

These risks are particularly exacerbated in the case of a high risk vendors, and as such the TSRs do not provide the primary mitigation. The mitigations for these are addressed in Section 8 of this analysis.

7.5.2 Supply chain governance

The TSRs recognise that large elements of the supply chain are outside the direct control of the operator, and thus operators should seek to impose obligations onto the supply chain to enhance security.

In the first instance, operators should understand and manage their supply chain risks. Operators place security requirements onto suppliers, ensuring the supplier imposes suitable conditions on their supply chain. Through this means, obligations are created across the supply chain to protect data, to support incident management and to support security testing. Operators are encouraged to avoid placing the same level of trust and reliance on third-party staff as they do on their own employees, with whom they have a direct employment relationship.

The TSRs stress that operators should take full responsibility for the management of cyber risk related to their networks and should not assume that the supplier will do so on their behalf.

7.5.3 Administration and management of 3PAs

The TSRs state that administrative access from third parties (e.g. MSPs or vendors) should be subject to the same security controls as those in operation at an operator itself (as described in Section 7.2). The principle is that MSPs should appropriately segregate the systems used to access operator networks, ensuring that compromise of the MSP does not compromise multiple operators.

Furthermore, to inhibit the impact that a 3PA could have on the operator's network the operator should aggressively limit access into their network, both in terms of scope and time. In some cases, real-time oversight of the 3PA's network access may be necessary. To support security investigations, the operator should have access to appropriate logs and audit data from the 3PA.

7.5.4 Equipment quality and security

Currently, there is little publicly-available information on the build quality and security of network equipment. Consequently, every operator must make an assessment on the security risk due to vendor equipment based on limited resource and limited evidence.

To increase security transparency in the market, the TSRs expect operators to require vendors to publish detailed security white papers, increasing transparency about the vendors' security practices and allowing operators and security researchers to collaborate on the testing of the vendors' claims.

To support this process, the NCSC has provided detailed guidance on the information that operators should request from vendors to allow security assessments to be conducted, and the tests that can be performed to verify these assessments.

The TSRs also expect operators to cost-in security risk into their procurement activities, and ensure that good security practice is rewarded.

7.5.5 Protection and sharing of data

The TSRs require that the operator retains control of their network and user data wherever this is technically possible. The TSRs expect every data item to have a data owner, who gives explicit permission for access to the data. If data needs to be transferred from the operator to a third party, it should be verified as being held as securely by the third-party, to the same standard as the operator. The TSRs also expect that when technically possible, data accessed by a third party is anonymised and obfuscated.

7.5.6 Protection of User Access Credential data

The intent of the TSRs with respect to user access credentials, such as SIMs, is to ensure that threat actors cannot access the necessary information needed to disrupt the credential at scale. The TSRs ensure that this information is only held within the operator, and that the operator appropriately protects it.

7.6 Retaining national resilience and capability

The intent of the TSRs is to ensure that there is always the ability to operate and control UK networks within the UK, and that decision making relating to UK networks involves UK oversight. The TSRs aim to ensure UK networks remain available, particularly in the event of any impact to international connectivity, as well as limiting the ability for malicious insiders, based outside the UK, from damaging UK networks.

7.7 Supporting functions

7.7.1 Security and audit

While not directly a set of preventative controls, security monitoring underpins the security posture of a network or system. Enabling the collection of relevant information from the right devices or systems within an operator environment will allow threat actors to be detected, and post-event analysis to be undertaken. Ultimately, this will allow operators to gain more confidence in their ability to find and respond to security-related events.

The TSRs also aim to ensure that operators take a proactive approach to monitoring for threats, including use of threat hunting where appropriate.

7.7.2 Business functions

Having an effective security governance framework ensures that procedural, personnel, physical and technical controls continue to work through the lifetime of a network, backed by an appropriate security culture. Without effective governance, it is likely that security improvements will not be sustained or consistent.

In this area the TSRs reference the NCSC’s Cyber Assessment Framework (CAF) [4] which comprehensively describes how security governance should be implemented.

7.7.3 Security critical functions

Operators use security critical functions to enforce security controls in their networks and mitigate risk. As risks are mitigated, the options available to attackers are reduced, and the security critical functions become the primary focus of attack.

The TSRs define additional controls for security critical functions to help ensure that they are resilient to targeted attacks from determined attackers.

8. Mitigating risks due to High Risk Vendors (HRVs)

8.1 Overview

The Telecoms Security Requirements (TSRs) are designed to mitigate universal attack vectors, independent of any vendor-specific risks. Full application of the TSRs will significantly improve the security of operator networks, but will not fully mitigate the risks due to vendors that pose a higher security risk to UK networks ("High Risk Vendors" or "HRVs"). Securing UK networks also requires HRV risk to be mitigated as described in this section.

Historically, the involvement of HRVs has been managed on an advisory basis by the NCSC, through advice provided to operators. The NCSC has now published non-binding technical advice to operators in respect of their use of equipment from HRVs, [2], and government has signalled its intention to put these onto a more robust footing.

Our recommendations to limit the risk due to High Risk Vendors are that:

- operators perform effective implementation of the TSRs described in Section 7, including applying appropriate controls to manage their suppliers
- the market share of HRVs is capped to limit the UK's national dependency (Section 8.2)
- HRVs are excluded from the sensitive parts of telecoms networks, from the most sensitive locations and from sensitive networks to protect network availability and confidentiality (Section 8.3)
- the HRV should only be used if a bespoke mitigation strategy has been agreed between the HRV and the NCSC (Section 8.4)

The following sections explain why we have recommended these measures.

8.2 Limiting dependency

As set out in Section 5.5.2, significant risks could arise if the UK were to become nationally dependent on any vendor. Should the UK become nationally dependent on a high risk vendor, then the national security risk becomes unacceptable.

The NCSC's recommendation is therefore that the market share of high-risk vendors should be limited at a level that does not permit national dependence. The NCSC's advice is that where an HRV is permitted to supply equipment, the market share as defined in the advice should be no more than 35%. This cap ensures that national dependence does not occur due to the scale of HRV deployments and ensures that removal of the vendor's equipment from UK networks remains feasible, should that become necessary.

For the NCSC's full HRV advice, see [2].

8.3 Maintaining availability and confidentiality

8.3.1 Exclusion from the core

A telecoms network is split into 'core' networks and 'access' or 'edge' networks. The role of the 'access' network is to manage the user's local access into the network and route their data traffic towards the 'core'. The 'core' acts as a hub both for all the data traffic, and all the user metadata needed to give a user service. Ultimately, the 'core' ensures your data goes to the right place.

'Core' functions provide user services nationwide and consequently, the availability of the core is paramount. Furthermore, there is extensive data within the core which needs to be kept confidential. As a result, the core network is significantly more sensitive than the access network.

For this reason, the NCSC recommends that no products or services from HRVs should be used in 'core' functions, in line with our long-standing advice. For the NCSC's full HRV advice, see [2]. This reduces the potential impact that HRVs could have on the availability or confidentiality of UK networks.

In 5G networks, core functions can be relocated nearer the 'edge' of the network. This has been described as blurring the line between core and edge. This is technically inaccurate as the 'core' is defined by a set of functions, standardised within [5], rather than a location. Consequently, the distinction between the two remains clear, as does the advice above. Our advice remains that HRVs are excluded from performing core functions, and this applies whether these functions are deployed centrally or towards the 'edge'. Our understanding is that this clarification is unlikely to be consequential in the UK, as we are informed that core functions may run near the edge, but not actually on edge access equipment (such as base stations).

8.3.2 Exclusion from sensitive locations

Access equipment, such as base stations, are able to generate anonymised metadata to support network diagnostics. For most of the network, this metadata is not particularly sensitive. However, in certain locations, the sensitivity of the metadata could be high enough to be a national security concern. For this reason, operators should not use any equipment from HRVs near sites that are significant to national security, removing the risk that the local supply of equipment by the HRV might allow access to this data.

8.3.3 Exclusion from sensitive networks

Sensitive networks either route or have access to sensitive information, and include those directly relating to the operation of government or any safety-related systems in wider critical national infrastructure. To fully protect and ensure the availability of these networks, the NCSC recommends that HRVs are excluded from providing equipment into these networks, in line with our long-standing advice.

8.4 Vendor-specific solutions

8.4.1 Overview

Alongside the NCSC's general HRV controls defined in Sections 8.2 and 8.3, the NCSC has also advised that equipment from HRVs should only be used when the NCSC has agreed a bespoke mitigation strategy with the HRV in question.

8.4.2 Huawei oversight and the Huawei Cyber Security Evaluation Centre (HCSEC)

The only bespoke mitigation strategy that the NCSC has agreed to date is with Huawei. Huawei has always been considered higher risk by the UK government for the reasons set out in our HRV advice and as such a risk mitigation strategy has been in place since Huawei first began to supply UK operators.

Since 2010, a set of arrangements have existed between Huawei and Her Majesty's Government (HMG) to mitigate any perceived risks arising from the involvement of Huawei in parts of the United Kingdom's (UK) critical national infrastructure. A fundamental component of these arrangements is the existence and effective operation of HCSEC.

HCSEC is a facility in Banbury, Oxfordshire, belonging to Huawei UK. HCSEC provides security evaluation for a range of products used in the UK telecoms market. Through HCSEC, the government is provided with insight into Huawei's UK strategies and product ranges.

HCSEC is overseen by the Huawei Oversight Board. The Oversight Board's primary purpose is to oversee and ensure the independence, competence and therefore overall effectiveness of HCSEC.

The existence of HCSEC provides the NCSC and HMG with clear and unbiased evidence on the risks posed to the UK through the use of Huawei's products by UK operators. It ensures that it is feasible that embedded malicious functionality could be detected should it exist. HCSEC deploys a range of tools and AI to scan Huawei's UK products, complemented by skilled analysts.

Due to the UK's mitigation strategy, which includes HCSEC as an essential component, our assessment is that the risk of trojan functionality in Huawei equipment remains manageable. Placing 'backdoors' in any Huawei equipment supplied into the UK is not the lowest risk, easiest to perform or most effective means for the Chinese state to perform a major cyber attack on UK telecoms networks today.

8.4.3 ZTE

ZTE is also considered a High Risk Vendor. The NCSC assesses that the national security risks arising from the use of ZTE equipment or services within the context of the existing UK telecoms infrastructure cannot be mitigated. The NCSC's advice to operators in relation to ZTE has not changed as a result of this analysis.

9. Market diversification

The government has acknowledged the importance of improving diversity in the supply of telecoms equipment to the UK [6]. The current situation, whereby the UK is able to choose from only three major companies to supply key parts of our infrastructure, has significant implications for security and resilience, increasing the likelihood of national dependence and the impact of a systemic equipment fault. The market failure that has allowed this situation to come about needs to be addressed.

Led by DCMS, but supported by the NCSC, the government is developing an ambitious strategy to help diversify the supply chain. This includes encouraging established vendors not currently active in the UK to operate here, supporting the emergence of new entrants, and promoting the adoption of open, interoperable standards that will reduce barriers to entry. Further details can be found in the supporting blog [1].

10. National Telecoms Lab

Telecoms networks will be among the UK's most critical infrastructure. However, how they operate remains opaque to those outside the industry, including security researchers, academia and the citizen. For this reason, it is essential that the UK's business and research community can get 'hands on' with the networks, to test the networks' security, robustness and performance under various conditions and to encourage research and development. The burden of supporting this interest, research and investigation cannot reasonably be placed on the operators themselves; their lab environments are primarily dedicated to enhancing the performance of their own networks.

Hence, as raised in the DCMS Supply Chain Review [6], the NCSC recommends building a 'National Telecoms Lab'; a single location housing representative, operational examples of each of the UK's critical next-generation telecoms networks. The lab will be a bookable, accessible research facility, allowing teams from academia, SMEs, critical industries and government to research, test and learn about security on the UK's telecoms networks. The lab will also be a secure facility, protecting the UK operator’s IP and network information, as well as any vulnerabilities found by researchers.

DCMS and the NCSC are working together to assess the feasibility of this recommendation, including costs and implementation options.

11. Network security testing and TBEST

Network security testing of live telecoms networks is essential to establishing the true cyber risk to telecoms networks. The NCSC recommends that operators establish a sustained programme of network security testing, supported by the NCSC’s TSRs and Ofcom’s TBEST scheme.

Today, some operators conduct some form of security testing against their own networks and systems, either using internal resources, or by employing independent external contractors.

In recent years, Ofcom’s TBEST scheme has been established supported by the NCSC. TBEST provides controlled, bespoke and intelligence-led security testing of telecoms networks to improve resilience against cyber-attacks. The TBEST testing mimics the behaviour of threat actors assessed by government and commercial intelligence providers as posing a threat. This could be at a nation state level, or from a well-resourced criminal or single interest group. TBEST focuses on sophisticated and persistent attacks on critical systems and essential services, across a range of scenarios, with priority given to the systems identified as systematically important.

TBEST is currently voluntary; the operators allow a commercial penetration testing team to ‘attack’ their network, using agreed attack scenarios. Attackers are given specific conditions when they must stop their attack to minimize the possibility of inadvertent service impact. Whilst senior management of the operator are aware of the activities being conducted, the majority of the operator’s employees are not.

By simulating the activities of a highly skilled and motivated attacker, the penetration testers are able to expose weaknesses in the operator's systems which could have serious consequences or indicate non-compliance with corporate policies. By being aware of and addressing such issues the operator is in a much stronger position to protect their network.

12. Conclusion

Our threat analysis highlights that our telecoms sector is potentially vulnerable to a range of cyber risks. This analysis is backed up by evidence generated from security testing of telecoms networks and by security incidents. In this paper, we have outlined the NCSC's approach to assessing the cyber risk to the telecoms sector, and our recommendations for reducing and managing this risk. While the risks are complex and interlinked, the NCSC has identified that it is feasible to manage these risks and by doing so, increase confidence in the telecoms services on which the nation relies.

It will naturally take time for the standard summarised in this document to be reached across the sector. However, the NCSC has now defined the direction of travel for the industry and, alongside, DCMS and Ofcom, is working with the operators to ensure that the sector reaches this level as soon as is feasible.

References

[1] The Future of Telecoms in the UK, NCSC Blog, Dr Ian Levy, Jan 2020, https://www.ncsc.gov.uk/blog-post/the-future-of-telecoms-in-the-uk

[2] NCSC advice on the use of equipment from high risk vendors in UK telecoms networks, NCSC, Jan 2020, https://www.ncsc.gov.uk/guidance/ncsc-advice-on-the-use-of-equipment-from-high-risk-vendors-in-uk-telecoms-networks

[3] Securing privileged access, Microsoft, Feb 2019, https://docs.microsoft.com/en-gb/windows-server/identity/securing-privileged-access/securing-privileged-access?redirectedfrom=MSDN

[4] NCSC CAF guidance, https://www.ncsc.gov.uk/collection/caf

[5] 3GPP TS 23.501, System architecture for the 5G System (5GS), Dec 2019

[6] UK Telecoms Supply Chain review report, DCMS, July 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819469/CCS001_CCS0719559014-001_Telecoms_Security_and_Resilience_Accessible.pdf

.

National Cyber Security Centre
a part of GCHQ

Security analysis for the UK telecoms sector

Summary of findings

January 2020