Mobile Telecommunications Security Threat Landscape

January 2020

Contents

Executive Summary

Welcome to the GSMA 2nd Annual Threat Landscape Report

As we enter the era of intelligent connectivity we are seeing ever more complex networks, both in the services they offer, in the use cases they will enable, and the range of technology used to build them.

Not only will such networks be critical to economic and societal health they will also be attractive to attackers and it is important that the industry is motivated to identify and mitigate the threats.

The ‘threat surface’ is increasing and with the continued presence of 3G and 4G networks in the ecosystem, traditional threats and vulnerabilities will have to be continually mitigated and managed.

Many threats are able to be anticipated and with good hygiene, continued action and vigilance, mitigated. New mitigation opportunities are arising through automation, machine learning and artificial intelligence, however these must be married to good procedural practices and appropriately skilled security staff, coupled with good strategic risk management practices.

Threats must be managed across people, process and technology and across the full lifecycle from definition through deployment, operation and ultimately decommissioning. The supply chain continues to be a critical consideration in the threat landscape.

This guide gives insights into the threat landscape of the mobile telecommunications ecosystem, details key dimensions of consideration, and offers guidance to mitigate and tackle such threats.

Introduction

The mobile telecommunications industry is under daily attack. The industry understands that no threat can be tackled in isolation, and that threat actors will continue to exploit vulnerabilities in deployed technologies to achieve their goal. In the face of this persistent threat it is crucial to develop a broad understanding of evolving threats facing the industry.

Our aim is to advise on the current threats and highlight potential future threats affecting the mobile telecommunications industry.

THE GSMA'S DESIRE IS TO ENHANCE AWARENESS AND ENCOURAGE APPROPRIATE RESPONSES TO SECURITY THREATS.

The GSMA believes security threats have been on the rise and will continue rising with the adoption of new technologies and services within an expanding ecosystem. Security must move with the threat and enable technology adoption if it is to outmanoeuvre those working against the industry.

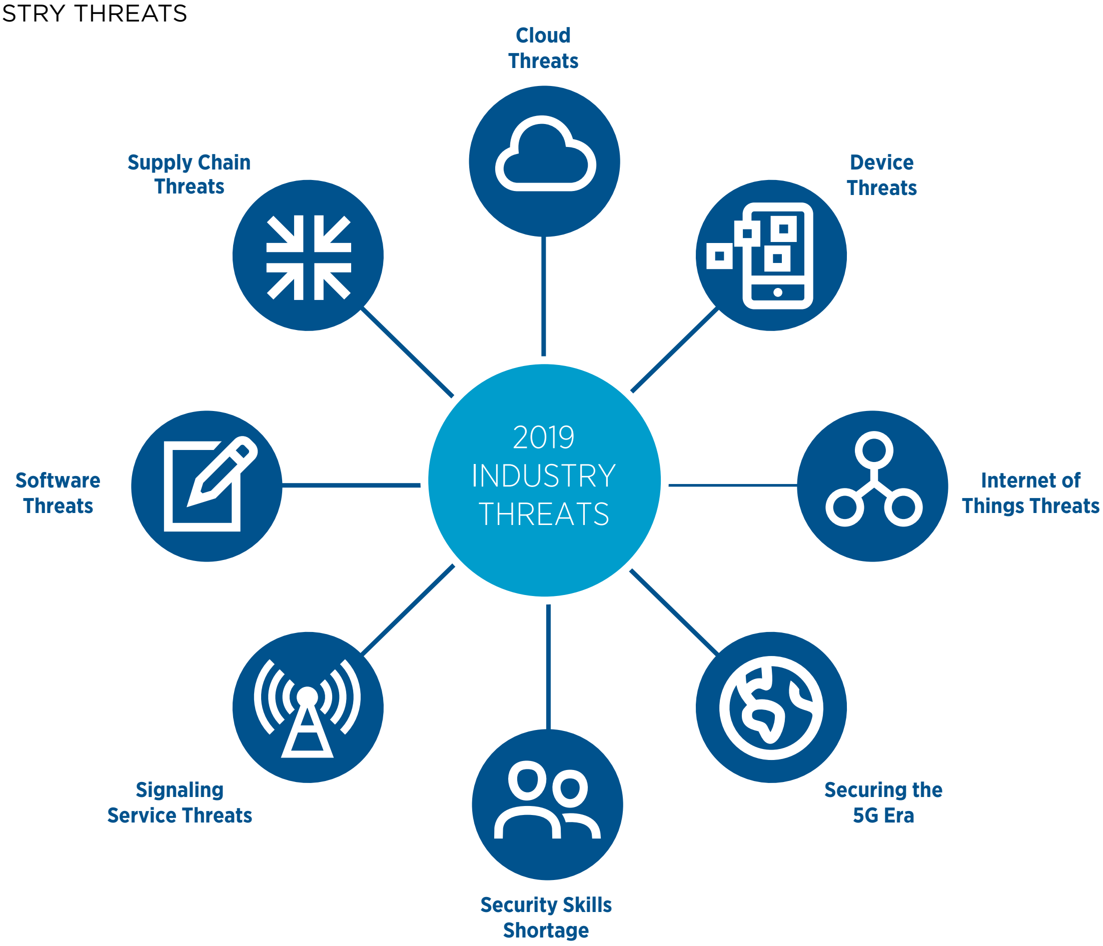
One overarching, ongoing challenge the industry faces is the lifespan of the technology they support. 2G and 3G networks still account for 50% of network traffic. The technologies these networks rely on have been in place since the 1990s and will remain for many years before closure. The protocols and systems in use in these generations were never designed for the world they are being used in today. Compensating controls, and retrospectively building security post initial deployment, is cumbersome and as such the mobile industry has to implement several add-on security technologies and requirements.

However, as the industry evolves, known threats become more defined and progress to defend against them is being made.

> **Next generation mobile will deliver feature rich intelligent connectivity and we must ensure it remains secure and resilient.**
>
> **Jon France,** Head of Industry Security , GSMA

FIGURE 1

2019 INDUSTRY THREATS



Threat Landscape Structure

This second version of the GSMA Security Threat Landscape report aims to provide understanding of mobile telecommunications threats at a high level. Each chapter in this report represents a single threat domain. All chapters that appeared in the 2019 report have been updated to reflect the current threats facing the industry. As the threat landscape has evolved, several threats seen in the past have been relegated to a lower status and been replaced with new threats (figure 1).

This does not mean that legacy threats have disappeared. They still need to be addressed. As a result this report builds on the 2019 Security Threat Landscape to present an updated view of the evolving threat landscape.[1]

For each threat the GSMA aims to outline the nature of the threat to the industry, offer insight and propose recommendations and actions the industry could implement. Each chapter is structured as follows:

THE GSMA'S OVERARCHING VIEW OF THE THREAT	FURTHER INSIGHTS INTO THE THREAT	RECOMMENDATIONS PROPOSED BY THE GSMA

[1] https://www.gsma.com/security/resources/mobile-telecommunications-security-threat-landscape/

Cloud and Virtualisation

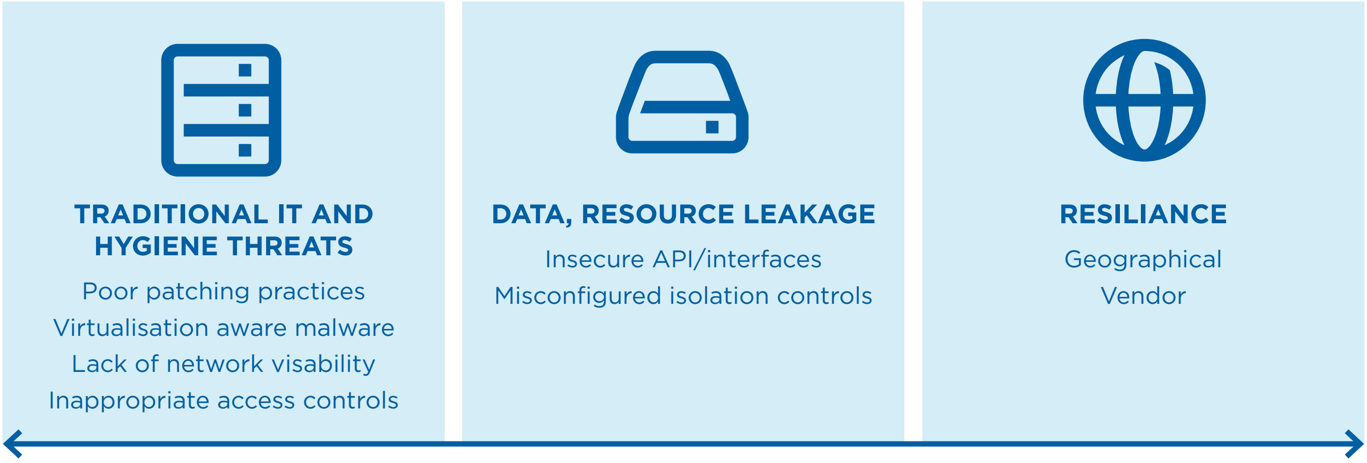
Cloud services usage is on the rise year on year. This includes IT and telecommunications alike, albeit telecommunications services currently prefer private cloud.[2] Any potential economies of scale, offered through virtualisation and cloud services, will only be realised if the security controls remain consistent when implemented.

Virtualisation, and as such cloud threats, are well understood (figure 2). Protecting against these threats requires a combination of traditional IT hygiene controls and recognition of the structural and supply chain changes affecting the network, especially in relation to visibility (data, asset etc.).

Cloud services rely on virtualisation, where it can offer granular security controls and policies if designed and implemented correctly. Once designed, the template-driven aspects of virtualisation allow automated deployment of systems that are secure by default, an aspiration of current and future networks. A combination of poor implementation and a lack of the correct skills within the industry can result in these controls being misconfigured or configured inconsistently, meaning a missed opportunity to protect the network; conversely, the misconfiguration can also result in a number of threats (figure 2) being realised.[3]

FIGURE 2

CLOUD AND VIRTUALISATION THREATS



TRADITIONAL IT AND HYGIENE THREATS

Poor patching practices
Virtualisation aware malware
Lack of network visability
Inappropriate access controls

DATA, RESOURCE LEAKAGE

Insecure API/interfaces
Misconfigured isolation controls

RESILIANCE

Geographical
Vendor

[2] A private cloud is a particular model of cloud computing that involves a distinct and secure cloud based environment in which only the specified client can operate.

[3] https://www.cisomag.com/elasticsearch-server-exposed-1-2-billion-people-data/

Cloud services and internal virtualisation mechanisms benefit from similar controls, these include:

- Local policy covering all cloud delivery and deployment models. Specific controls may relate to provisioning, service implementation, vendor choice, data management and destruction, and threat detection services
- Use microsegments to isolate high security or legacy areas; use virtualisation-aware security tooling to enforce policy and monitor these segments
- Isolate services, memory, tenants and processes effectively. Only house like-for-like security levels on the same hypervisor
- Use modem hardware that supports appropriate security controls and that these are enabled and supported within the virtualisation layer
- Purchase security controls that are virtualisation-aware and are able to protect microsegments and virtual services. Adopt the same approach for cloud services
- Develop consistent management and orchestration (MANO) services that include security controls at build phase (secure by design)
- Design and implement resilience through redundancy and use of multiple availability zones.
- Subject virtualised systems to the same IT hygiene best practice as physical systems. This includes patch management, vulnerability management, hardening practices, authentication, access controls etc.
- Cover in-life threat modelling as part of the ongoing risk management process. Develop a threat model for each deployment model and consider hypervisor-based attacks, VM-based attacks, and VM image attacks
- If outsourcing, ensure that the above expectations are passed on to the vendor via the request for information (RFI) / invitation to tender (ITT) process
- Check that suppliers hold appropriate compliance to industry-standard certifications to assure that it is following industry best practice and regulations[4]
- Develop and retain appropriate skillsets amongst staff to manage cloud deployments, specifically cloud-based security skills[5]

[4] https://cloudsecurityalliance.org/star/

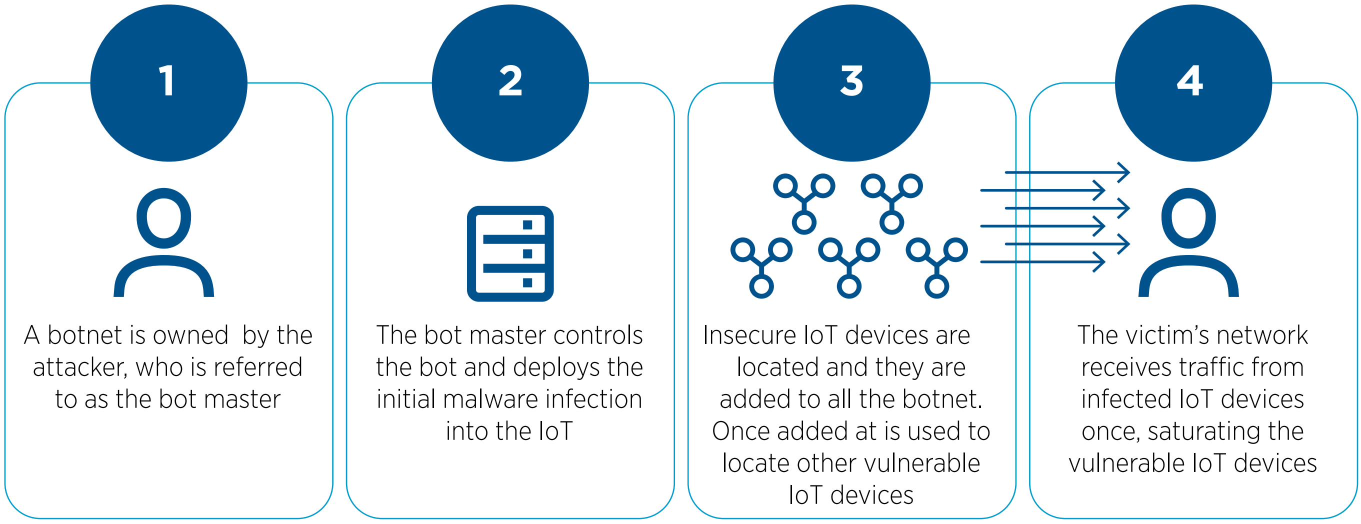
[5] The Cybersecurity Insiders Cloud Security Report 2019 highlights that 26% of people cite that a lack of skills impacts their ability to secure cloud services; 41% say that a lack of training and skills stop them updating to cloud based specialised security tooling.

Internet of Things

The number of IoT devices being added to botnets increased in 2019 and a change in attack vectors to target enterprise IoT devices has been identified.[6] The impact on enterprise IoT devices being attacked and becoming unavailable is not only a service quality threat but potentially a health and safety, and patient care concern.

FIGURE 3

IoT BOTNET



1

A botnet is owned by the attacker, who is referred to as the bot master

2

The bot master controls the bot and deploys the initial malware infection into the IoT

3

Insecure IoT devices are located and they are added to all the botnet. Once added at is used to locate other vulnerable IoT devices

4

The victim's network receives traffic from infected IoT devices once, saturating the vulnerable IoT devices

[6] Shodan is a search engine for Internet-connected devices and it reports a 15,000 growth of insecure MQTT devices in 2019

GSMA Intelligence estimates a total of 13 billion IoT connections in 2020, a year-on-year growth of 15%. 57% of these are classified as consumer IoT connections and 43% are classified as enterprise IoT.[7] This trend is expected to continue with an estimated 25 billion IoT connections by 2025.[8]

The Vodafone IoT Barometer highlights how all industries surveyed were adopting IoT initiatives and with senor dense environments such as logistics and manufacturing alongside health management it is vital the verticals are protected. The impact of these services becoming unavailable is not just service quality but also health and safety and patient care.[9]

The ways to protect enterprise IoT are understood – failure to deliver on these security requirements however will potentially result in organisations' IoT devices becoming part of a wider attack, using up resources and potentially removing their availability.

Therefore, the GSMA recommends IoT service providers:

- Know what IoT devices are on their estate
- Secure their IoT devices; the GSMA maintains a flexible set of IoT Security Guidelines and an IoT Security Assessment. Advice includes:
  - Where possible confirm all IoT devices are compliant with corporate policies, including authentication, encryption, patching and password requirements
  - Where passwords cannot be changed, segregate the IoT devices within the network and place compensating controls in place
  - Where legacy (i.e. vulnerable M2M) devices, infrastructure and operating systems are in place, segment these services away from other areas of the network
  - Enable segment blocking in the event of an attack
- Identify what a device is and sense-check the data received/transferred ensuring it is sending the anticipated/expected data to the right location:
  - Monitor IoT device traffic e.g. for unexpected outbound widget or PowerShell requests attempting to pull malicious payloads on to your IoT devices
  - Restrict access to IoT devices by placing them behind network defences
  - Restrict outbound activity for IoT devices that do not require external access. (e.g. using IP address white-listing, barring of SMS/voice services etc.)
- Prepare an incident response plan for when the network is attacked by a botnet

[7] https://www.gsmaintelligence.com/research/?file=5a33fb6782bc75def8b6dc66af5da976&download

[8] https://www.gsmaintelligence.com/research/2019/02/the-mobile-economy-2019/731/

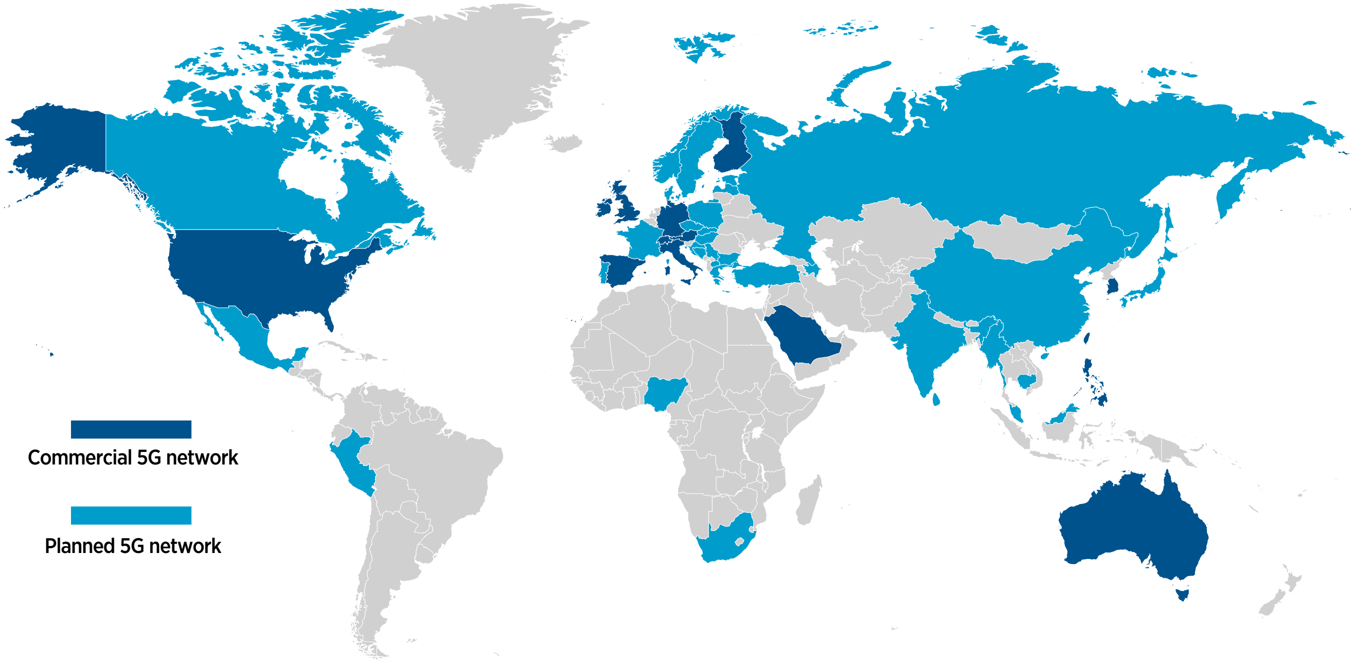
[9] https://www.vodafone.com/business/news-and-insights/white-paper/vodafone-iot-barometer-2019

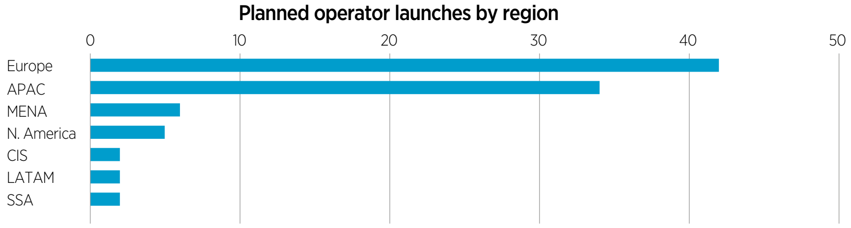
Securing the 5G Era

Last year 5G was a future consideration, this year saw the first non-standalone (NSA) 5G network deployments (figure 4).[11] This rollout period is a pivotal time, as the approach taken to implement and operationalise the architecture and underlying technologies, may result in missed opportunities afforded by the secure-by-design 5G standards.

FIGURE 4

5G COMMERCIALISATION[12]





Operator launch plans

As of Q3 2019:

76 operators from **51** markets had announced launch dates for mobile 5G services.

14 operators had stated plans to launch 5G-based fixed wireless services.

[11] https://www.gsma.com/futurenetworks/wiki/5g-implementation-guidelines/

[12] GSMA Intelligence Global 5G Landscape, Q3 2019

5G promises to revolutionise the way enterprises and consumers interact with mobile operators, providing richer services on more devices of varying capabilities. Government bodies, media and security researchers have been discussing security dangers of 5G this year as how the 5G era introduces numerous new technologies, new ways of working, and unprecedented increases in scale.[13, 14, 15] Telstra's 2019 Security Report stated that 'new technology impacting security' was a security team's biggest concern for the future. The AT&T Cyber Insights Report 2019 states:[16, 17]

Much of what is driving this threat is uncertainty. The 5G standards outline a service architecture that closes several of the gaps currently being exploited, including fraud and security issues.[18] At present NSA deployments are not making full use of this standards-based security, as much of this only comes when a 5G core (5GC) is deployed. Therefore, although there is potential for significant security enhancements, the security implementations that 5G can deliver are yet to be realised. With these rollouts and service launches, the opportunity to embed security, and prevent various known threats before they impact the network, is a possibility.

> **72.5% of the respondents rated their level of concern as high or medium-high when it comes to the potential impact of 5G on security.[17]**

5G needs to leverage many technologies and processes already in use, including:

- Management and network orchestration (MANO), and building of secure templates for server deployments and management. In 5G networks this should be used for network slicing, network function virtualisation (NFV) and container management.
- Supply chain risk assessment and product testing, and ensuring vendors offer appropriate security protection and are accountable for security lapses.
- Security operations, using Security Orchestration, Automation and Response (SOAR) and embedding 5G data into protective monitoring capabilities.
- Consider the whole lifecycle through design, development, procurement, deployment, operations and decommissioning and implement appropriate security for each stage.

These processes should be assessed against potential 5G threats and be validated to confirm that they scale at the rate and to the level required.

Operators should:

- Continue to build 5G networks that comply with 5G standards
- Drive industry interoperability to develop economies of scale among security controls
- Use 5G deployment programmes to rationalise and potentially isolate or close down less secure 2G/3G networks
- Join industry initiatives currently developing the implementation models for 5GC and 5G Non Stand Alone (NSA):
  - GSMA Fraud and Security Group (FASG) for the development of the Security Edge Protection Proxy (SEPP)[19]
  - GSMA Networks Group for secure roaming development[20]
  - GSMA Coordinated Vulnerability Disclosure programme for disclosing vulnerabilities impacting the industry[21]

[13] https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks

[14] https://www.forbes.com/sites/kateoflahertyuk/2019/11/13/new-5g-security-threats-spark-snooping-fears/#1c1f14f65025

[15] https://www.nytimes.com/2019/09/25/opinion/huawei-internet-security.html

[16] https://www.telstra.com.au/content/dam/shared-component-assets/tecom/campaigns/security-report/Summary-Report-2019-LR.pdf

[17] https://www.business.att.com/categories/cybersecurity-insights-report.html

[18] https://www.3gpp.org/release-15

[19] https://www.gsma.com/aboutus/workinggroups/fraud-security-group

[20] https://www.gsma.com/aboutus/workinggroups/networks-group

[21] https://www.gsma.com/security/gsma-coordinated-vulnerability-disclosure-programme/

Securing Device Applications

Failing to update applications (apps) installed on devices results in outdated privacy measures remaining in the ecosystem. This is a threat as potentially harmful apps (PHA) or data leaking apps are not blocked/controlled using the latest updates.[22, 23] This may lead to unauthorised use of consumer data.

There are over five billion unique subscribers, and mobile device usage accounts for 50% of internet traffic.[24] Consumers expect to be able to run their lives from their device, yet increasing awareness of inadequate privacy controls and unauthorised use of data diminishes consumer trust in the entire mobile telecommunications ecosystem.

Where app developers use standard software development kits (SDK) to build apps, 2019 has seen the following SDK related threats (figure 5):[25]

- Sharing tracking information with 3rd parties (no user awareness)
- Accessing data on the device that is unnecessary for its core function[26]

The combination of the above with vulnerabilities within an out-of-date app and this data may be exploited by an attacker.

[22] Potentially Harmful Applications (PHAs) are apps that could put users, user data, or devices at risk. These apps are often generically referred to as malware.

[23] Unauthorized or unintentional transfer of sensitive information from a mobile device to a 3rd party

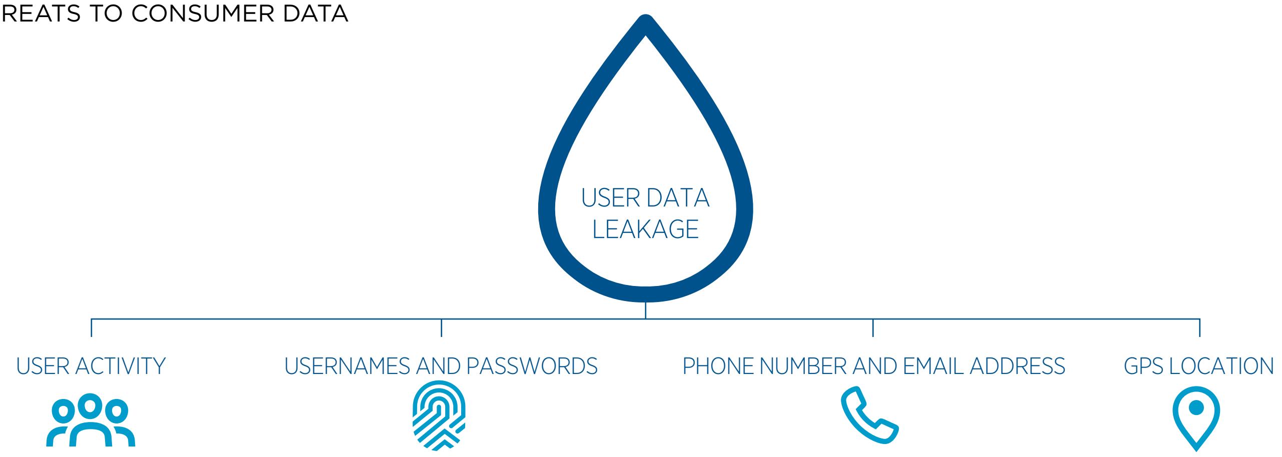
[24] https://www.gsmaintelligence.com

[25] https://www.hackread.com/85-adware-infected-apps-on-play-store

[26] https://www.zdnet.com/article/cheap-kids-smartwatch-exposes-the-location-of-5000-children/

FIGURE 5

THREATS TO CONSUMER DATA



The 2 major app stores, Google Play and the Apple App Store, have responded to these issues with updated privacy requirements for app developers.[27, 28, 29] However, users not updating their phones on a regular basis results in the measures having little impact on the underlying threat. There have also been reports of apps circumventing these controls.[30]

The GSMA is committed to working with stakeholders from across the mobile industry to develop a consistent approach to privacy protection and promoting trust in mobile services.[31] This commitment has resulted, among other initiatives, in the provision of leadership in this space through the GSMA Privacy Design Guidelines for Mobile Application Development.[32]

The GSMA Mobile Privacy Principles specifically emphasise that:[33]

- Mobile network operators should ensure that privacy risks are considered when designing new apps or services, and develop solutions that provide customers with simple ways to understand their privacy choices and control their data
- Developers of mobile device applications should embed industry-developed privacy principles and related design guidelines such as the GSMA mobile privacy principles
- Protection should be designed into new applications and services (i.e. privacy by design) to provide transparency, choice and control for the individual user, to build trust and confidence

Mobile network operators are encouraged to engage with and contribute to industry initiatives, such as the GSMA's Device Security Group (DSG) to develop secure device best practice for the industry.[34]

[27] https://www.theregister.co.uk/2019/03/20/googles_call_and_sms_clampdown_trips_up_tons_of_apps/

[28] https://developer.android.com/about/versions/10/privacy/changes

[29] https://latesthackingnews.com/2019/10/14/ios-13-now-warns-users-of-background-apps-secretly-tracking-location/

[30] https://www.itpro.co.uk/security/33980/more-than-1000-android-apps-deceptively-harvest-personal-data?_mout=1&utm_campaign=itpro_newsletter&utm_medium=email&utm_source=newsletter

[31] https://www.gsma.com/publicpolicy/wp-content/uploads/2017/02/GSMA_Safety-privacy-and-security-across-the-mobile-ecosystem.pdf

[32] https://www.gsma.com/publicpolicy/resources/privacy-design-guidelines-mobile-application-development

[33] https://www.gsma.com/publicpolicy/wp-content/uploads/2016/02/GSMA2016_Guidelines_Mobile_Privacy_Principles.pdf

[34] Join the DSG here https://infocentre2.gsma.com/_layouts/InfoCentre/Login.aspx?ReturnUrl=%2fgp%2fwg%2fFSG%2fDS%2f_layouts%2fAuthenticate.aspx%3fSource%3d%252Fgp%252Fwg%252FFSG%252FDS%252FPages%252FDefault%252Easpx&Source=%2Fgp%2Fwg%2FFSG%2FDS%2FPages%2FDefault%2Easpx

Security Skills Shortage

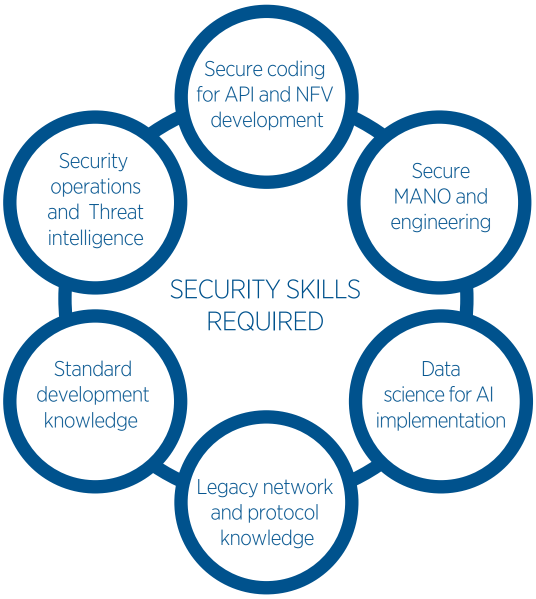
Reports indicate that the wider security industry is facing a global skills shortage. This is impacting the mobile industry, either through direct hire or supplier skills. Mobile telecommunication networks are some of the most complex, wide reaching and long-standing networks in the world. Developing the right skills to protect future and legacy networks in the current skills shortage is challenging.

> **A lack of skilled and experienced cybersecurity personnel tops cybersecurity professionals' list of job concerns (37%)[35]**

Mobile networks consist of standardised and proprietary elements, unique configurations and numerous protocols that have developed over five generations. The 5G era revolutionises the way these networks work, introducing new skill requirements yet legacy generations will remain for years to come, meaning legacy skills need to be retained (figure 6).[36] Couple this with the persistent advanced threats these networks are subjected to, and the environment becomes a niche area to resource.

FIGURE 6

SKILLS REQUIRED TO EFFECTIVELY PROTECT THE TELECOMMUNICATIONS NETWORK


Secure coding for API and NFV development
Secure MANO and engineering
Data science for AI implementation
Legacy network and protocol knowledge
Standard development knowledge
Security operations and Threat intelligence
SECURITY SKILLS REQUIRED

[35] https://blog.isc2.org/isc2_blog/2018/10/cybersecurity-skills-shortage-soars-nearing-3-million.html

[36] https://www.infosecurity-magazine.com/news/gartnersec-hiring-strategies/

Highlighting a specific concern. Automation should be the preferred way to manage threats effectively in a telecommunications network where possible. Based on this it should concern the industry that the Cost of a Data Breach Report 2019 stated the following with regard to automated security tooling rollout:[37]

> **16% of companies reported full deployment and 36% reported partial deployment. Another 36% do not deploy security automation today but they do plan to deploy automation technologies within the next 24 months. Finally, 12% did not deploy, and had no plan to deploy security automation.**

To limit the impact the industry should:

- Model and define the current and future threats, clarify what skills are required to protect against them, and ensure that training plans and skills matrices recognise these required skills
- Define formal and informal training mechanisms to diversify skills
- Have a structured skills management capability, focusing on function based skills analysis, highlighting skills gaps. Where gaps are located consider:
  - Build or buy: does the skills gap require immediate externally procured skills or is the threat longer term, allowing the skills to be developed internally?
  - Whether to integrate graduate and apprentice schemes into security skills development
- Reassess cybersecurity roles on an annual basis, driving the right knowledge and capabilities within the teams
- Consider succession planning for senior leadership positions, moving from technical into senior leadership requires different, often softer, skills e.g. communications, influencing and strategy building
- Ensure supplier skill resilience is understood before partnering for strategic initiatives
- Automate when possible – as a manual security controls matures, consider using automation to remove human touch points. Not only is this more efficient, it allows the teams to upskill based on the threats faced

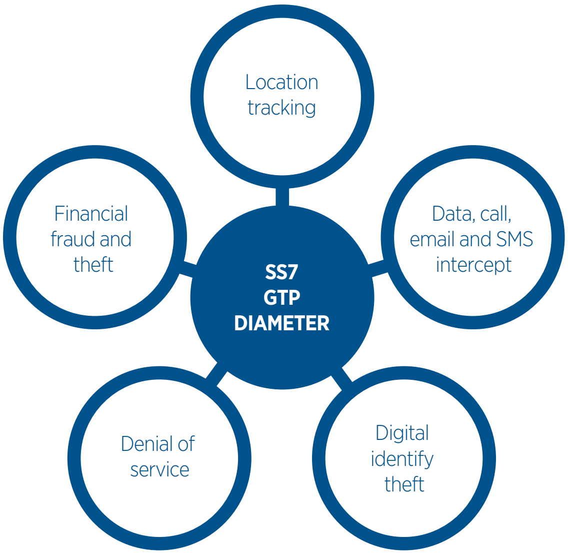
[37] https://databreachcalculator.mybluemix.net/executive-summary/ (not telecommunications specific)

Signalling Threats

2G and 3G networks are still deployed globally, and it is unlikely that they will disappear from the ecosystem for many years to come. This means that legacy threats (figure 7) will continue to require compensating technologies and controls to protect consumers whilst they connect through these dated technologies.

FIGURE 7

THREATS IN SIGNALLING



The industry understands threats posed by signalling protocols, SS7, GTP and Diameter – however their fixes are not straightforward to apply to complex and large scale networks.[38, 39, 40] As such, these threats are unlikely to be removed from any threat landscape relating to the mobile telecommunications industry for several years to come.

Recent research found that:[41]

- 53% of call tapping attempts on 3G networks succeed
- 67% of networks fail to prevent bypass of SS7 protection
- 9 out of 10 SMS messages can be intercepted

The insecurity of SMS has affected verticals that rely on SMS as part of their 2-factor authentication (2FA) processes, specifically finance.[42] This trend highlights the ongoing and legacy nature of this threat as the same threats were reported within industry since 2014.

Current signalling protocols will remain in use within the industry for many years to come; as a result, the GSMA recommends that operators implement compensating controls, specifically:

- Provide guidance for consumers and enterprises on the risks of using SMS as a multi-factor authentication mechanism
- Implement signalling controls outlined in the GSMA Fraud and Security Group (FASG) guidelines on securing interconnect protocols[43]
- Have a fraud management system (FMS) to identify, detect and prevent potential fraud transactions within the signalling messages
- Deploy signalling firewall, or equivalent, technologies to support the monitoring and blocking of signalling traffic
- Prepare for realistic threat scenarios where the network is compromised. Once these threats are modelled, a set of security parameters, based on the signalling protocols, can be deployed
- Use 5G deployment programmes to rationalise and potentially isolate or close down less secure 2G/3G networks[43]

[38] Signalling System 7 (SS7) is an international telecommunications standard that defines how network elements in a public switched telephone network (PSTN) exchange information over a digital signalling network. Signalling Transport (SIGTRAN) is the standard telephony protocol used to transport Signalling System 7 (SS7) signals over the Internet.

[39] GPRS Tunnelling Protocol (GTP) is a group of IP-based communications protocols used to carry general packet radio service (GPRS) mobile telecommunication networks

[40] Diameter protocol is a subscriber authentication, authorisation and accounting protocol created to replace SS7.

[41] https://conference.hitb.org/hitbsecconf2019ams/materials/D1T2%20-%20Bypassing%20GSMA%20Recommendations%20on%20SS7%20Networks%20-%20Kirill%20Puzankov.pdf

[42] https://www.scmagazineuk.com/criminals-hit-metro-bank-multi-factor-authentication-bypass-ss7-attack/article/1524670

[43] https://infocentre2.gsma.com/gp/wg/FSG/AFS/Pages/Default.asp

[44] Although 4G networks use another signaling protocol (Diameter), they still need to interface with previous-generation mobile networks for converting incoming SS7 messages into equivalent Diameter ones

Software Threats

In the GSMA's last annual review open source software (OSS) was highlighted as a threat to mobile operator networks. This has not altered; 2019 saw software utilisation within operator networks take centre stage with regard to 5G network rollout.[45]

In previous generations software was often proprietary and supported by major vendors. As the networks have developed even proprietary software relies on OSS or shared libraries to drive business support systems (BSS) and operational support systems (OSS). Operators may also develop their own code to support various services through DevOps teams. The 2019 DevSecOps Community Survey states that:[46]

> **47% of released OSS components had a vulnerability discovered in one of its dependencies, during the period in which that version was current.**

[45] 5G will open up the operator networks to allow richer services. Ultra high speed and low latency will be delivered through optimisation of the network, using virtualisation and/or edge computing. Core technologies, previously protected centrally, will become decentralized. All of this is enabled by software, many of the OSS practices that will be leveraged will remain the same.

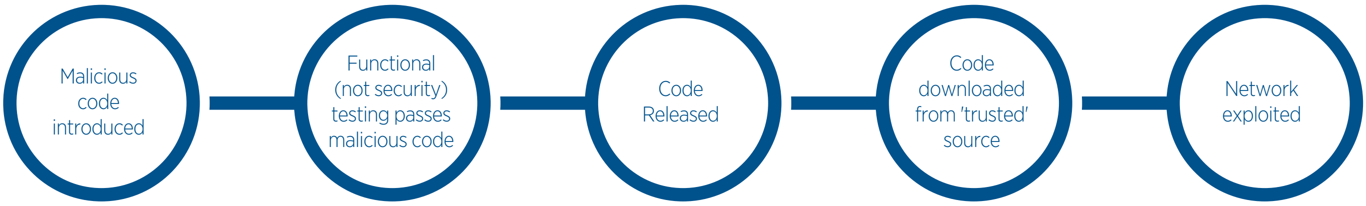
[46] https://www.sonatype.com/en-us/2019ssc

In addition, their study explains how actively supported open source projects took 3 weeks to fix reported vulnerabilities. Latent vulnerabilities within unsupported projects remain an unknown, but highly likely, industry threat.

Open source does not mean zero cost, only the license component is free, deployment and management of codebases used within the network continues to needed in operational costs. Failure to review and test code prior to use leads to potential latent or known vulnerabilities being deployed into the network; increasing the threat surface.

FIGURE 8

OSS DEPLOYMENT, COMPROMISING THE SUPPLY CHAIN


Malicious code introduced
Functional (not security) testing passes malicious code
Code Released
Code downloaded from 'trusted' source
Network exploited

This threat was actively exploited in 2019: RubyGems, Ruby's package manager, and Ruby libraries were exploited allowing malicious libraries to be introduced into the supply chain.[47, 48] The issue with this type of attack is that the malicious downloads came from a 'trusted' site (figure 8). Trusted sources within the software community must therefore become a thing of the past.

Based on the increased use of OSS and shared libraries, the GSMA predict that this threat will increase over time and recommends the following with regard to software supply chain security:

- Operators should verify that vendors and service implementers can provide a list of:
  - OSS/shared libraries in use in their products and services
  - Versions used, to allow patching
- Vendors and service implementers should ensure:
  - They know which OSS/shared libraries are present in their products and services, potentially through use of a repository manager
  - Prior to deployment or using shared libraries make sure there are no known public vulnerabilities (e.g check CVE databases)
  - Only current OSS libraries are present in their products
- Verify all deployed OSS libraries are from supported projects with long term management
- Ensure all software used within the network is subject to internal software development lifecycle (SDLC) processes. For instance, check for known vulnerabilities before usage and apply patches/updates in a timely manner
- Include OSS in vulnerability management programmes
- Implement runtime application security protection (RASP) to prevent vulnerabilities from being exploited within deployed libraries

[47] https://arstechnica.com/information-technology/2019/08/the-year-long-rash-of-supply-chain-attacks-against-open-source-is-getting-worse/

[48] https://www.zdnet.com/article/backdoor-found-in-ruby-library-for-checking-for-strong-passwords/

Supply Chain Resilience

2019 saw supply chain threats develop with regard to supply chain resilience. Specifically, a lack of supply chain resilience affects operators' abilities to deliver products and services to society. Two resilience issues have come to the forefront this year:

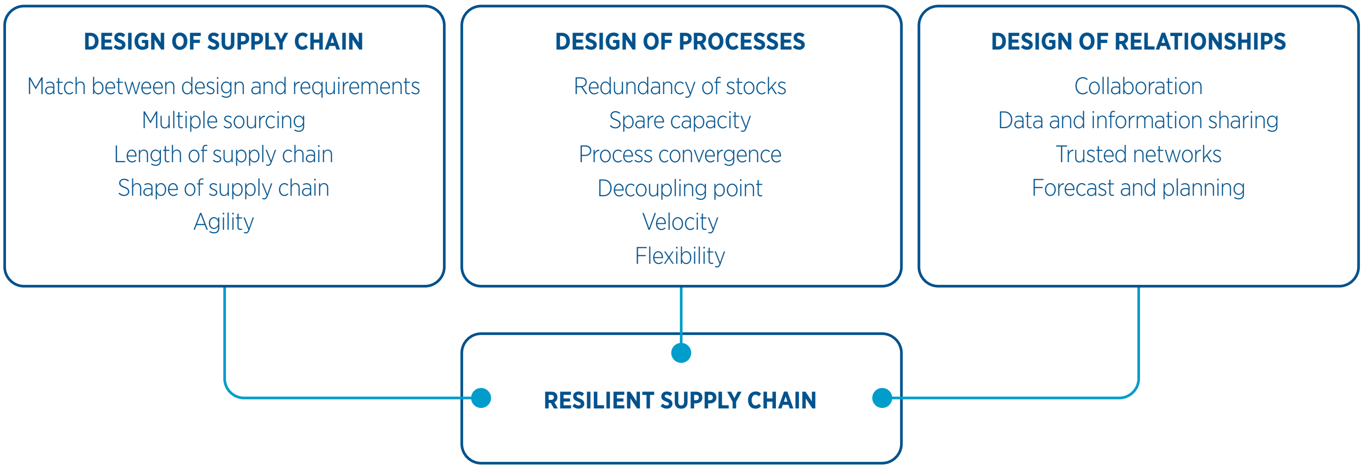
- Trusted suppliers and geopolitical relations for critical national infrastructure (CNI) / security sensitive components[49]
- Component availability based on the global supply chain

Availability of equipment and diverse suppliers are vital for market economies and to prevent vendor lock-in. A resilient supply chain has components available from multiple sources (figure 9). These sources should be geographically resilient to manage geopolitical or natural disaster type threats. 2019 has seen several countries ban or restrict Huawei equipment from being used within 5G networks. This has highlighted the lack of diversity and resilience within the network equipment supply chain.

[49] Many Operators in North America and Europe are considered CNI, meaning local governments have a certain authority within the industry. 5G will enhance the services provided by the Operator networks and as such the political view is that 5G networks will require a higher level of protection for National Security reasons.

FIGURE 9

SUPPLY CHAIN RESILIENCE



As new technologies are standardised, suppliers carrying out research and development mature their technologies that subsequently lends itself to increasing their technology footprint in the market. This makes it possible to realise economies of scale, but it also means components are often sourced from one supplier, which in the mobile industry can be a cause for concern as the number of these suppliers has diminished over the years with few new entrants reaching sufficient scale to alleviate the challenge.

There are no quick fixes to resilience threats. The threat has emerged due to the long term and complex nature of the industry sourcing activities, contract lifecycle support needs and technology interoperability requirements. For example, hardware is supplied by one supplier but the service contract for hardware support may be outsourced to another. As a result, removing one vendor may have a knock-on effect on other contracts and services.

The GSMA recommends the following with regard to supply chain security:

- Understand who you do business with; prioritise and risk assess each supplier with specific focus on redundancy, flexibility and the technical and procedural ability to switch supplier if required
- Map and assess the criticality of any component / service offering within the supply chain. Plan and manage operational security (along with reliability etc.) accordingly
- Build business continuity plans that consider the removal of critical vendors; understand the impact if one were to be removed
- Work with local legislators and regulators to understand how potential decisions with regard to supplier bans
- Engage with and support international standards development. LTE was the first global standard for the mobile networks. Moving away from global standards for 5G would impact the deployment and long term security of the industry
- Encourage suppliers to participate in industry recognised security assurance schemes, such as GSMA's Security Accreditation Scheme (SAS) and Network Equipment Security Assurance Scheme (NESAS) and source equipment from suppliers that participate in these schemes

2020 and beyond

5G standalone and scaled security

The first standalone 5G networks are expected to be deployed in 2020-21. These networks will enable the secure-by-design service architecture defined in the 5G standards.[50] The GSMA prediction is that these networks will not have considered all implementation and integration requirements for security dependencies that come with protecting a 5G network in life.

For example, network slicing may be deployed for a specific use case. Security controls for each use case are likely to differ. These controls will need to include secure deployment, in-life isolation controls and automatic monitoring upon launch. Failure to plan for these varied situations may result in an add-on implementation required post-deployment, impacting overall service delivery.

[50] 5G Networks can be implemented in different and diverse ways and not all regions will deploy at the same time or deploy the same services, such diversity brings challenges.

Network visibility

Traffic within networks continues to be move to encrypted channels and the GSMA predicts is that most protocols will move to being encrypted, e.g. DNS is the latest protocol likely to move to encrypted HTTPS tunnel (DoH), the result of which will be reduced traffic visibility.

This means that signature-based detection will become void, and the need for anomaly based detection will become essential. This may be hampered by the fact that older telecommunications protocols may not be understood by off-the-shelf products, limiting their effectiveness.

Increased blended attacks

A natural evolution will occur in which the threats outlined in this document are combined to have higher impact. For example:

- Cloud threats are already being impacted by a lack of skills to support rollouts and security requirements
- The growing IoT will be used to launch higher impact availability attacks
- 5G networks will bring together IT and mobile networks and the hybrid technologies will result in many blended threats the industry has not had to traditionally handle
- Lateral movement attacks will increase and 'non-network' assets such as business support systems will be a significant target

Threat modelling, network understanding and cross pollination of skills via job rotations for IT and mobile engineers should be considered.

Supply chain service impact

At present the industry focus is on network equipment. However, the GSMA predicts that there are underlying problems within the service supply chain as well. A system is as secure as its in-life support. As suppliers disappear from the supply chain, so does service implementation and in-life management support, and these are the services that apply secure by default configurations, apply security patches and manage various other security hygiene activities. Reduction in the quality of this service will increase the threat surface for their customers and make exploitation easier for threat actors.

Final Thoughts

This threat landscape provides a set of recommendations for the industry to consider in the context of current threats facing the industry. These threats and recommendations are not new, and effective responses are possible.

The threats faced and protection required should not stand in the way of society's desire for technological advancement. Security must stand side-by-side and support innovation as close to technology conception as possible. This is the only way for secure-by-design to become commonplace in the industry.

Threats are not just technical in nature, but involve the whole lifecycle across people, process and technology, and responses and mitigations to such threats must also consider this.

The threats discussed above relate to technologies that may have been designed with security as a consideration, but deployment and ongoing management has resulted in vulnerabilities that have been exploited in successful attacks. This shows how important it is to ensure security remains in place throughout the lifetime of a product or service.

Over the coming year the GSMA will continue to support its members on security matters. To get in touch, please email **security@gsma.com.**

GSMA Member Security Services

Further reading

Telecommunication Information Sharing and Analysis Centre (T-ISAC)

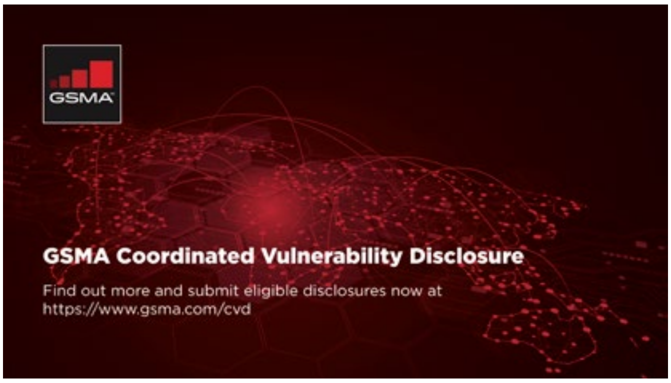
For Security Threats within the Mobile Industry

Security Accreditation Scheme

Accredited Supplier

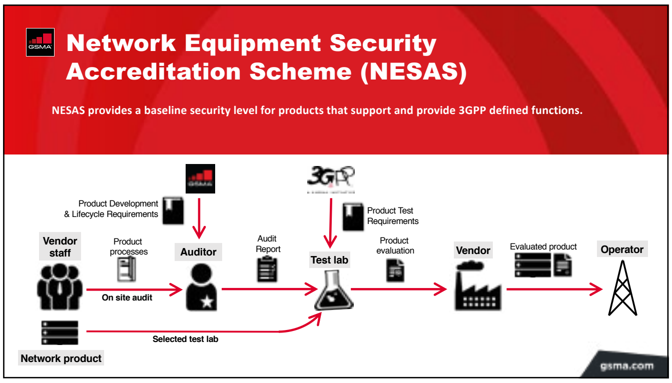
(SAS-UP) (SAS-SM)

- Two GSMA security audit schemes for supplier sites
  - SAS for UICC production (SAS-UP)
  - SAS for Subscription Management - supporting eSIM (SAS-SM)
- Security audit conducted against high standard by GSMA's auditors
- GSMA certifies successful sites for 1-2 years



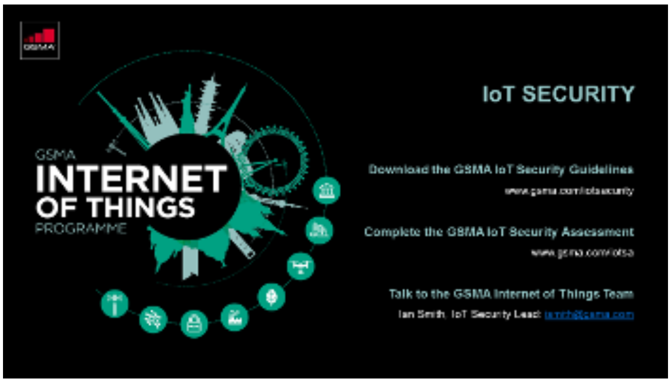
GSMA Coordinated Vulnerability Disclosure

Find out more and submit eligible disclosures now at https://www.gsma.com/cvd



Network Equipment Security Accreditation Scheme (NESAS)

NESAS provides a baseline security level for products that support and provide 3GPP defined functions.



GSMA INTERNET OF THINGS PROGRAMME

IoT SECURITY

Download the GSMA IoT Security Guidelines
www.gsma.com/iotsecurity

Complete the GSMA IoT Security Assessment
www.gsma.com/iotsa

Talk to the GSMA Internet of Things Team
Ian Smith, IoT Security Lead: ismith@gsma.com

FASG Fraud and Security Group

GROUP MEMBERS 1400+
PLENARY ATTENDANCE 150+

Drive the industry's management of fraud and security matters related to GSM technology, networks and services.

KEY INDUSTRY BENEFIT

Build and maintain trust in mobile networks and technologies. Information sharing on latest fraud & security risks and mitigation reduces operator losses and protects brands.

LATEST FOCUS

- 5G Security
- Security assurance scheme for network equipment (NESAS)
- 5G & Diameter Interconnect Security & Key Management.

FASG SERVICES

Security Accreditation Scheme | Intelligence Sharing (T-ISAC) | Coordinated Vulnerability Disclosure | IMEI Security testing | Stolen handset data sharing

LEADERSHIP

CHAIR
David Rogers, Copper Horse Limited

DEPUTY CHAIR
Andy Mayo, Vodafone

GSMA HEAD OF SECURITY
James Moran, GSMA

DIRECTOR
David Maxwell, GSMA

COORDINATOR
Karola Rajoo, GSMA

gsma.com

About the GSMA

The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with over 350 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces the industry-leading MWC events held annually in Barcelona, Los Angeles and Shanghai, as well as the Mobile 360 Series of regional conferences.

For more information, please visit the GSMA corporate website at **www.gsma.com**

Follow the GSMA on Twitter: **@GSMA**

About the GSMA Fraud and Security Team

The team's purpose is to analyse the industry's threat landscape and provide information that enables our member's ability to protect the mobile ecosystem.

The team manage the GSMA's Coordinated Vulnerability Disclosure (CVD) programme, the GSMA's Telecommunication Information Sharing & Analysis Centre (T-ISAC), Security Accreditation Schemes and Fraud and Security Groups (FASG).

For further information, please visit:
www.gsma.com/security

GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London EC4N 8AF
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601

January 2020