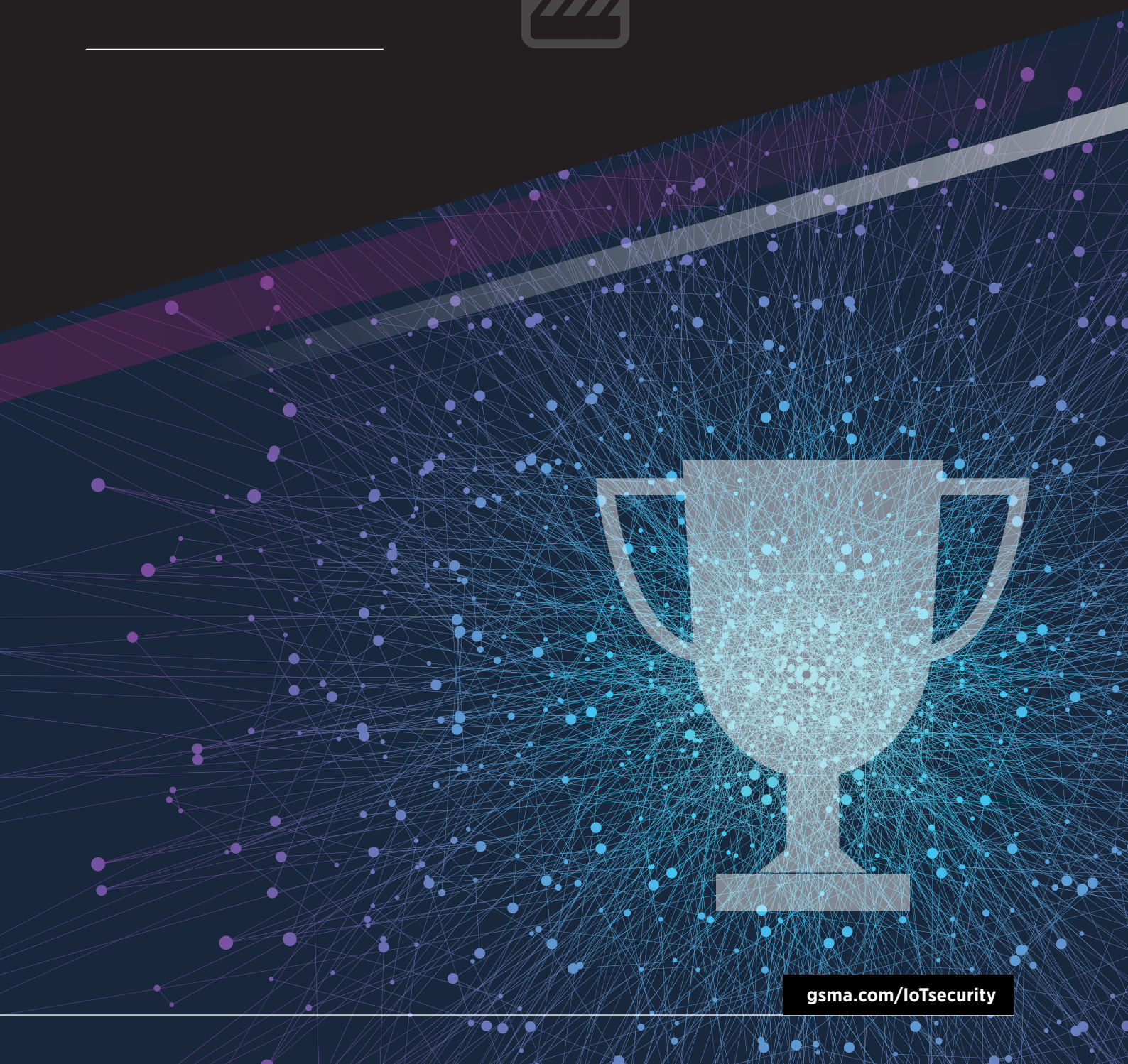
IoT SECURITY CHAMPIONS

BUILDING TRUST INTO THE IoT



gsma.com/IoTsecurity

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 industry-leading events such as Mobile World Congress, Mobile World Congress Shanghai, Mobile World Congress Americas and the Mobile 360 Series of conferences.

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

Follow the GSMA on Twitter: @GSMA.

About the GSMA Internet of Things Programme

The GSMA's Internet of Things Programme is an industry initiative focused on:

- **COVERAGE** of machine friendly, cost effective networks to deliver global and universal benefits.
- **CAPABILITY** to capture higher value services beyond connectivity, at scale.
- **CYBERSECURITY** to enable a trusted IoT where security is embedded from the beginning, at every stage of the IoT value chain.

By developing key enablers, facilitating industry collaboration and supporting network optimisation, the Internet of Things Programme is enabling consumers and businesses to harness a host of rich new services, connected by intelligent and secure mobile networks.

Visit gsma.com/iot to find out more about the GSMA IoT Programme.

EXECUTIVE SUMMARY

Security concerns and threats could inhibit the expansion of the Internet of Things (IoT). The provision of wide area connectivity to an ever-greater variety of devices is increasing the IoT ecosystem's exposure to fraud and attack.

As well as using licensed spectrum and 3GPP standards to provide secure connectivity, mobile operators and their partners are increasingly employing the GSMA's IoT Security Guidelines and Assessment to build end-to-end security into IoT solutions. Based on interviews with 14 leading mobile operators[1], this paper explores how players across the ecosystem are integrating the GSMA framework into their product development and testing processes.

The interviews revealed that leading operators regard the GSMA IoT Security Guidelines and Assessment as both rigorous and thorough. Operators' security experts lauded the comprehensive and end-to-end nature of the Assessment. "It is a way to ask good questions of the overall security of the platform, to check every security measure," says Ivan Lovric, IoT Expert and IT Security Specialist, Orange Group. "It provides a way of seeing everything that anybody has ever experienced," adds Ben Tyson, Business Security Officer at Telenor Connexion. "With the GSMA Assessment, you have access to a wide range of expert knowledge." Furthermore, the Assessment is providing operators with a valuable global perspective on IoT security. "The GSMA brings the experience and knowledge of a large number of global operators, which is very useful for customers and partners that are developing their business globally, such as automotive companies," says Keigo Harada, General Manager, Head of IoT Business Planning Department at KDDI.

The robustness and completeness of the GSMA's Assessment and Guidelines is giving enterprises the assurance they need to deploy IoT solutions for sensitive applications. "The Assessment is helping us to deploy video surveillance solutions with banks, airports, export agencies and others," says Alberto Araque, Vice President, Internet of Things & Digital Payments, at Etisalat. "That could not happen without security: customers, many of which are government agencies, need to have full confidence in the solution."

The Assessment is also proving to be highly versatile. Telefónica, for example, has used it to evaluate the security of everything from personal tracking devices to the sophisticated marine traffic management system deployed by the port of Seville. It can also scale: Etisalat has used the Assessment to evaluate the security of a public safety solution, involving the rollout of approximately four million connected sensors in about 400,000 locations.

In many cases, the Assessment has helped operators identify and fix vulnerabilities. For SK Telecom, for example, the evaluation revealed that its M2M router product had an additional management port that could be accessed by anonymous actors. In line with the GSMA Guidelines, SK Telecom advised the vendor to apply two-factor authentication or a stronger authentication mechanism, such as a VPN.

Some operators, such as Turkcell, are integrating elements of the GSMA Guidelines into their request for quotation (RFQ) and request for proposal (RFP) processes. At the same time, the Assessment is providing a consistent framework that operators can use to discuss security with both suppliers and customers. "The assessment process has also raised awareness among our partners," notes Vicente Segura of Telefónica. "It has forced them to start thinking about the key risks in supply chain security."

[1] AT&T, Bharti Airtel, China Mobile, China Telecom, China Unicom, Etisalat, KDDI, Omantel, Orange, SK Telecom, Telefónica, Telenor, Turkcell and Verizon

TABLE OF CONTENTS

GSMA IoT SECURITY GUIDELINES AND ASSESSMENT

The provision of secure products and services is as much a process as it is a goal. Vigilance, innovation, responsiveness and continuous improvement are required to ensure the solutions address the threats. To safeguard new IoT products and services, mobile operators, together with their network, service and device equipment partners, are sharing their security expertise with providers looking to develop new IoT services.

First published in February 2016, the GSMA IoT Security Guidelines are a set of best practices for the secure end-to-end design, development and deployment of IoT solutions on any mobile network. Based on the expertise and collective knowledge of the mobile telecoms industry, the guidelines offer valuable insights and recommendations to enable the creation of trusted, reliable and scalable IoT services. Since their initial publication, the guidelines have been regularly reviewed and updated by industry experts to ensure they address the latest security threats and issues.

The GSMA IoT Security Assessment scheme enables IoT companies to verify that their products are aligned with the GSMA Guidelines. It allows IoT companies to demonstrate the security measures they have taken to protect their products and services from cyber security risk, enhancing their reputation as trusted IoT service providers.

The GSMA IoT Security Assessment scheme covers security controls for the whole ecosystem and further enhances the alignment of all stakeholders by putting in place a concise framework with consistent terminology and a structured approach to IoT security information. It enables companies to check whether their security measures align with the best practice outlined in the GSMA IoT Security Guidelines. Companies can use the assessment to address weaknesses in their products and services, and demonstrate to their customers that they are taking cyber security seriously.

The GSMA IoT Security Guidelines:

- Include 85 detailed recommendations for the secure design, development and deployment of IoT solutions
- Cover networks as well as service and endpoint ecosystems
- Address security challenges, attack models and risk assessments
- Provide several worked examples

The GSMA IoT Security Assessment:

- Is based on a structured approach and concise security controls
- Covers the whole ecosystem
- Can fit into a supply chain model
- Provides a flexible framework that addresses the diversity of the IoT market

The primary audience for the IoT Security Guidelines are:

- IoT service providers – organisations looking to develop new and innovative connected products and services
- IoT device manufacturers – who provide IoT devices to enable IoT services
- IoT developers – who build IoT services on behalf of IoT service providers
- Network operators – who provide services to IoT service providers

CASE STUDY

AT&T

HIGH-LEVEL APPROACH TO IoT SECURITY

AT&T, one of the largest operators in the US, has developed an end-to-end IoT security strategy and framework. It employs a multi-layered approach, breaking down the ecosystem into segments that need to have an independent security solution and into solutions that cut across the segments. "There is the device or endpoint layer, the connection layer, the application layer, and the threat management layer, which wraps around the others," says Senthil Ramakrishnan, Lead Member of Technical Staff, Product Development, at AT&T – IoT Solutions. "We are deploying security solutions in each layer, and across the layers."

If a customer buys an end-to-end IoT solution, including devices, from AT&T, it comes with security pre-integrated. However, in most cases there is also some level of customisation, beyond the base level of security built into the product. For example, compliance with GDPR is critical in Europe. "With partners, we use an IoT security lifecycle framework: a new project always follows the secure design lifecycle," adds Senthil Ramakrishnan. "Security needs to be included from day one. When the product team defines the feature requirements, we also define the security."

THE IMPLEMENTATION AND IMPACT OF THE GSMA IoT SECURITY ASSESSMENT

AT&T says the big advantage of the GSMA IoT Security Assessment over alternatives is its coverage of the end-to-end ecosystem. "We work with several other industry bodies, which are focused on certain pieces, but the GSMA Assessment goes across the ecosystem," explains Senthil Ramakrishnan. "It provides a very solid base for our internal teams, partners and customers. Its strength is how comprehensive the Assessment is."

AT&T says the GSMA Assessment can be applied regardless of the business model that underpins the IoT solution. In cases where AT&T is just selling connectivity, it provides the GSMA IoT Security Assessment and Guidelines to customers so they can use them to build a solution with end-to-end security. "Customer feedback has been very strong," notes Senthil Ramakrishnan. The GSMA documentation "is particularly important for small and medium-sized enterprises (SMEs) and companies that are new for IoT. For them the guidelines are an excellent source of information, as they are the simplest comprehensive set of requirements that we can provide to customers. The GSMA is the only set that we provide, aside from the AT&T requirements, which is a testament to their quality."

AT&T has performed the GSMA IoT Security Assessment on its own network and on its asset management solution. "We have validated that we do indeed meet the GSMA requirements, which gives us and the customers a lot of confidence," says Senthil Ramakrishnan. The operator is now systematically applying the Assessment to new IoT solutions. When preparing to launch a new product or service, AT&T employs multi-phase checkpoints, one of which is a security checkpoint. It has integrated the GSMA IoT Security Assessment into that checkpoint to ensure the new product or service meets both AT&T's requirements and the GSMA's requirements. The Assessment "is an integral part of the approval process before a product gets to launch," notes Senthil Ramakrishnan.

> *"the guidelines are an excellent source of information, as they are the simplest comprehensive set of requirements that we can provide to customers"*
>
> **Senthil Ramakrishnan,** Lead Member of Technical Staff, Product Development, AT&T

CASE STUDY

BHARTI AIRTEL

HIGH-LEVEL APPROACH TO IoT SECURITY

As the IoT expands in India, Bharti Airtel is seeing growing demand for a telco-grade platform that enables enterprises to connect their devices securely to the cloud. Airtel offers enterprises everything from secure connectivity with authentication to complete end-to-end IoT solutions in which the operator takes responsibility for securing the end-points, the connectivity and the resulting data. Airtel assesses the full stack of the service, encompassing the device, the operating system, the hardware, the firmware source, the communications module, the authentication mechanism, the encryption mechanism, cloud data, application and analytics for any possible loose ends and/or security threats.

As its IoT business grows, Airtel is building a broad ecosystem in India, working with its partners to ensure they follow security best practices. "We are in the process of forming a team of security experts within the security organisation to focus on IoT – this team will work closely with the partners and customers to carry out risk assessments and provide recommendations to fix any gaps," explains Tarun Bhatia, Enterprise Architect at Airtel. "Security cannot be thought of as an add-on to a device, but rather as integral to the device's reliable functioning."

Airtel encrypts data at rest and data in motion, both on the device-side and the cloud-side. It is also introducing software security controls at the operating system level to take advantage of new hardware security capabilities on the market, and continuously maintain the trusted computing base.

THE IMPLEMENTATION AND IMPACT OF THE GSMA IoT SECURITY ASSESSMENT

Airtel is employing the GSMA IoT Security Assessment to "fine tune" its security assessment methodology for IoT, which it will share with suppliers and customers. "The GSMA IoT Security Guidelines provide a high-level outline of what to think through while designing the solution, so we are using them to help create an Airtel Assessment Framework," says Tarun Bhatia. It makes sense to leverage the GSMA IoT Security Assessment because it provides "vigilance, innovation, responsiveness and continuous improvement using collective global knowledge," he adds. "The guidelines are quite open ended for

operators to comprehend and adapt as needed." During 2019, Airtel plans to use its new assessment framework to evaluate the security of its new connected car and smart home solutions.

At the same time, Airtel is developing a robust and thorough threat model and risk assessment that clearly identifies areas of security concern and appropriately directs and apportions security countermeasures. "With 5G and NB-IoT, there will be an explosion of unstructured devices supporting new use cases, which will lead to new security threats," notes Tarun Bhatia. "It is changing so fast. The IoT Security Assessment will not be a destination, but a journey which will keep evolving in 2019 and beyond."

> *"With 5G and NB-IoT, there will be an explosion of unstructured devices supporting new use cases, which will lead to new security threats"*
>
> **Tarun Bhatia,** Enterprise Architect, Airtel

CASE STUDY

CHINA MOBILE

HIGH-LEVEL APPROACH TO IoT SECURITY

China Mobile's IoT business is growing rapidly. It was serving 384 million IoT connections at the end of June 2018, after adding an additional 155 million IoT connections in the first half of the year. China's largest mobile operator publishes general security requirements for the IoT devices it distributes, supplemented by recommended security implementation requirements, while also evaluating and testing individual IoT devices. In particular, the operator checks the security design, hardware security implementation (a secure element or trusted execution environment) and performs penetration tests.

THE IMPLEMENTATION AND IMPACT OF THE GSMA IoT SECURITY ASSESSMENT

China Mobile describes the GSMA IoT Security Assessment as "helpful" to assess IoT device security. "The coverage of the checklist is wide, not only from the technical point of view, but also from the perspective of management," says Jie Ma, Project Manager at China Mobile.

Working together with its partners, China Mobile has used the GSMA Assessment to verify the security of several own-brand NB-IoT-enabled devices. The operator has deployed NB-IoT networks, which offer low power wide area connectivity, across much of the country. The assessed own-brand devices include NB-IoT connected smoke detectors aimed at enterprises, campuses and homes, and cameras for monitoring home security. It has also assessed NB-IoT-enabled smart home routers, which provide routing, remote web login and whitelist services, as well as connectivity modules designed to protect vehicles from theft by keeping track of their location and their driving history, while sounding the alarm if there is anomaly.

After using the GSMA collateral, China Mobile has expanded the scope of its security assessment to include supply chain security and device components' security. Moreover, Jie Ma says its "basic assessments for the same category devices" draw on the GSMA IoT Security Assessment to improve the efficiency of the process.

CASE STUDY

CHINA TELECOM

HIGH-LEVEL APPROACH TO IoT SECURITY

Together with its partners and customers, China Telecom is developing end-to-end security solutions for the IoT. It has just established an IoT security framework, and is in the process of verifying its effectiveness. "IoT security is critical for the stability of the operation of digital economies and the healthy development of the whole of society," notes Yongpan Ren of the Internet Security Department, Shanghai Research Institute, China Telecom. "With the extensive development of the IoT, there are more and more security incidents. IoT security issues not only result in data leakage, as with traditional Internet security issues, but can also endanger life and property."

He stresses the need to move on from the traditional thinking of "launch the service first and enhance the security later," adding that "before deploying a new IoT service, multiple levels of security checks and a strict evaluation are needed." Yongpan Ren highlights the need to take into account the new security risks arising from the introduction of the "perception layer" of the IoT. "We should not only focus on the traditional security risks, we should put more efforts on the new security risks in the sensor level and put forward more systemic, in-depth security evaluation mechanisms that are suitable for IoT devices," he says.

THE IMPLEMENTATION AND IMPACT OF THE GSMA IoT SECURITY ASSESSMENT

China Telecom has used the GSMA IoT Security Assessment to evaluate several NB-IoT connected devices and a smart speaker. "Through the evaluation, we can detect any existing shortcomings in a timely manner, supplement and improve the business safety assessment process and guidelines, and further enhance China Telecom's IoT security protection and detection capabilities," says Yongpan Ren. "After the evaluation of the IoT devices, we found that a large portion of IoT devices had security vulnerabilities, such as no password or a weak password, or lack security certification. We will use our enterprise specifications and improve the security awareness to reduce the risks."

China Telecom says conducting the GSMA IoT Security Assessment is straightforward. "From the beginning until the end of the evaluation process, the GSMA Assessment scheme is clear and easy to implement," says Yongpan Ren. Through its use of the Assessment, China Telecom identified some gaps in its previous evaluation process and principles and has since improved its security protection and detection capabilities. "The GSMA IoT Security Guidelines contain important principles that need to underpin IoT security assessments," notes Yongpan Ren.

CASE STUDY

CHINA UNICOM

HIGH-LEVEL APPROACH TO IoT SECURITY

To prevent attacks on its IoT solutions, China Unicom takes an "exhaustive" end-to-end approach to security encompassing devices, its network, and cloud services, underpinned by a series of internal security reference books or operation manuals. "From the perspective of devices, we are using SIM cards, chips, modules, and endpoints jointly to perform authentication and encryption," says Fuzhang Wu, Principal Security Architect of China Unicom Internet of Things Co. On the network side, Unicom has created a data model to analyse the communication behaviour of IoT endpoints, which then triggers an alert or control command, if the system detects an abnormality. "From the perspective of the cloud, we are still focusing on the traditional data security, such as host, OS, network infrastructure, application and other components that could have potential risks," Fuzhang Wu adds. Unicom also cooperates with partners and customers to analyse and predict the security risks in different vertical sectors of the economy.

THE IMPLEMENTATION AND IMPACT OF THE GSMA IoT SECURITY ASSESSMENT

As the GSMA IoT Security Assessment collates expertise from global operators and IoT vendors, it covers almost everything in the IoT ecosystem, according to Unicom. "Both the GSMA Assessment and the Guidelines can help us to find the security gaps and quickly fix them, as these two documents have very excellent operability and correspondence," says Fuzhang Wu.

Unicom is using the GSMA Assessment to improve its IoT service reliability and define the security level of its IoT systems. "We use the GSMA IoT Security Assessment to evaluate our platforms, including the IoT portal, the authentication platform, and the open platform for IoT capabilities," explains Fuzhang Wu. It also recommends its customers use the Assessment to check their IoT products.

Unicom implemented the GSMA Assessment by collecting hardware, OS, third-party components, existing security measures and other

information on each of its IoT platforms. After making an initial evaluation on the basis of this information, Unicom conducted interviews with relevant people. The final step was to summarise the discovered problems and write the assessment report, including a description of the risks, the type of risk, the degree of impact, and the recommended remedies, referencing the GSMA IoT Security Guidelines.

"Through the GSMA IoT Security Assessment, we found some risks that we did not find when we did our initial security risk assessment," Fuzhang Wu notes. "For example, some local monitoring did not do the job, and the organisation-level process needs to be further strengthened and improved." Unicom says it has mitigated some security risks using the suggestions provided by the GSMA IoT Security Guidelines and improved the whole system's security.

Unicom has also integrated the assessment questions and checklist items in the GSMA IoT Security Assessment into its own checklist for future security risk assessments.

> *"We use the GSMA IoT Security Assessment to evaluate our platforms, including the IoT portal, the authentication platform, and the open platform for IoT capabilities"*

Fuzhang Wu, Principal Security Architect, China Unicom

CASE STUDY

ETISALAT

HIGH-LEVEL APPROACH TO IoT SECURITY

Etisalat, which has operations across 16 countries, is increasingly providing customers with complete "turnkey" IoT solutions. In some cases, the UAE-based operator group also operates these solutions, taking responsibility for the end-to-end security. "Three years back, when we started offering IoT solutions, security was customers' first question," says Khalid Shareef, Vice President Smart Solutions at Etisalat.

Etisalat employs encryption, firewalls, security protocols, such as TLS and AES, and other mechanisms to keep its IoT services as secure as possible. "Some of the solutions are mission-critical solutions for governments or closely tied into the processes of companies," notes Alberto Araque, Vice President, Internet of Things & Digital Payments, at Etisalat.

Etisalat's security labs in the UAE run tests on IoT equipment, before certifying these products for use in its solutions. The operator also incorporates security standards and guidelines, such as those from the GSMA, into its RFQ process: new products, services and solutions are evaluated using a "holistic" security checklist both in the design phase and prior to launch. Etisalat also shares best practices with fellow operators Singtel, SoftBank and Telefónica, helping to offer a managed security service that tracks threats in real time.

THE IMPLEMENTATION AND IMPACT OF THE GSMA IoT SECURITY ASSESSMENT

As it looks to deploy world-class IoT solutions, Etisalat believes it is important to harness the best resources, such as the security expertise being aggregated and distributed by the GSMA. "The GSMA Assessment takes an end-to-end approach and is constantly updated to highlight the crucial security issues, so we can tackle all of them," says Khalid Shareef.

Since it first adopted the GSMA IoT Security Assessment in the summer of 2018, Etisalat has used it to evaluate multiple platforms and solutions. For example, the operator is using the Assessment to evaluate the security of a public safety solution, involving the deployment of fire alarm systems in homes, overseen by the

Ministry of Interior in the UAE. The solution will see the rollout of approximately four million connected sensors in about 400,000 locations. "Using the GSMA Assessment, we found some areas where we can enhance the security," notes Alberto Araque.

The GSMA Assessment has also prompted Etisalat to make changes to a smart transportation system it is developing. "The Assessment found some direct connectivity between the normal public Internet and the core of the solution," says Khalid Shareef. "So we have changed to a more secure channel using a VPN." More broadly, the robustness and completeness of the GSMA's collateral is helping to bolster customers' willingness to adopt Etisalat's IoT solutions for sensitive applications. "The Assessment is helping us to deploy video surveillance solutions with banks, airports, export agencies and others," adds Alberto Araque. "That could not happen without security: customers, many of which are government agencies, need to have full confidence in the solution."

As more and more IoT players follow the GSMA Guidelines, Etisalat has found it straightforward to align its standards with those of its primary vendors. For example, the widespread adoption of the GSMA's recommendations is driving alignment in key areas, such as equipment identification, authorisation and authentication, and data protection, Khalid Shareef explains.

> *"The Assessment is helping us to deploy video surveillance solutions with banks, airports, export agencies and others"*
>
> **Alberto Araque,** Vice President, Internet of Things & Digital Payments, Etisalat

CASE STUDY

KDDI

HIGH-LEVEL APPROACH TO IoT SECURITY

KDDI, one of Japan's leading mobile operators, believes the widespread adoption of the IoT depends on dealing with security issues, such as unauthorised remote control and eavesdropping of data. KDDI evaluates the security of its IoT services using an in-house checklist that draws on the Japanese government's security guidelines and covers networks, devices and IoT solutions. KDDI says the checklist encompasses the GSMA IoT Security Assessment, but is more specific. "Every time we purchase carrier communication equipment from outside vendors, we check the items against our list," says Keigo Harada, General Manager, Head of IoT Business Planning Department.

KDDI will start offering a worldwide IoT platform from 2019, spanning everything from connectivity to data analytics. Underpinned by its in-house checklist, this platform will enable KDDI's corporate customers to benefit from IoT connectivity and related services in many different countries.

THE IMPLEMENTATION AND IMPACT OF THE GSMA IoT SECURITY ASSESSMENT

KDDI supports standardisation activities. Drawing on its experience of conducting rigorous security check items and security self-audits of new products, KDDI contributed to the development of the GSMA IoT Security Guidelines and Assessment. KDDI has since analysed the differences between the check items in the GSMA IoT Security Assessment and its own checklist to confirm that all the necessary items are included in the KDDI checklist.

KDDI says the expertise shared through the GSMA provides its members with a valuable global perspective on IoT security. "The GSMA brings the experience and knowledge of a large number of global operators, which is very useful for customers and partners that are developing their business globally, such as automotive companies," says Keigo Harada.

KDDI believes the GSMA IoT Security Guidelines are particularly valuable for the many companies operating in the IoT market that are not familiar

with telecommunications. KDDI welcomes the fact that the GSMA IoT Security Guidelines have been published on the web separately in four documents (an overview document, and three documents aimed specifically at IoT services, devices, and network operators) in Japanese, as well as English. "We also hope that if the security level of developing countries improves through the Guidelines, that will drive the global expansion of the IoT business," says Keigo Harada. "Significant incidents are taking place all over the world, and interest in the security of the IoT is increasing."

> *"We also hope that if the security level of developing countries improves through the Guidelines, that will drive the global expansion of the IoT business"*

Keigo Harada, General Manager, Head of IoT Business Planning Department, KDDI

CASE STUDY

OMANTEL

HIGH-LEVEL APPROACH TO IoT SECURITY

The largest mobile operator in Oman, Omantel (GSMA Intelligence, 2019), sees IoT security as a combination of securing the network, the logical assets, such as software, intellectual property, documentation, data-in-motion and data-in-rest, and the customer equipment. "Our internal processes allow the corporate security department to have end-to-end visibility on implementation of all new systems deployed in Omantel, including IoT," says Muhammad Moqeet ur Rab, Senior Manager, Security Architecture & Operation at Omantel. "I see IoT security assessment as an offshoot of the wider network assessment practice, however, in a tailored manner."

All of Omantel's suppliers are contractually obliged to implement a set of minimum security controls to adequately protect Omantel-owned data and data about Omantel customers that is transferred, processed or stored on the supplier's infrastructure, together with the systems and services it deploys on behalf of Omantel. Later in the procurement process, Omantel's corporate security team shares recommendations with suppliers on how to design and deploy the solution in a secure way. Finally, during the acceptance testing, the operator's corporate security specialists verify that all the new systems and services have been installed in line with given recommendations.

THE IMPLEMENTATION AND IMPACT OF THE GSMA IoT SECURITY ASSESSMENT

Omantel believes that a consistent approach to IoT security is required to ensure suppliers and customers appreciate the magnitude of the security risks in the IoT ecosystem. "Having a deep and full understanding of challenges related to security of the IoT, as well as issues that arise from unregulated and non-standardised approaches to security problems, Omantel has decided to embrace and follow the GSMA IoT Security Guidelines," says Muhammad

Moqeet ur Rab. "The guidelines are very well structured, and provide the necessary capabilities to evolve along the security path."

As the Guidelines and Assessment draw on the expertise of operators around the world, they address technological advances and emerging threats, he adds. Omantel, which was closely involved in the development of the wider GSMA fraud and security framework, is hosting a meeting of the working group in Oman early in 2019. "Our ICT team has been actively involved in this whole process for them to get a better understanding in designing the services portfolio," adds Muhammad Moqeet ur Rab.

Omantel is in the early stages of developing its IoT solutions portfolio, which will initially focus on the smart metering and smart home markets. Working with its suppliers, the operator is integrating the GSMA IoT Security Guidelines and Assessment into the solution development process. "We have had a fairly comfortable experience in implementing the assessment process as it came in at a very early stage in the design of our services portfolio," says Muhammad Moqeet ur Rab. "Implementing the assessment process at the beginning is helping us design our services, keeping the Guidelines in perspective."

He also notes that the adoption of the GSMA framework is providing Omantel's corporate customers with a lot of assurance, which is giving the operator a competitive advantage in Oman's emerging IoT market. Muhammad Moqeet ur Rab expects demand for IoT solutions to grow rapidly in Oman, leading to a significant increase in traffic on Omantel's networks.

> *"Having a deep and full understanding of challenges related to security of the IoT, as well as issues that arise from unregulated and non-standardised approaches to security problems, Omantel has decided to embrace and follow the GSMA IoT Security Guidelines"*
>
> **Muhammad Moqeet ur Rab,** Senior Manager, Security Architecture & Operation, Omantel

CASE STUDY

ORANGE

HIGH-LEVEL APPROACH TO IoT SECURITY

Orange Business Services, part of multinational group Orange, has an extensive IoT offering, spanning much of the value chain. Orange says it manages 14.8 million connected objects each day and processes more than 330 million pieces of data every minute. It has an online and print catalogue of certified connected objects that it has sourced, tried and tested. Orange carries out end-to-end security tests on all the IoT products and solutions sold through its distribution channels or branded Orange. The operator also has its own cyber-security unit that sells security services.

THE IMPLEMENTATION AND IMPACT OF THE GSMA IoT SECURITY ASSESSMENT

Orange says the GSMA IoT Security Assessment makes it very clear how important it is to take an end-to-end perspective, helping to frame internal processes and discussions with its partners. "It is a way to ask good questions of the overall security of the platform, to check every security measure," says Ivan Lovric, IoT Expert and IT Security Specialist, Orange Group.

Orange has used the GSMA Assessment to evaluate its Live Objects IoT platform, which was launched in 2016 and is designed to enable customers to safely collect and store the data being generated by their IoT devices. A wide range of devices can be connected to the platform using different kinds of networks, via application programming interfaces (APIs). "It is one of the most important Orange IoT products," notes Ivan Lovric.

The assessment, which took about 10 man days, showed the security of the platform is sufficient for the short term, but needs to be continually improved to meet security requirements for the medium term. "The GSMA IoT Security Guidelines allowed us to define new kinds of implementation of security measures," says Ivan Lovric. Orange is continuously maintaining the

security of the Live Objects IoT platform to meet the requirements of the ISO standards and the new GDPR, as well as to achieve full alignment with the GSMA Assessment.

In future, Orange may also use the GSMA Assessment to evaluate other IoT products and services, including its cellular networks and individual devices, while also integrating the process into its software development lifecycle.

> *"The GSMA IoT Security Guidelines allowed us to define new kinds of implementation of security measures"*

Ivan Lovric, IoT Expert and IT Security Specialist, Orange Group

CASE STUDY

SK TELECOM

HIGH-LEVEL APPROACH TO IoT SECURITY

SK Telecom, the largest mobile operator in Korea (GSMA Intelligence, 2019), applies security-by-design principles to its IoT products and services. It also implements various security management processes, such as a security assessment, before launching a product or service, and penetration testing after launch, together with continuous security monitoring.

However, as SK Telecom works with many partners in devices, network operations, and service platforms, it acknowledges that end-to-end (E2E) security can be complex and difficult to achieve. To address this challenge, the operator has published an IoT security whitepaper and developer-friendly guidelines and assessment requirements. "We believe they are key factors of E2E security... developers are a significant factor in IoT security and, if they understand our security guidelines, that will achieve the IoT security that we want to reach," says Sungkyu Cho, IT Security Manager. "For these reasons, we designed our guidelines technically, but simply, so developers can read them easily." The operator reviews and updates its guidelines and checklists annually to make them simpler, more valuable and more up-to-date.

THE IMPLEMENTATION AND IMPACT OF THE GSMA IoT SECURITY ASSESSMENT

SK Telecom says the GSMA IoT Security Assessment provides an entire framework for IoT security, adding that it brings an E2E perspective that had been missing from its own security guidelines, which covered discrete elements, such as network operations, elements of IT infrastructure and IoT devices. "Infrastructure-centric security guidelines and processes are well-defined, but IoT security was not, so we focused IoT security from an end-point perspective," adds Sungkyu Cho. "Traditionally, our assessment overlooked the E2E perspective, so it is helpful for us to enhance our security guidance."

SK Telecom has used the GSMA Assessment to check its M2M router product, which supports SIM-based authentication and connections to the operator's legacy networks. The assessment found that an additional management port could be accessed by anonymous actors. "We found (the weakest) default password was installed on the device and it allows root privileged access from the Internet," Sungkyu Cho explains. "It was a kind of management port, and the vendor had a need to access it when the device was corrupted." In line with the GSMA IoT Security Guidelines, SK Telecom advised the vendor to apply two-factor authentication or a stronger authentication mechanism, such as VPN. "As there were many problems like time to market, cost and resource, and update schedule, we decided to apply a device-unique password, rather than a single password," Sungkyu Cho adds. "The latter is easier for the customer, but if an attacker obtained the password, all devices could be compromised."

SK Telecom is now considering how to integrate the GSMA Guidelines on supply chain security, TCB (Trusted Computing Base) and tamper resistant features into its own process and checklists.

> *"Infrastructure-centric security guidelines and processes are well-defined, but IoT security was not, so we focused IoT security from an end-point perspective"*
>
> **Sungkyu Cho,** IT Security Manager, SK Telecom

CASE STUDY

TELEFÓNICA

HIGH-LEVEL APPROACH TO IoT SECURITY

Telefónica, which has operations across Europe and Latin America, takes an end-to-end approach to IoT security, spanning devices, networks and platforms. "The fragmentation of devices is really a new element with IoT," says Vicente Segura, Head of IoT Security at Telefónica. "You have everything from IP cameras to highly personal devices, such as watches and telematic control units in cars, while the communications modules inside the devices and chipsets are provided by different manufacturers. There could be ten players in a supply chain."

In response, Telefónica is creating a methodology in which security is built in from the start, by including a set of security requirements during the RFI and RFP processes. "We also do a technical security audit of the products and services we plan to launch, to make sure there are no critical vulnerabilities," adds Vicente Segura. "A team of experts performs audits on the services."

Besides ensuring that its own IoT services are secure, Telefónica is also working on an IoT security value proposition for its B2B customers. This value proposition is composed of three services: secure device authentication leveraging the SIM, an IoT threat detection service, which can detect anomalies in patterns of communications, and DNS-based blocking service when a device is making a request for a malicious domain. The operator also supplements these offerings with consulting and auditing services.

THE IMPLEMENTATION AND IMPACT OF THE GSMA IoT SECURITY ASSESSMENT

Vicente Segura says the GSMA IoT Security Assessment meets the "clear need for a reference guide to approaching IoT security in a holistic way. There is extensive literature on security, but IoT requires an end-to-end approach. You can look at references for each of the components, but you need to handle several references. The GSMA Guidelines compile all that information in a single set of documents and simplify the application with a checklist."

Telefónica has used the GSMA IoT Security Assessment to evaluate a diverse array of IoT solutions, including personal IoT services for tracking assets, smart meters and even the sophisticated

marine traffic management system deployed by the port of Seville as part of the Tecnoport 2025 project[2]. Telefónica typically performs a risk assessment first, focused on the key sections in the GSMA Assessment, before doing a complete assessment. It also uses a scoring system to summarise the security of the solution for managers.

"The assessment process has also raised awareness among our partners," adds Vicente Segura. "It has forced them to start thinking about the key risks in supply chain security: most of the partners with whom we deploy IoT services don't manufacture the devices, but they have to make sure that the device provided by their partners is secure. They now deploy secure operations in order to access that device and look to block the device, if it is tampered with."

> *"There is extensive literature on security, but IoT requires an end-to-end approach. You can look at references for each of the components, but you need to handle several references. The GSMA Guidelines compile all that information in a single set of documents and simplify the application with a checklist"*
>
> **Vicente Segura,** Head of IoT Security, Telefónica

[2] www.gsma.com/iot/securing-port-future

CASE STUDY

TELENOR

HIGH-LEVEL APPROACH TO IoT SECURITY

The specialised IoT company within the Telenor Group, Telenor Connexion provides multinational enterprise customers with global connectivity and cloud services. In addition to supplying the necessary machine-to-machine (M2M) SIM cards, custom billing profiles and custom roaming profiles, Telenor Connexion also offers Managed IoT Cloud (MIC), a secure cloud platform for device and data management, which generates insights about connected products.

Although it doesn't demand customers adopt specific security mechanisms, Telenor Connexion does offer private APNs that enable the customer to use a VPN, as well as advising customers on encryption.

"Our customers are not always asking about security, but whatever their security engagement level, we want to take them in that direction," says Ben Tyson, Business Security Officer at Telenor Connexion. "You don't stick a Windows PC anywhere near the Internet without a firewall and anti-virus, but occasionally there still seems to be some kind of surprise that you can't just connect an IoT device to the Internet without securing it first. Change is happening though: customers are becoming more and more aware of the need for security and the need to take action."

THE IMPLEMENTATION AND IMPACT OF THE GSMA IoT SECURITY ASSESSMENT

Telenor Connexion finds the holistic nature of the GSMA IoT Security Assessment valuable. "It provides a way of seeing everything that anybody has ever experienced," says Ben Tyson. "No matter how many people are on your security team, and no matter how much you read blogs and use social media, you still can't cover everything. With the GSMA Assessment, you have access to a wide range of expert knowledge. Some of the topics may not be relevant to your particular product or service, but a comprehensive security assessment is valuable to make sure nothing is forgotten."

[2] Source: https://www.orange-business.com/en/solutions/iot

Telenor Connexion also supplies the GSMA IoT Security Assessment and Guidelines to its customers, enabling them to pick out the things that are relevant to them. Internally, the operator has used the Assessment to evaluate the security of its connectivity and its Managed IoT Cloud (MIC) product, which allows users to view, manage, and analyse data from their products, as well as interacting with them. "We went through it, picked up odds and ends that we missed," says Ben Tyson. "We didn't see any major issues, but it does help our security architects and it helps to build confidence: you know what you are doing is the right thing, as we have now checked it against hundreds of other people's knowledge."

> *"No matter how many people are on your security team, and no matter how much you read blogs and use social media, you still can't cover everything. With the GSMA Assessment, you have access to a wide range of expert knowledge"*

Ben Tyson, Business Security Officer, Telenor Connexion

CASE STUDY

TURKCELL

HIGH-LEVEL APPROACH TO IoT SECURITY

Although the IoT market in Turkey is still in its infancy, it is developing fast. Turkcell is fuelling that growth by providing customers with complete end-to-end IoT solutions, as well as connectivity. As the operator develops these solutions in conjunction with partners and vendors, it requires its suppliers to follow the GSMA's IoT Security Guidelines. It has integrated these guidelines into its product security analysis, request for proposal (RFP) and procurement processes for all IoT related projects. Turkcell also conducts a security evaluation, as part of its acceptance process for new products and services.

THE IMPLEMENTATION AND IMPACT OF THE GSMA IoT SECURITY ASSESSMENT

As Turkcell began to ramp up its IoT business in 2018, the operator adopted the GSMA's IoT Security Assessment as a framework to ensure its solutions are robust and secure. "We implemented the GSMA IoT Security Assessment to kick start the IoT security work within Turkcell and ensure an industry-accepted level of security for our IoT services," says Ahmet Eker and Saime Aydın, Information Security Experts, at Turkcell. "It's a comprehensive list and some of the requirements are not applicable for our IoT products, as yet, so we need to do some customisation based upon each product's security risk assessment." Still, the breadth and depth of the GSMA IoT Security Assessment means Turkcell doesn't need to employ any other checklists or security evaluation processes.

Turkcell is using the GSMA IoT Security Assessment to evaluate its existing IoT solutions, as well as new products and services under development. "We are evaluating the solutions we already offer and if we find some gaps, we ask the vendor to fix them," says Saime Aydın. For example, it has assessed its new Supercam service, which enables householders or building managers to view live footage from internal cameras. The footage is relayed via Wi-Fi to a Turkcell-run data centre. After completing the security assessment, Turkcell provided feedback to the vendor and asked for modifications to

enhance the current security level. "The GSMA Assessment opened up a new view on security," notes Ahmet Eker.

The operator is also using the GSMA IoT Security Assessment to evaluate its Kopilot service, which enables consumers to track the location of their vehicles, as well as metering solutions aimed at the energy and agricultural sectors. Turkcell is also planning to use the Assessment to help secure the smart city projects it is working on with municipalities and new solutions to meet rising demand from industry and agriculture. "2019 will be a fruitful year for the IoT in Turkey," says Saime Aydın.

Although it took some effort to educate the business on the value of the IoT Security Assessment, Ahmet Eker says Turkcell's related IoT business owners have now bought into the concept and are proactively initiating the process. "The assessment process has created an IoT security awareness within Turkcell and our partners, including business and service owners, vendors and upper management," he adds.

> *"The GSMA Assessment opened up a new view on security"*
>
> **Ahmet Eker,** Information Security Expert, Turkcell

CASE STUDY

VERIZON

HIGH-LEVEL APPROACH TO IoT SECURITY

Based in New York, Verizon provides IoT solutions and other services to enterprise customers around the world. To safeguard security, Verizon aims to deliver a "chain of trust" encompassing devices, connectivity, data, transactions, applications, platforms and authentication. Following its own dedicated methodology, Verizon employs an array of tests to ensure the security of an IoT solution is appropriate to the application and use case.

"We cover all the different segments, we do penetration testing, we check the OS and implement patches," says Bharadwaj Pulugundla, Manager IoT Strategy and Innovation at Verizon. "We only source devices from trusted manufacturers. We look at the encryption technologies and where the data is stored. We also look at the physical security of a device in a public place." As well as maintaining the security of its own networks, Verizon considers other forms of connectivity used by the solution, including short-range technologies, such as Bluetooth. It also verifies how the IoT platform registers each device. It supplements these processes with a certification system, application testing and ethical hacking to test whether it can break into the application.

"In some use cases, you need to focus on the device," adds Bharadwaj Pulugundla. "For example, in the case of monitoring a patient in hospital, there is no room for error. You can't have the data corrupted. People are very excited about what all these services and devices can do, but they are not aware of the potential threats. With the IoT, there are more opportunities for hackers to break in – you have so many end-points. If you can compromise any of the end-points, then you have access to the network."

THE IMPLEMENTATION AND IMPACT OF THE GSMA IoT SECURITY ASSESSMENT

Verizon is integrating the GSMA IoT Security Guidelines and Assessment into its enterprise propositions, encouraging customers to use these tools to evaluate the overall security of their IoT deployments. For example, Verizon is working with a customer to use the GSMA framework to review the security of a totally automated retail store, which uses sensors to

enable people to check out automatically. Bharadwaj Pulugundla says that two Verizon customers in the logistics market, where connected sensors are used to monitor shipping containers, are also employing the GSMA Assessment to ensure their deployments are secure.

"I believe security should be approached in a comprehensive way," explains Bharadwaj Pulugundla. "You also need to look at security from a maturity point of view and you need to draw on up-to-date documentation. That is where the GSMA IoT Security Assessment comes in. It asks the right questions, such as: Do you have privacy management in place? It is a very interesting and useful framework. It brings a level of comprehensiveness that creates value."

Verizon also believes the GSMA toolkit can play a role in raising awareness of the importance of security among its customers. "We are educating the customer with the framework and the checklist, so they understand the importance and that robust controls are required," says Bharadwaj Pulugundla. "In the case of business-critical applications, depending on what the requirements are, you can establish controls. You can use the checklist as a self-diagnostic tool."

> *"With the IoT, there are more opportunities for hackers to break in – you have so many end-points. If you can compromise any of the end-points, then you have access to the network"*
>
> **Bharadwaj Pulugundla,** Manager IoT Strategy and Innovation, Verizon

CONCLUSIONS

As mobile operators and their partners develop and deploy an increasingly diverse array of IoT products and solutions, they are grappling with a wide range of security challenges. The roll out of new low power wide area connectivity is making it viable to connect everything from highly personal devices, such as wristbands and watches, to sensors monitoring industrial machinery. As a result, the fast expanding IoT market is now served by many thousands of hardware and software companies using many different communications modules from multiple manufacturers: the value chain can be long and complex. Furthermore, many new connected devices rely solely on battery power, limiting the local processing power available for security and authentication processes.

In this multi-faceted and fast-moving market, the GSMA IoT Security Guidelines and Assessment are providing a robust and holistic framework for IoT security. Mobile operators say they bring an end-to-end perspective that can be missing from their own security guidelines or alternative assessment processes: there had been a tendency to consider the security of the various elements of an IoT solution, such as the network, the platform or the end-device, in isolation. The comprehensive nature of the GSMA Guidelines and the Assessment is helping to build confidence in IoT solutions, prompting governments to commission mobile operators to deploy new public safety solutions, such as the fire alarm system in the UAE.

Mobile operators have already used the GSMA IoT Security Assessment to evaluate a wide range of products and solutions, including their proprietary IoT platforms, which generally enable customers to safely collect and store the data being generated by their IoT devices. Orange, for example, used the Assessment to evaluate its Live Objects IoT platform, a process that took 10 man days. Some operators, such as China Mobile, are using the Assessment to evaluate the security of new low power wide area networks, which generally involve the deployment of many compact, low-cost devices, such as NB-IoT-connected smoke detectors and cameras for monitoring home security. In some cases, the Assessment highlighted vulnerabilities in existing solutions, while the Guidelines have provided a clear and robust way to remedy these flaws. China Unicom, for example, reported that the GSMA Assessment and the Guidelines have helped it find the security gaps in its solutions and quickly fix them.

The Assessment is also helping to raise awareness of the value of security among senior managers both inside mobile operators and within the broader value chain. Rather than having to be cajoled into implementing security processes, many product developers and project leads are proactively following the GSMA Guidelines and Assessment process.

As more and more IoT players follow the GSMA Guidelines, mobile operators say it is becoming increasingly straightforward to align their standards with those of their primary vendors in key areas, such as equipment identification, authorisation and authentication, and data protection. Some operators, such as AT&T, highlighted the value of the GSMA Guidelines and Assessment to start-ups and companies that are new to the IoT market. For such players, the guidelines can be an important source of clear and comprehensive information on how to design security into a new IoT device or solution.

Download the GSMA IoT Security Guidelines and IoT Security Assessment for free at

gsma.com/IoTSecurity

For more information please visit:
www.gsma.com/IoT

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