Embedded Mobile (M2M) - Telecoms Fraud & Security Management

A Præsidium Business Consultancy White Paper

JULY 2011

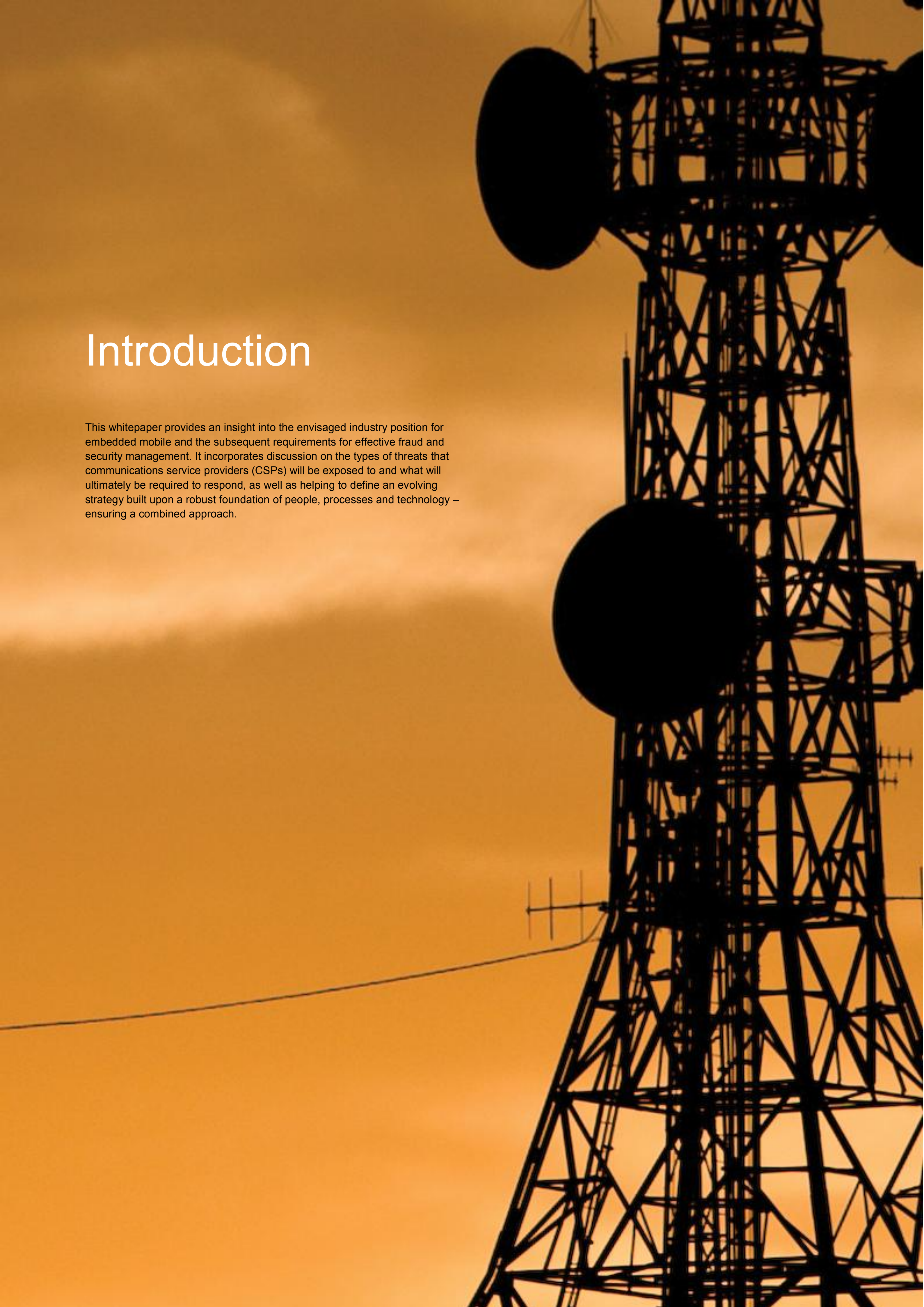
WeDo technologies
Assuring your Business for the Future

præsidium
WeDo technologies • Consulting division

Table of Contents

Introduction

This whitepaper provides an insight into the envisaged industry position for embedded mobile and the subsequent requirements for effective fraud and security management. It incorporates discussion on the types of threats that communications service providers (CSPs) will be exposed to and what will ultimately be required to respond, as well as helping to define an evolving strategy built upon a robust foundation of people, processes and technology – ensuring a combined approach.



Background

Embedded Mobile (EM) refers to a host of devices and services using wide-area mobile network technologies to provide communications between machines themselves (machine-to-machine, or M2M) and also with people. Wireless devices for M2M communications based on 3rd Generation Partnership Project (3GPP) technologies such as GSM, 3G, HSPA and LTE are intended to grow exponentially over the next 2 – 3 years.
The GSMA's forecast is that connected devices with a SIM will exceed 500million.

Embedded solutions will encompass a range of devices and end to end services involving consumer electronics, business enterprise, automotive, industrial/utilities and medical industries. The demand and requirements for this progression of service delivery are eagerly awaited by both CSPs and their respective business partners, which will result in the formation of more strategic partnerships. This increased reliance on third party providers brings with it a new risk perspective. CSPs must therefore consider the implications and requirements to enable them to minimise exposure to fraud risks associated with Embedded Mobile devices, applications, processes and different business models. Due to the extensive range of host devices, configuration requirements and the fact that embedded devices will be mass deployed and used in unguarded and possibly unprotected locations, it will be impractical to simply apply the more traditional security and fraud countermeasures used in mobile communications to date.

Fraud and revenue risks associated with M2M may mean different things to different people depending on where they reside within the product and service delivery chain. Essentially, the fraud management professional will need to consider what new fraud risks are introduced when developing and deploying EM devices or services. They should consider and evaluate from a risk perspective what elements of their existing fraud type exposure will increase (or decrease) as a result of EM device or service deployment. This will be a fundamental requirement when considering the fraud management coverage of the CSP products and services portfolio and the fraud strategies that are to be defined.

"“...M2M communications are intended to grow exponentially over the next 2-3 years”

As evidenced by recent high profile fraud and security incidents and breaches, the criminal fraternity are becoming more innovative, deploying new and more focused techniques for obtaining exactly what they want from the services and products they target. M2M will be no exception. CSPs must never become complacent or forget that these highly organised fraudsters operate their own businesses and need to “service” their own customers. Their business model for committing fraud spans all types of technology and crosses international boundaries, and has traditionally relied heavily on the CSP's inability to respond and recover in a timely manner. It is this aspect that they will again look to prey upon. Therefore one of the essential business requirements for CSPs will be ensuring clearly defined fraud, security and risk protection models for M2M. It will be essential to continually consider the risk and not become complacent. In other words, performing a single action to assess the fraud risk, but ensuring that risk is continuously assessed as M2M device and service deployment evolves. CSPs must not rely simply on existing practices to protect these new and varied revenue streams but will need to consider end to end fraud management requirements, including the new third party relationships.

What will be offered and who owns the risk?

In recent years, the telecoms industry has witnessed even more interaction and alignment with the financial services sector relating to m-banking and m-commerce and has needed to consider ownership and accountability for fraud control. The position over "customer responsibility" has been unclear in certain frauds such as SIM Swap, resulting in considerable bad publicity for the CSP when the actual fraud relates to a compromise at the bank. Unfortunately, the consumer only sees the method of fraud being the SIM. The requirement for protecting the CSP will therefore need to be further extended with M2M due to the range of new markets and business partners entering into the arena – vehicle manufacturers, insurance providers, utility and medical businesses, vending machine suppliers, etc.

In automotive, for example, the M2M features envisaged will relate to breakdown call (bcall), emergency call (ecall), pay as you drive insurance, stolen vehicle tracking, speed monitoring between fixed points and providing all forms of in-car entertainment. There will be associated data protection requirements from a security perspective and for fraud the criminal fraternity will be looking to determine how they can capitalise on these new initiatives. The attractiveness might not simply be based upon obtaining fraudulent service or avoiding payment for entertainment features received for example. The risk could be extended to compromising a person's medical records by unscrupulous insurance investigators looking for evidence in an insurance claim or using vehicle tracking capabilities to identify the whereabouts of a person under some other type of investigation, but outside the legal considerations for that service.

"...well organised and financed criminal gangs will be assessing what the boundaries are for providing M2M and looking to identify the "softer and easy target" …

It will therefore be vitally important for CSPs to appreciate where their responsibility begins and ends for securing the delivery of services that they are directly responsible for providing. Recent experiences in the UK of unlawful interception of voicemail services has received very high profile and negative publicity within the media and resulted in criminal investigations. With M2M, there could be a risk of a service being offered for "home protection" that is compromised; and the criminals actually identifying when the property is empty rather than secure or effectively intercepting the alarm signal and disabling the transmission path. Alternatively, they may be able to obtain "footage" of a high profile customer's home environment and sell this to the media. Consumers will only remember how the service is provided by telecoms technology (if and when compromised) and not consider that the CSP might not be the actual service provider or device owner.

Well organised and financed criminal gangs will be assessing what the boundaries are for providing M2M and looking to identify the "softer" or "easy targets" to maximise their revenues. Telecoms fraud has climbed steadily over the years, with the level of concerted fraudulent attacks as opposed to opportunistic ones actually increasing rather than decreasing. The introduction of innovative solutions and services for M2M will serve to further fuel the greed of the criminal fraternity.

Types of Fraud & Security Attacks & CSP Requirements

The CSP will need to evaluate the level of risk by initially defining some basic areas to be subjected to a risk assessment. For example; radio interface (communication path), provisioning, authentication (device & customer), actual product security, attended/unattended devices, operational control, device management, privacy and confidentiality of information. The types and severity of fraud attacks for M2M will primarily revolve around the market environment that the CSP operates within and will also relate to the range of products and services actually offered or being considered. The fraudsters' modus operandi will likely follow some tried and tested techniques or look to exploit new vulnerabilities evidenced from the technology or devices used. For the core network protection, the security threat could take the form of impersonation of devices, traffic tunneling between impersonated devices, and firewall mis-configuration specific to the modem, router or gateway or attacks against the radio network being committed by rogue devices.

It will be vitally important for CSPs to consider how services are actually being provisioned, so controls and requirements for ensuring provisioning assurance will be essential in providing the fundamental basis for securing devices and the associated services. In addition, due to the nature of the product being offered, embedded mobile devices will often be left unattended - increasing the risk of attack. This position could result in them being more vulnerable to tampering as a criminal could be motivated to tamper with an EM device in order to fraudulently obtain mobile service (i.e. the removal and use of the Universal Integrated Circuit Card (UICC) in an alternative mobile device). Fundamentally, the UICC serves to ensure the integrity and security of all kinds of personal data and will therefore be a possible target for the fraudsters.

Due to their remote location and unattended deployment, the risk of physical attack could also increase to facilitate insertion of valid authentication tokens into a manipulated device, inserting or booting with fraudulently modified software (re-flashing), or straightforward theft once the devices have been operationally deployed. Protection will require validation of the integrity of M2M device software, data and authentication and some level of physical protection.

Attacks against unattended devices were recently highlighted by experiences in South Africa when fraudsters targeted high tech traffic lights fitted with SIMs, used to alert the road traffic agency to faults. Fraudsters stole more than 400 SIMs and made calls costing thousands of USD via a systematic and co-ordinated attack. The modus operandi would have definitely required "insider" knowledge to ensure the fraudsters targeted the correct traffic lights, but the big question is, did the CSP and their partner (the road traffic agency) determine the fraud risk prior to installation? For embedded mobile, ensuring the provisioning process is secure will be paramount and in this case the SIMs could have been provisioned to only contact one designated number to reduce exposure to airtime fraud.

Fraudsters could also look at identifying a means of suppressing payment or usage-related messages being sent from the EM device, for example, relating to a road toll charging system or interfering with information being generated from a utility meter. Due to the devices being unattended, this could result in unauthorised use of EM devices going unnoticed for longer compared to more traditional mobile devices.

There will be a requirement for remote provisioning and for re-provisioning mechanisms to support these business models and the usage scenarios associated with EM. During product development CSPs will need to consider the associated risks and define the required fraud and security controls. Remote provisioning solutions will involve the transfer of operator credentials to the UICC outside their secure and trusted environment. Therefore, where these highly sensitive credentials are not adequately secured as part of the generation, storage and transfer process, there will be an opportunity for subscription cloning against the CSP. In addition, any weaknesses within the mechanism used for remotely upgrading security credentials, or in the configuration of UICC security algorithms within the EM device, could result in the device being compromised. The risks associated with this type of attack are likely to be either financially based or directly impact the CSP's brand and image. In some instances, where the customer witnesses a bad experience using the services, this will have a greater impact on the CSP.

Due to the actual EM deployments, the risk of being targeted by malware (similar to what is already experienced in telecoms devices), will also pose a threat. The level of malware risk will be dependent on the EM application and device interfaces, while the range of risks will vary considerably so the CSP must consider exactly what level of protection is in place. For example, within the utilities industry, EM-enabled utility meters could be "sealed" and only allowed to communicate with the designated utility company. This approach would provide more protection as opposed to consumer gaming devices that support application download and installation, making them more prone to malware attack and directly impacting on the whole customer management process. Consumer education will be an essential part of the experience. Also, as part of the provisioning risk, consideration will need to be given to ensuring malware is not introduced on the UICC via applications introduced erroneously or maliciously as part of the remote provisioning process.

CSPs will need to determine how, once provisioned and using the service, a customer has the ability to change their subscription or, alternatively, how they can actually select their preferred CSP once the M2M device has been remotely provisioned by a third party provider. For example, motor vehicles will already have the embedded device at the point of manufacture. M2M customers may also wish to churn to an alternative CSP, so any associated risks for ensuring safe transition will need to be assessed.

There will always be the more traditional types of attack to consider, stemming from the criminal fraternity's infatuation with targeting telecom services and customers. Primarily this could relate to Denial of Service attacks (DoS) directly against the EM devices and services where the fraudsters will, based upon the large number and variation of devices, seek out and target those that are insecure. There will also be the threat from a distributed DoS attack targeted directly at a CSP or partner's customer services where large numbers of terminals with a similar configuration are targeted. The threat of a malicious attack via a remotely operated botnet (a collection of infected devices that have been commandeered by hackers) could take place. It will be imperative within the application design stage to consider the threat from DoS attacks, considering the actual extent, level of risk and resulting impact. For example, distributed DoS against the emergency services during a major incident would be considered as being very high impact and damaging for the CSP.

As already accepted by CSPs, they have a responsibility for storing and managing highly sensitive and confidential data associated with their customers and business partners. Consideration will need to be given as to how these new devices will be secured to maintain the integrity of the information held or exchanged with their partners. EM devices and applications will be collecting large volumes of information that will be possibly classed as "confidential and private", and any breach of security or wrongful disclosure could significantly impact the CSP brand image and result in regulatory or legal action taking place. Data and privacy protection risks will include the potential for eavesdropping on other users, a device's data being transmitted over 3G or LTE by the criminal masquerading as the customer's device, or network ID and information being subsequently provided illegally to third parties.

The CSP must also consider any additional requirements relating to supplying information to law enforcement agencies and their obligations for lawful interception. There is no doubt that with the extent and level of these "new" information sources, increased demand will be placed on the CSP to support these external agencies. For example, from a criminal investigation perspective, there will be invaluable intelligence to support the investigative process. This wealth of new intelligence could potentially relate to a motor vehicle's travel history – date, route taken, timings at a specific location, for instance, or alternatively energy consumption at a private or commercial premises to identify links to involvement in harvesting drugs. Based on these new intelligence sources, CSPs will need to consider exactly what their obligations to law enforcement will entail and what will be required to actually fulfil any legal obligations.

The progression to M2M will also introduce new device manufacturers and application providers that the telecoms industry has previously not worked with and who don't understand the risks; as witnessed with the new round of mobile providers. This will result in additional security and fraud risk as these "trusted" parties will need to be audited to ensure the levels and expectations of the CSPs are being applied. So a similar position to the very successful GSMA Security Accreditation Scheme (SAS) for SIM card manufacturers may need to be considered for EM devices. CSPs must ensure that their third party providers and business partners are audited by industry professionals and not simply rely upon some other non-telecom industry body certification.

As with all products and services provided by the telecom sector, there will be the inherent risk of internal fraud either at the CSP, device supplier or business partner level, and this could relate to compromised security credentials, deliberate mis-configuration attacks or theft/sale of software for malicious activity.

Considerations for a Successful Risk Management Strategy

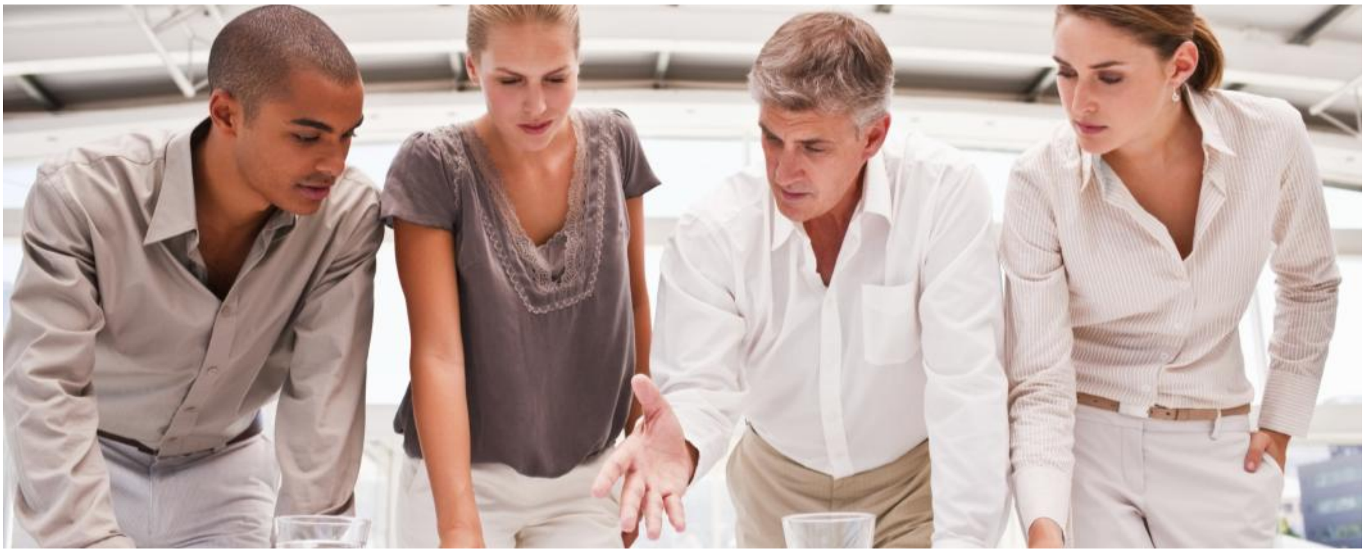
CSPs have business plans in place to determine the innovative products they will provide via M2M to the respective customer segments (corporate, business and residential and via third party relationships). The criminal fraternity will also be actively determining their own "business strategy" for defrauding what is provided. Due to devices primarily being un-guarded and mass deployed, and taking into account the extent of services they will provide, these wireless communication architectures and device solutions will attract new security and fraud threats.

CSPs should identify within their strategy exactly what can result from failures within the technology, methods used to deploy and deliver the M2M services or avoid simply failing to evaluate the benefits fraudsters will gain from attacking the services. Concerns already being expressed in the industry over the varying level of risk will mean that there will be no single solution to fraud and security risk for CSPs formulating their defence mechanisms. What is needed is a balanced approach taking technology, people and processes working together to create an effective strategy. As part of the product and service lifecycle, the fraud and security functions will need to be directly involved in performing "product and services risk assessments" that are ultimately linked to defining the required strategies.

> "...The criminal fraternity are also actively determining their own "business strategy" for defrauding what is provided…"

The following areas are referenced for consideration as part of the overall fraud and security strategy requirements:

- Device manufacturers – security auditing (initially and on an on-going/annual basis)
- Requirements for security based on a dispersed model rather than centralised control
- Risk assessment of the "trusted" parties within the delivery of services
- Provisioning management – including OTA and/or local management validation
- Device authentication and credentials – incorporating strength and testing
- Configuration management – software updates, configuration changes and access control
- Subscription and remote management and alarming – incident escalation and investigation
- UICC protection from fraudulent attack – incorporating SIM resistance to tampering and theft
- Device malware protection
- Trustworthiness and verification of M2M lifecycle - manufacture, installation/deployment, configurational change and maintenance
- Fraud management controls coverage – identification of any responsibility gap
- Ownership of risk – CSP, device manufacturer, software provider, customer etc
- CSP and third party suppliers etc. (SLAs) specific to fraud & security - obligations & liability
- Defining requirements for secure personal data protection – incorporating collection, storage (by all parties) and transfer internally, as well as with third parties
- Defining the fraud and security monitoring – i.e. FMS, Firewall management etc
- Defining the limitations of the SIM within the embedded device – service restriction and traffic volumes
- Data privacy (customer related) and law enforcement obligations
- FMS and any other detection and monitoring requirements – information sources and frequency
- CSP organisational changes for the fraud team – training and development of skill sets



What defences can be defined?

Having considered potential risks and exposure, the CSP should consider how these new threats and risks will both be defended against and detected on an on-going basis. Fraud control and detection will in certain cases be via the existing traditional methods, for example, adapting the Fraud Management System (FMS) for usage profiling based initially on normally expected EM device usage and subsequently generating event or high usage profiling to identify any anomalies.

Fraud and security management defences and monitoring requirements will need to be defined as an essential part of the risk management strategy but also extend beyond the more traditional methods by factoring in the way the devices and services are provisioned and offered. For example, a CSP will require the capability to detect tampering or physical removal of a device and location updates to ensure integrity of the device. This may well be covered via technical security controls over authentication and responses being monitored via the CSP network. For example if the device is programmed to call in every X hours or the cell ID changes, indicating movement of a fixed device. In all suspicious cases, the fraud team will still need to be informed that all is still "secure and as expected". For example, a defined International Mobile Subscriber Identity (IMSI) paired with a specific device and/or International Mobile Equipment Identity (IMEI) range is not identified as going "rogue". It will be paramount to consider that were a UICC is identified as being removed from a device that this will result in termination of the connection and escalation for investigation.

"…Remember that our battle against fraudsters will never be entirely won due to the fast moving telecoms environment, and the drive to launch more complex products and services quickly….but we need to think What If."

The deployment of M2M type devices, whether embedded or by using separate communication equipment to the monitored or controlled device, may or may not have an embedded UICC or even the functionality contained within the software. In these cases the ability to develop secure devices is far greater and will require appropriate security design. It has already taken the last 25 years in the mobile industry to overcome the security failures of the mobile device ID (IMEI), which is now relatively secure. If we also consider the computing/IT devices, such as SIP phones, routers, ADSL terminals etc, then the majority have been poorly designed from a security perspective. If M2M device design follows the same approach then criminals will easily compromise them. In addition, embedded mobile devices will need to incorporate ability for the CSP or provider to remotely diagnose potential security issues and have the capability to remotely install firmware changes securely.

Summary

The overall battle against fraudsters will never be won due to the fast moving telecoms environment and the drive to launch more complex products and services quickly to attract market share and maintain that competitive edge. This will always result in procedural weaknesses and technical risks being introduced which fraudsters will seize upon at the earliest opportunity to keep their fraudulent 'business' activities operational and profits high. However, CSPs can deploy various defence mechanisms to mitigate against losses and ensure fast detection by ensuring processes are continually reviewed, staff are educated in new M2M fraud trends, and new products and services are assessed for fraud and security weaknesses. In support of this, state of the art technology should be used to quickly raise alerts for suspect activity.

Key drivers increasing the risk of fraud and revenue loss in M2M are:

- Remote, unguarded/unattended locations
- The introduction of new (unknown) business partners
- Reduced cost of equipment
- Lack of M2M device control once deployed
- Devices not valued by the consumer in the same way people own and look after their mobile
- If a soft device is easy to modify this will enable fraud - its key design purpose is the control application not the communications
- Billing model approach - where M2M usage is not controlled or monitored until something actually goes wrong

Effective fraud management relating to the envisaged changes and introduction of new risks can be a time consuming and overwhelming activity especially for those CSPs who are not yet mature in the development of fraud and security control and prevention strategies. Præsidium is able to support CSPs in this space, having served over 100 CSPs worldwide to review, provide advise upon and implement fraud and security strategies, train fraud and security personnel, or deliver and optimise fraud solutions.

About Præsidium

Præsidium is a Global Business Assurance consultancy.
Founded in 1997, the company has successfully provided risk management consultancy to more than 100 Communication Service Providers in over 80 countries on 6 continents. Præsidium has gained solid recognition in the market amongst its substantial customer base and among global standards agencies. These include the GSMA Security Group & Fraud Forum, the Telemanagement Forum and ETSI.

Offices:

United Kingdom
Davidson House, Forbury Square,
Reading, RG1 3EU,
Tel: +44 118 900 1054
Fax: +44 118 900 1055

Portugal
Edifício Picoas Plaza
Rua do Viriato, 13E núcleo 6 - 4º andar
1050-233 Lisbon
Tel: + 351 210 111 400
Fax: + 351 210 111 401

Brazil
Torre Rio Sul, Rua Lauro Muller 116;
27º Andar – Sala 2701
CEP: 22299-900 Botafogo
Rio de Janeiro
Tel: +55 21 2543-5419
Fax: +55 21 2543-5419
Spain
Edifício Cuzco IV
Paseo de la Castellana, 141 8ª planta
28046 Madrid
Tel: + 34 91 572 6400
Fax: + 34 91 572 6641

Ireland
Maple House,Temple Road, Blackrock,
Co. Dublin
Tel: + 353 (0)1 400 3900
Fax: + 353 (0)1 400 3901

On the Web **www.praesidium.com**
General Information **info@praesidium.com**

About WeDo Technologies

WeDo Technologies is the number one preferred supplier for revenue and business assurance software and services.
Present in 15 countries on 5 continents, with more than 100 innovative bluechip customers in more than 70 countries, the company has a solid and envious project management track record of being on-time and within budget while achieving superior customer satisfaction.
Business Assurance RAID®, WeDo Technologies' flagship software suite covering Revenue Assurance, Fraud Management and Business Processes Control has been implemented in a number of different industries where it has delivered significant business results and powerful return on investment. WeDo Technologies pioneered the telecom revenue assurance space in 2002 and is now breaking new ground in the enlarged business assurance arena in Telecom, while also servicing the Retail, Energy and Finance industries.

Offices:

Portugal _ Lisbon

Portugal _ Braga

Australia _ Sydney

Brazil _ Rio Janeiro

Brazil _ Florianopolis

Chile _ Santiago

Egypt _ Cairo

France _ Paris

Ireland _ Dublin

Malaysia _ Kuala Lumpur

Mexico _ Mexico City

Panama _ Panama City

Poland _ Poznan

Poland _ Warsaw

Singapore _ Singapore

Spain _ Madrid

Spain _ Barcelona

UK _ Reading

USA _ Chicago

On the Web **www.wedotechnologies.com**
General Information **customerservices@wedotechnologies.com**