

White Paper

Voice, Network & Process Security within the TeleWare Service Provider Network

Abstract

The move to IP has served to increase the exposure of the telephony world to potential abuse and manipulation. Risks such as Denial of Service (DoS), Protocol Attack, Registration Theft and Proxy Impersonation need to be considered when selecting a hosted services provider to ensure the issues have been addressed within the platform design.

TeleWare provides telephony applications and SIP VoIP communications from its central hosted, highly resilient environment in London. It provides telephony services over any infrastructure, to any device and, in doing so, needs to ensure that security and privacy is not compromised or abused.

This document provides information on the security provided and discusses TeleWare's analysis of the security of their hosted service and the resulting audit processes in place.

Contents

Abstract.....	1
Areas of Potential Security Risk.....	3
Logical security	5
TeleWare Local Area Network	5
Routers.....	5
Servers	7
Software	9
Wide Area Network	12
Web Applications	12
Voice Applications.....	13
Process Security	15
Change Control	15
Authorized Persons and Request Logging.....	15
Physical Security.....	16
Data Centre Security Features.....	16
Conclusion	18

The growth of various ASPs, ISPs and traditional carriers providing hosted services within the SME environment has made the delivery of applications such as mobility, call centre, messaging, IVR and conferencing no longer a privilege of the corporate entity. Essentially, they are procuring enterprise services on an enterprise type platform at SME prices. This mode of operation comes at a price since adoption of the open standards necessary to deploy these services can provide a more open door to the IT and communications environment than is found in a proprietary solution.

Areas of Potential Security Risk

TeleWare supplies intelligent telephony applications from the hosted platform that provide the user the ability to access their voice services (be it basic voice services or intelligent applications) from any device, over any infrastructure in any environment. This provides the ultimate in mobility and accessibility, and the challenge of operating a secure environment is equivalent to any other application within the IT arena.

TeleWare have considered fully the security aspects of their systems and have implemented policies and procedures to make their services robust and protect them from misuse and disruption.

Security should be considered holistically and implemented at all levels of the service; these include the electronic systems, the physical systems and the processes that govern their operation.



Within TeleWare Hosted Services, the overall approach to security is multi-layered with each layer being connected to its neighbours but not to anything else. Thus the core platform is not directly accessible from external networks processes and personnel.

The aspect of 'logical security' groups together the data, application and voice and refers to the possible vulnerabilities and threats to the applications, both voice and data components, of the platform.

As the TeleWare Hosted Communications platform delivers cloud applications, this mandates connectivity to several kinds of networks; these include the PSTN (Public Switched Telephone Network), the internet as well as a number of data network providers which can supply ADSL MPLS, VPLS and other leased line networks. TeleWare always recommend using a secure network such as MPLS, VPLS or similar leased line when connecting to the Hosted platform so that a customer can secure their communications to and from the platform as much as possible. However, as a service provider platform, TeleWare must consider the lowest common denominator factors of the public internet and PSTN interconnects when designing the security policy to ensure that protection is provided to the assets hosted within the TeleWare data centres.

The TeleWare platform consists of a network of servers which provide voice and web applications to a range of connected networks which include the internet, the PSTN and Wide Area Networks.

The following assets need to be considered in relation to the logical security policy:

Physical systems:

- The Local Area Network
- Routers
- Servers

Software:

- Intelligent Exchange
- Voice Applications
- Web Applications

Even the most stringent logical security policies cannot alone secure any computer system, whether it is a desktop PC or a hosted service provider system. Computers have many physical interfaces which could equally pose a security risk. This document explains the aspects of physical security which have been implemented to control physical access to the hosted service.

Furthermore, policies and processes must be implemented to make sure that the security system cannot be compromised by a change to any element of the system, whether software upgrades or a change of personnel. As such policies and processes are part of the overall security system, this document shows how TeleWare implements its policies and processes to attain service provide security.

Logical security

TeleWare Local Area Network

The lowest common denominator of these components is the LAN to which all the assets are connected. Therefore, the LAN needs to be secured in order that the other assets are secured. The LAN is secured by the network edge. It is the role of the network edge to enforce a policy which admits the permitted traffic into the LAN from the outside data networks which are the Internet and the private network providers with which TeleWare partner. It should be noted that at this stage in the examination, the PSTN is considered to be an application which connects over an outside data network. Therefore, security against the PSTN will be discussed as part of the examination of application security later in this document.

As the LAN connects the platform IP network, the LAN itself can only be at risk from devices which are directly connected to it and the external networks which access the LAN do so via the network edge which is protected by the platform routers. The platform routers provide packet filtering and the Access Control List (ACL) which effectively firewall the entire platform. The ACL is a policy followed by the core routers which each have specific rules as to which servers can communicate with the outside world (effectively, a firewall). The ACL also restricts which IP ports can be used by each server or external party. Additionally, packet filtering rules are configured on each of the servers to restrict which ports and addresses they may communicate with, providing a 'double lock' complementing the Access Control Lists on the core routers. The combination of ACL and packet filtering effectively restricts the communications that is allowed with the platform to HTTP, HTTPs, SMTP, FTP, RTP and SIP and ensures that each protocol is only allowed to communicate with the designated server. Furthermore, in the case of SMTP and FTP the ACL restricts which external client servers can communicate with the platform.

The ACL and packet filtering rules described above combine to ensure that only the correct device receives and transmits permitted traffic. In simple terms, all VoIP traffic is forced by the ACL towards the Session Border Controller and all Web traffic is forced to the Web servers where it can be dealt with appropriately. Web and VoIP security is dealt with later in this document under the application security heading.

Routers

As previously discussed, the routers enforce the ACL policy which protects the LAN from unauthorised access. However, the routers' exposure to external networks puts them at risk of attack. The following section describes the potential attacks the routers could suffer and the corresponding protection built into the TeleWare network.

Simple DoS Attacks

An important factor to be considered is a concerted DoS (Denial of Service) attack directed at the platform routers from the internet or, indeed, the malicious use of a private interconnect. A simple DoS attack (by this we mean not a load-based DoS attack which is discussed later in the document) would flood the routers with traffic and try to make the router forward the packets, the aim of the attack being to 'swamp out' the legitimate traffic, hence disrupt the service at the IP layer.

Smurf Attack

A smurf attack is one particular variant of a flooding DoS attack on the public Internet. It relies on misconfigured network devices that allow packets to be sent to all computer hosts on a particular network via the broadcast address of the network, rather than a specific machine. The network then serves as a smurf amplifier. In such an attack, the perpetrators will send large numbers of IP packets with the source address faked to appear to be the address of the victim. The network's bandwidth is quickly used up, preventing legitimate packets from getting through to their destination.

Ping Flood

Ping flood is based on sending the victim an overwhelming number of ping packets, usually using the "ping" command from unix-like hosts (the -t flag on Windows systems has a far less malignant function). It is very simple to launch, the primary requirement being access to greater bandwidth than the victim.

Router protection against Simple DoS, Smurf and Ping Flood attacks

The TeleWare platform uses the ACL to disallow servers from within the LAN from sending such traffic and the platform is configured to not send broadcast messages out to the connected networks. These two actions protect the hosted platform from being exploited as a smurf amplifier.

Protection from DOS in general is also provided by the Cisco edge routers which ensure that packets denied by the ACL are dropped at the fast level interrupt which is close to hardware speed. With the exception of two packets per second per access-list line, these two packets will be used to send an ICMP unreachable message back to the amplifier.

As the ACL policy is designed to minimise the impact of an attempted DoS attack, it is very likely that the attacker will curtail their activities as the service will remain unaffected. In the unlikely event that a DoS attack has impacted the network, then the platform intrusion detection system will alert the TeleWare NOC. Once the TeleWare NOC has been alerted, the engineers will access the routers and edit the ACL to block the source IP addresses of the attack to reject the unwanted packets.

Ping of Death

Ping of death is based on sending the victim a malformed ping packet, which might lead to a routing system crash. If a ping packet makes an echo request with more than 65,507 bytes of data, an attacker could cause a remote system to crash while reassembling the packet fragments.

Within the TeleWare platform, ping is not allowed to the edge routers, hence restricting the risk. However, ping is allowed to a device which is purely used as a 'responder' for testing and the main session border controller which employs (Committed Access Rate) CAR which is very similar to packet shaping to limit the number of Ping packets that it responds to at a safe level. The Session Border Controller is also hardened to the risk of malformed packets.

General Router Protection

Overall, the TeleWare Hosted Services platform reduces the potential impact of DoS, using packet shaping within the edge routers. Packet or traffic shaping is normally seen as a method of improving QOS (Quality of Service). However, the edge routers use packet shaping to drop traffic generated by denial of service.

Traffic shaping provides a mechanism to control the volume of traffic being sent into a network (bandwidth throttling), and the rate at which the traffic is being sent (rate limiting). For this reason, traffic shaping schemes are commonly implemented at the network edges to control traffic entering the network. This means that if a particular message is being sent at too high a rate (a DoS attack), the packet shaping rules within the edge router will, effectively, allow these messages to be ignored.

In addition, TeleWare have implemented core and edge routing, meaning that only the edge routers would be impacted during any attack.

Servers

We have now demonstrated how the platform is secured at the basic IP and network level. The next level of consideration is the server hardware or, essentially, the operating systems and other software services which run on them.

There are two fundamental issues to consider in protecting the servers; unauthorised access or load-based DoS attack.

Unauthorised access is the process of an attacker accessing either the operating system or the application and manipulating the environment, for example, by accessing the platform with malware (malicious software) either to invoke as much damage as possible or to take advantage of services provided without permission.

Manipulation of this environment may be either local or remote and is usually the result of inadequate firewall protection or anti-virus software protection, or poor security processes such as open identification and authentication information. Let us now consider specific attacks which could be inflicted on the servers.

Load-Based DoS Attacks

The principles of basic DoS attacks which work at the IP level are discussed in the previous section. Load-based DoS attacks are intended to exploit vulnerabilities in the network protocols which servers use by sending malformed or out-of-sequence packets intended to lock a server's network connection into an error state, rendering it unable to communicate with the outside world.

Ping of Death

The ping of death, as discussed in the previous section, is also a potential threat to server devices as they have similar ping functionality encoded into their network stacks. The use of the ACL at the network edge prevents servers from being accessed by Ping traffic.

SYN Flood

SYN flood occurs when a host sends a flood of TCP/SYN packets, often with a forged sender address. Each of these packets is handled like a connection request, causing the server to spawn a half-open connection, by sending back a TCP/SYN-ACK packet and waiting for a packet in response from the sender address. However, because the sender address is forged, the response never comes. These half-open connections saturate the number of available connections the server is able to make, keeping it from responding to legitimate requests until after the attack ends.

Low-rate Denial-of-Service (LDoS)

Recently, a new kind of DoS attack, Low-rate Denial-of-Service (LDoS) attack, has been proposed that exploits TCP's retransmission timeout mechanism to reduce TCP throughput without being detected. Compared to traditional flooding-based Denial-of-Service attacks, the low-rate DoS attack does not employ a 'sledge-hammer' approach of high-rate transmission of packets and, consequently, eludes detection. These kinds of attacks were also called shrew attacks, Pulsing DoS (PDoS) attacks, and Reduction of Quality (RoQ) attacks.

The Low-rate DoS (LDoS) attack exploits TCP's slow timescale dynamics of retransmission time-out (RTO) mechanisms to reduce TCP throughput. Basically, an attacker can cause a TCP flow to repeatedly enter a RTO state by sending high-rate, but short-duration, bursts and repeating periodically at slower RTO time-scales. The TCP throughput at the attacked node will be significantly reduced while the attacker will have low average rate making it difficult to be detected.

Server Protection

It is worth noting that the ACL and the rate limiting provided by the platform routers provide a level of protection to the servers which complement the server's own security as they control the access of external networks to the core of the platform.

TeleWare use Windows Server 2008 as the server operating system within their platforms. Windows Server 2008 is the most secure Windows server to date. Its hardened operating system and security innovations help protect servers, networks, data, and user accounts against failure and intrusion, providing unprecedented levels of protection for the network, data, and service.

In response to the above threats, the TeleWare platform leverages the following Windows 2008 features:

Windows Service Hardening

This helps keep systems safer by preventing critical server services from being compromised by abnormal activity in the file system, registry, or network such as a load based denial of service attack.

Public Key Infrastructure (PKI) enhancements

Available only with Windows Server 2008 Enterprise and Windows Server 2008 Datacenter, include support for enterprise auto-enrolment, Network Device Enrolment Services (NDES), the Online Certificate Status Protocol (OCSP), the Online Responder service, and are fully compatible with version 3 certificates. OSCP allows the TeleWare platform to check security certificates before using or revoking them.

Windows Firewall with Advanced Security

A stateful host-based firewall that allows or blocks network traffic, according to firewall policy and the applications that are currently running, to protect the network from malicious users and programs. At a basic level, the firewall provides a packet filter which complements the ACL in blocking unwanted traffic from the servers. The stateful firewall provides protection from attacks such as SYN flood and LDoS.

Additional Hardening

There are also a number of practical steps which TeleWare undertake to ensure that the Windows 2008 security features are optimally managed:

- TeleWare use the Microsoft Windows update services which are managed by an internal change control process to ensure that the latest patches are implemented on the platform when Microsoft identify a new vulnerability.
- TeleWare further harden their server operating system platforms by restricting the active services which run on the server to only those that are needed to facilitate the platform, hence restrict the scope for service vulnerabilities and reduce the possible 'attack surface'.
- TeleWare enforce the use of strong passwords for both user and administrator access to all elements of the platform. There are standard recommended policies for user account usage. Briefly, this covers the use of strong passwords, regular changing of passwords, prompt removal of old accounts and a different password for each new account.

Of course, there is always a risk of even the most stringent security policy being breached. In order that a breach can be detected, intrusion detection is deployed throughout the platform to alert the TeleWare NOC of any abnormal activity which might suggest a breach of the server security policy.

Anti Virus Protection

A computer virus could be considered to be an intrusion and is, of course, a malicious attack. TeleWare employs best of breed Antivirus technology and enforce the installation of Antivirus software on all servers throughout the platform domain. This helps ensure system safety by detection and cleaning known viruses from the system which may have circumvented the security policy.

Software

Intelligent eXchange

Intelligent eXchange requires separate analysis as compared to other voice applications because it uses VoIP protocols which are accessed via the routers and LAN. General voice applications such as Intelligent Office and Intelligent Connect use Intelligent eXchange and the PSTN to deliver and receive calls and will be discussed in the Voice Applications section.

As previously discussed, the TeleWare platform has been restricted to allow only the protocols which are necessary for the service. The SIP protocol is used by Intelligent eXchange to communicate with customer equipment over Wide Area Networks. Since this represents external access, then the security policy requires examination.

The ACL is pivotal in the SIP security policy as it restricts the access of external networks using the SIP protocol to the Session Border Controller (SBC). The security features enforced by the SBC are described below.

As the threats to SIP telephony are diverse and varied, a detailed examination and response to each is provided in the following section.

Session Tear-Down

Session tear-down risk is associated with the open standards operation within the SIP IP environment; a SIP user agent could be denied the ability to utilise voice services through the manipulation of the voice messaging stream. Essentially, the attacker monitors the network for SIP traffic and then sends spoofed SIP 'bye' messages which prematurely terminates the call and places the user back into the idle state. As these are seen as valid messages by the proxy server, the attack is often difficult to recognise or resolve.

Essentially, the result of a Session Tear-Down attack is Denial of Service (DoS) which can be either specific (i.e. user based) or general (i.e. firewall, media gateway, IVR, etc.).

Within the TeleWare Hosted Services platform, this is addressed by the use of the ACL and SBC described above. The control of unauthorised access is the single most effective method of preventing this type of attack and is described in section a). The SBC only accepts a BYE message from the original IP and port address. As well as the techniques already described, the use of intrusion detection is also important with this type of security risk. Intrusion detection monitors all network traffic passing through the platform and uses rules to detect malicious traffic. Intrusion detection aims to identify and stop all malformed information that would not normally be prevented by a simple firewall.

Load-Based Denial of Service (DoS)

A Load-based DoS involves bombarding a server with millions of requests while a Malformed Request DoS uses protocol request to exploit vulnerable areas such as the operating system. Although this attack does not control or damage the application, it achieves the desired effect of compromising the system's ability to provide service and rendering it unavailable to its user base.

As previously shown, the edge routers on the platform limit the opportunity for DoS attacks by packet shaping which reduces the impact of the threat. With a targeted load-based DOS attack against Intelligent eXchange, the SBC inspects the SIP messages and rejects malformed requests, therefore negating the attack. The SBC also contains rate limiting capabilities, in case the DoS attack comprises 'legitimate' SIP i.e. all SIP traffic is subject to throttling and limiting on a per-IP address basis which virtually eliminates the impact of a DoS attack.

Protocol Attack

A protocol attack typically exploits vulnerabilities in protocol stacks with the aim of hijacking a stream and making free VoIP calls. In the SIP environment, messaging is text based which can be manipulated by a LAN / WAN sniffer. An individual could monitor the network (especially in the wireless environment) and capture call setup information from the messaging field and then manipulate this information to make calls without the need for an edge device.

Within the TeleWare Hosted Services platform, this is addressed by the use of the session border controller (SBC). The SBC is, essentially, a Firewall for voice over internet protocol (VoIP) traffic. It isolates all SIP traffic and forwards only legitimate traffic to the inside of the platform. The SBC is used as an access controller because every session (call or attempted call) is filtered against specific criteria, for example, the source IP address. Registration Security is enhanced because, once an endpoint (phone) registers, the SBC validates all subsequent requests against its source IP address and, therefore, duplicate requests are then denied. The SBC is a dumb device and validates all traffic against the databases inside the platform. An additional feature is the rate limiting capability as mentioned above which is used in DoS attacks.

The Session Border Controller appropriately secures the platform from a voice perspective. However, if not correctly enforced, there are still loopholes within SIP implementations for the would-be attacker. Intelligent eXchange itself provides authentication and logging mechanisms to afford the following protections:

Call SPAM

Spam, which is the transmission of bulk unsolicited email, has been a plague on the internet email system for some time. SIP is used for multimedia communications between users, including voice, video, messaging and presence; consequently it can be just as much a target for Spam as email.

Call Spam is defined as a bulk unsolicited set of session initiation attempts (i.e. INVITE requests), attempting to establish a voice or other type of communications session. If the user should answer, the spammer proceeds to relay their message over the real-time media. This is the classic telemarketer spam applied to SIP. This is often called Spam over Ip Telephony, or SPIT.

Every subscriber that connects using SIP to Intelligent eXchange is authenticated ensuring that subscribers can be identified and correct detail plans and classes of service can be applied.

SIP extensions use dynamic registration, this facilitates security whilst allowing the flexibility sometimes required by mobile users. Such users might use their SIP devices from several locations. This necessitates the support of changing source IP addresses which would otherwise not be allowed by the ACL. Dynamic registrations are validated with a password which the handsets are challenged to provide. The password is allocated by the TeleWare Service Manager portal on creation of the account and is held in the Intelligent eXchange database. The password will have been previously configured on the handset along with the rest of the SIP account details, when it is deployed. Whenever the handset sends a registration message, the SBC validates the request and challenges the extension to provide its password. The handset then sends the password with MD5 encryption to the SBC which validates the session.

SIP Trunk devices such as PBXs do not require dynamic registration as they are not likely to move networks. SIP Trunk devices are instead authenticated by their pre-agreed source IP address which means that the ACL can be used to verify the identity of the device. By ensuring that only authenticated SIP subscribers can access the platform and place calls within their company or the PSTN, TeleWare removes the opportunity for Call Spam.

Toll Fraud

The concept of toll fraud has existed for some time within the traditional on-premises PBX environment. Essentially, it is the unauthorised access and use of resource (usually enterprise voice circuits) without paying for them and presents a tangible cost to the corporate. A typical example would be use of the PBX/voicemail infrastructure of a corporate private network to access international numbers. The introduction of VoIP services only increases potential exposure to abuse. Toll fraud is most likely to be the result of a user application which has suffered a password breach or security information has fallen into the wrong hands. Less likely is a breach of the layers of security described in this document which surround the hosted platform.

Within the TeleWare Hosted Services platform, this is addressed by the use of logging tools that calculate the calls being made from individual tenancies. Only endpoints that have authorised access to the platform are able to use its features. The Service Manager application is designed to manage and control access to the platform by each tenancy. As part of this application, access to statistical information from the call display records (CDR) is available. This can be used to identify unusual patterns of activity. Service Manager is also used to set up tenancy dial plans, trunk access calling, etc., all on a class-of-service basis. This restricts what a tenancy is able to do and all of these parameters can be applied in real-time.

TeleWare work with your connected network providers to do audits of users and resource utilisation to identify peculiar patterns of operation, potential insecure configurations (e.g. allowing toll bypass scenario) and unusual traffic volumes and timings.

Wide Area Network

As demonstrated throughout this document, the hosted platform is secured on many levels to prevent unauthorised access and other malicious activities which could be initiated from the Wide Area networks to which the platform is connected. The boundary of the hosted platforms policed by the ACL which prevents unwanted access; however, the Wide Area Network design is also an important consideration.

The Wide Area network risks to be considered are:

Interception / Eavesdropping

Interception is the process of compromising a communications link with the intention of monitoring (eavesdropping), recording or manipulating the data stream – ultimately, gaining control and taking advantage of the intended end user services. The ability to record and manipulate information can also elevate this attack to a more sinister level. This takes place at the transport layer and protocol environment and is particularly prevalent in the wireless arena.

Within the Wide Area Network the two most important measures are using a private network for connection to the customer premises such as an MPLS, VPLS and other leased line network. This is because it is not possible to access the traffic from a different network or network segment.

It may be desirable for a customer to use the open internet to deploy VoIP, for example, to a home worker or branch office. TeleWare advises such customers to satisfy themselves as to the sensitivity of the data in question and plan their network deployment accordingly.

Proxy Impersonation

Proxy impersonation is the process of tricking a SIP user agent into communication with a rogue proxy server. Once again, many installations communicate using UDP and, due to the lack of authentication, it is relatively easy to manipulate the messaging stream via Address Resolution Protocol (ARP) cache spoofing and Domain Name Service (DNS) spoofing. Once control has been obtained, the attacker has complete control of the call allowing them to block, conference, record and manipulate services.

Within the TeleWare Hosted Services platform, this is addressed by use of MPLS, VPLS and leased line partner networks. This is because this is primarily an issue of open internet access. Therefore, THS recommends that either a VLAN or a VPN is used where possible.

Web Applications

As we have explored the layers of the TeleWare security model, we have discussed the elements of ACL, hardening, group access policy, intrusion and other techniques which are used to secure the platform servers in general. Additional measures have been put in place to protect the servers which provide the Web applications as the servers are, to a degree, exposed to the open internet by virtue of their operation.

- The accounts used to run the web servers are low privilege accounts
- The web servers are fully patched to the latest Microsoft recommendations
- To reduce their attack surface the servers run the minimum number of services for their role

Additional features apply to specific applications such as secure and encrypted call recording.

Secure FSA Recording - Tamper Evident

To meet FSA regulations, all recordings are held securely in the TeleWare data centre for 185 days and can only be accessed via a secure web interface.

Encrypted call recording are marked as 'secure' and will be digitally signed with the customers 2048 bit RSA key at the point of recording, they become tamper evident. This allows for detection of any modifications of the content of any downloaded recordings.

Encryption in the Platform

For an additional layer of security where conversations may be of a particularly sensitive nature, speech is recorded in an encrypted format. A unique capability and strength of the TeleWare solution is that encryption is applied during the actual recording process. This avoids the limitations of using an encrypted file server, where the same encryption key is used for all recording files on the server. Customers are provided with software to generate their own unique 2048 bit RSA signing and encryption keys. The system ensures that no-one else with access to the platform can decrypt a customer's recordings.

As additional security against hacking, no unencrypted data is stored, even on a temporary basis. All recordings are written and processed in real-time to the file server.

Call Recording Access

Our Call Recording solution records and stores all inbound and outbound calls automatically. Calls can then be retrieved using the service's web interface. Access to the stored call recordings is through a secure web interface housed on the platform. The web application utilises HTTP. The download is via a secure FTPES.

Voice Applications

The voice applications are Intelligent Office and Intelligent Connect. As previously discussed, they are accessed via Intelligent eXchange for which the aspects of security have already been discussed and the PSTN. The threats to voice applications are, therefore, voice calls which can be made using the PSTN or SIP devices which are connected to the Intelligent eXchange.

Voice applications can be vulnerable to unauthorised access where an attacker could access a user's messages or make calls through an application at the user's cost. There has been a great deal of publicity recently regarding mobile handset voicemail hacking. This is the practise of discovering the access number, or the mailbox number of an individual's voicemail account and calling into it. If a user has been lazy and not changed their password from the default which is likely to be an easily guessable combination such as 1234 or 1111 which makes a poor defence against even the most casual attacker. Mailboxes that have 'make a call' or 'return a call' functionality are also open to being used to place ongoing calls which could be used to commit toll fraud by dialling through to premium or international numbers.

This is addressed in the TeleWare platform using a number of techniques that enhance the security of users' mailboxes.

The default passwords allocated to mailboxes when they are created vary on a per company basis; therefore, there is no universal default password for the service.

When a user first accesses their mailbox, they are forced to change their password before they can access their messages and other features. The password a user chooses must not be one of the following patterns: 1111, 2222, 3333, 4444, 5555, 6666, 7777, 8888, 9999, 0000, 1234, 4321 or the default password.

When a user changes their password, they are also prevented from using their previous password. Only three consecutive failed login attempts are allowed to a mailbox before it requires unlocking by an administrator.

By using the above procedures, TeleWare enforces the access security of its voice applications, virtually eliminating the possibility of an attacker accessing the correct password for a user's mailbox.

Additional features can be added to mailboxes to limit the potential impact of toll fraud in the unlikely event of a mailbox being breached. A user's profile may be configured to restrict their right to dial national, international and or premium rate numbers through their mailboxes.

Process Security

Change Control

In order to ensure that the security and reliability of the platform is not undermined, any technical change that has to be made to the platform must go through the change control review process.

The process dictates that a person cannot change the system without first reviewing the change with all stakeholders. All stakeholders then assess the impact of the change and sign off once the change has been verified as not having an adverse impact on the service. If an adverse impact is identified, then correcting action must be taken prior to the change being signed off. The change control process also makes provision for an out-of-hours maintenance window should this be required to minimise the impact of any outages that may be required to implement the change.

Authorized Persons and Request Logging

It is important when high levels of security are required, such as for FSA Compliance requirements, that TeleWare work closely with the customer to ensure that any changes made are fully authorized and logged. Typically, the customer cannot make changes to their administration accounts on the platform directly; these are instead performed by TeleWare's dedicated Customer Services team.

Typically, TeleWare will agree processes on a case by case basis covering the processes and authorized contacts to:

- Request new accounts
- Change passwords
- Close old accounts

Typically, the agreed processes will include authentication of requestors through password validation.

Physical Security

Data Centre Security Features

Security is not just about the provision of secure gateways, hardened operating systems and robust applications. Any solution needs to be complemented with clear and precise policies and procedures to physically secure the platform as well as the 'logical' security methodologies already discussed.

The TeleWare data centres are located in purpose built facilities; Harbour Exchange Tower 2, Docklands and Equinix Heathrow. Building security ensures that only authorised TeleWare personnel are allowed access to the secure data rooms and platforms at each location. If a third party requires access to the platforms they must also be supervised by an authorized TeleWare person, ensuring that all activities can be monitored.

The primary site is the Harbour Exchange data centre in which TeleWare lease a dedicated facility. TeleWare provide and maintain their own systems within the data centre which is secured in conjunction with the building's own security systems and personnel.

The Heathrow site is managed by Equinix, a well known data centre provider who provide and maintain the security and supply systems. TeleWare rent collocation space within the site for their secondary platform. Both the data centres benefit from outsourced, high quality security guarding. Examples of the guarding companies' accreditations and codes of practice are as follows:

- ISO 9001: 2000 Quality Management System, (UKAS)
- BS 7499 : 2007 Static Guarding and Mobile Patrol Services
- BS 7984 : 2001 Keyholding and Response Services
- BS 7858 : 2006 Security Screening of Personnel
- BS 7959 : 2006 CCTV Management and Operations
- BS 8418 : 2003 Installation and Remote Monitoring of detector activated CCTV systems.
- Membership – approved Contractor by Security Industry Authority (SIA)
- Membership – International Professional Security Association
- Gold Award – Security Watchdog

Additionally, both data centres benefit from segregated public and private areas with swipe card access control to ensure that physical access is restricted to authorized personnel only. TeleWare operate an access policy that is reviewed every three months which ensures that only authorized TeleWare personnel are able to access the hosted systems. TeleWare do not permit unsupervised access to their systems ensuring that any third party working on or accessing the servers, network and associated systems are supervised at all times.

There are a number of other features within the data centres that are designed to protect the service. However, these are considered to ensure the availability of the service and the following features are discussed in a separate document.

- Fire detection
- Fire suppression
- Flood and water detection

- Diverse data networks
- Diverse power networks
- Uninterruptable power supply
- Generator backup
- N+1 availability
- Disaster recovery

Conclusion

This document demonstrates how TeleWare are well on their way to compliance with ISO 27001 Information Security Management System (ISMS) by enforcing systematic examination of the organisation's information security risks, taking account of the threats, vulnerabilities and impacts.

TeleWare compliance to ISO27001 will be achieved during September 2011 and TeleWare expect to have an Accreditation certificate issued by an external party at the end of December 2011.

TeleWare have designed and implemented a coherent and comprehensive suite of network security controls and have adopted an overarching management process to ensure that the information security controls continue to meet the organisations information security needs on an ongoing basis.

Whilst the hosted platform is securely connected to the internet and it is possible to gain access to the hosted services and applications using the internet, it should be noted that it is the platform that is secured against the unpredictability of the internet and not the transmission of data itself. TeleWare cannot provide assurances regarding the security of actual transmitted data over the internet. Therefore, the customer should satisfy themselves as to the sensitivity of the data in question and plan their network deployment accordingly.

Within the hosted environment, the security is the responsibility of the platform provider and, as with resilience and reliability, the hosted solution provides an opportunity to deploy a greater level of security than might be affordable for many companies within an on-premises solution.

wptw110801

A TeleWare Group plc company. This document is provided for information only. In line with company policy of continued improvement of products and services, TeleWare reserves the right to alter product specification without notice. TeleWare and Intelligent eXchange are registered trademarks. Intelligent Office, Intelligent Number, Intelligent Assistant, Intelligent Connect, Intelligent Mobile and Intelligent Application Builder are trademarks of TeleWare plc. All third party trademarks and registered trademarks are acknowledged. Copyright 2011 TeleWare plc.

TeleWare plc

TeleWare House, York Road, Thirsk,
North Yorkshire, YO7 3BX, UK
Registered in England No 4756742

T: +44 (0) 1845 526830

F: +44 (0) 1845 522165

E: enquiry@teleware.com

W: www.teleware.com