Call Recording Security in the Cloud

Cloud based Call Recording confers many benefits, including the ability to capture calls from distributed locations and mobile devices. Cost models are significantly cheaper than legacy on-premise systems. However, the perception of greater accessibility and less control in the cloud brings concerns over data security.

IT and IS Managers need to understand their provider's attitude and measures taken to secure call recordings, particularly when these can contain sensitive financial, commercial and patient sensitive information. With this knowledge and a sensible policy structure, it can be seen that cloud based call recording can offer equal, and sometimes greater information security than on-premise systems.

Encryption

01A07700
53D03C00

Encryption of the call recording media when at rest (in storage) and in transit is the first stage in ensuring that information does not reach untrusted ears, although recordings stored within a secure data centre are more likely to be stolen through unauthorised access to portals than physical removal.

Web access should always use SSL / HTTPS with trusted certificates so Internet connections are private. The added benefits of peer to peer networks or VPNs for access are contentious issues, but X-on can offer these options if required.

Access Control

Access to call recordings on any system will involve authorised users with appropriately strong passwords. By controlling groups and access lists with a "need to access" policy, call recordings can be restricted to departments based on extensions or phone numbers dialled. This reduces the surface area. Complex situations where calls are transferred between departments under different authorities may need to be considered.

Further levels of access control can restrict recording access to sessions from particular IP addresses or ranges, public or private. Recordings can also be individually deleted on request by users with Manager access.

Geographic Redundancy

A cloud recording solution can replicate your recordings across data centres to ensure high availability in the event of a major disaster.

To achieve geographic redundancy with an in-house solution immediately presents the challenges of a cloud solution but with local management issues.

x-on.co.uk
surgeryconnect.co.uk
0333 332 0000

Private Keys

As an option, it may be arranged to encrypt recordings such that a private key, known only to you the customer, is required to decrypt them locally. Although this “ultimate security” may sound attractive, it may be worth considering that an element of trust in your network operator and service provider is always required, regardless of where calls are recorded. Even with an in-house recording solution, you are entrusting the network operator not to make illicit recordings of your calls.

With this option, your provider’s engineers, even with your permission, will be unable to assist with any issues with recording, and access to recordings will require a download and decrypt process which is marginally more laborious.

Card Data - the Special Case

The Payment Card Industry has a special set of rules, known as PCI-DSS, governing the storage and transmission of credit and debit card data. With online web payment systems becoming more secure, fraudsters are turning their attention to telephone systems to steal card data.

PCI-DSS does not allow certain parts of the card data, such as the CV2 security code, to be stored under any circumstances. If you are taking credit card payments by the phone therefore, it is not acceptable to record those calls, even if those recordings are encrypted and all the precautions detailed above are taken.

Fortunately, there are mechanisms, such as X-on’s CardByPhone system that allow card payments to be taken over the phone and transacted in real time during a call. Card data is removed from the scope of your staff and operations and does not appear on call recordings.

RECORDING SECURITY AT A GLANCE

- Access recordings over password controlled SSL layer (HTTPS)
- Security access lists, password strength and groups to enforce restrictions
- IP Based access control to limit access further
- Recordings stored encrypted at rest
- Optional private key encryption owned by client
- Remove card data from recordings using PCI CardByPhone
- Compliance to ISO27001, PCI-DSS, ICO
- UK Data Centres with physical access control
- Geographic redundancy to avoid data loss in major disaster

x-on.co.uk
surgeryconnect.co.uk
0333 332 0000