CommandHub
securing sensitive information

CommandHub Use Case

Telecommunications

How to Secure Collaboration on Sensitive Network Reports

USE CASE: Telecommunications

How to Secure Collaboration on Sensitive Network Reports

Your Situation

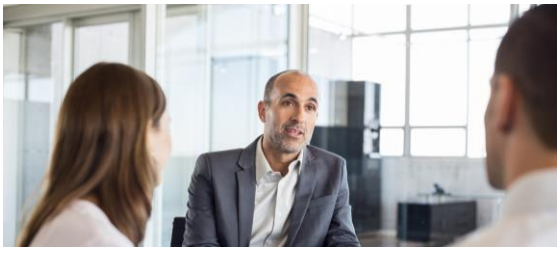
You are the Chief Security Architect or CISO of a Telco. Your company offers diverse services and products, from cell phones for consumers to fibre networks for corporate clients, and data centres providing secure and redundant hosting for cloud services.

Part of your service for major corporates is to review their network security and document your findings. These detailed reports are compiled by cyber-security professionals inside your and clients' organisations who collaborate closely, discussing the findings, commenting, editing and revising before final release.

Your Challenge

Your clients expect you to keep their network data confidential. Any data leakage, breach or theft could cause serious damage to the relationship and your reputation. Since collaboration on these reports involves multiple steps, numerous contributors and diverse locations, your challenge is to safeguard both clients' data and the collaboration process.

Your safeguards must be stringent and effective but can't become barriers to collaboration. If the collaboration processes aren't intuitive and easy to use, users will be tempted to seek risky work-arounds or Shadow IT.



Your Vulnerability

Sharing documents via email attachments is risky, especially since phishing attacks are more refined. Other risks are internal; accidental loss by careless staff or malicious actions by informed insiders. Together these account for the majority of security breaches. Restricting user access to clients' data is one step; cyber-security professionals with authorised access who are not under your control are also involved.

You have little way to ensure they'll follow your business processes for collaborating on your clients' data.

Mobile devices pose a risk too; they're less secure and more likely to be mislaid, and most professionals use them. You need to extend your content protection to mobile devices, especially because data is retained in caches and remote wiping is ineffective when WiFi is disabled or the device is turned off.

Your Options

If securing collaboration on client's sensitive data is critical for your telco, there are five main options:

1. **Do Nothing.** This may appeal if you've had no breaches to date or none reported. You may feel that your rules and processes are adequate and your user education will ensure adherence to them. This would only be your choice if the client data is not sensitive and the perceived risk of breach is low.

2. **Choose an Enterprise File Sharing System.** These systems make file-sharing easy and provide some file security but are not designed for collaboration. You'll need to add third party tools which could add cost and complexity and open security gaps. This would be your choice if lowering rather than eliminating risk to client data is enough.

3. **Choose Enterprise Collaboration Tools.** These widely-used tools were designed to facilitate collaboration with security added later. You may find that specified security levels apply to the environment not the tools. This would be your choice if your client data is not critical and mobile device use is not widespread among contributors.

3. **Choose Secure Collaboration Tools.** These recent developments, designed for closed networks, promise to secure sensitive content by checking the alignment between user, content and context. They may restrict users' access but won't control how they use content, especially on mobile devices.

This would be your choice if restricting access is enough, you have a controlled network and mobile device use is limited.

5. **Choose an End-to-End Secure Collaboration Platform**. This approach, in use for over a decade, creates ultra-secure content compartments to which access is restricted on a 'need to know' basis. It extends protection beyond who accesses your data to how it is used and where it is stored, including on mobile devices. This would be your choice if you need complete end-to-end protection of client data, and your risk profile demands a proven solution.

How CommandHub secures your sensitive collaborations

Military grade architecture
CommandHub was designed from the ground up for secure collaboration, based on the Military Principle of multiple layered servers.

The CommandHub solution is IRAP certified to the Australian Signals Directorate (February 2020) ISM PROTECTED standard. All data is wholly hosted and managed in Australia under the Sovereign Cloud Principles for Critical Infrastructure.

'Need-To-Know' Compartmentation
CommandHub applies the Intelligence Community principle of compartmentation, restricting user access to a 'need to know' basis. This means that even personnel with seniority or high security clearance will only be granted access to specific compartments if they 'need to know' the contents for their roles.

Patented End-to-End Protection
Providing the highest level of server security is the minimum; CommandHub also provides data protection in transit and in use.

With patented HubVault technology, contributors can securely access and use your client data on mobile devices, via a multi-encrypted tunnel that replaces vulnerable browsing.

HubVault also secures content stored on mobile devices, using further encryption and a non-recoverable key, rendering them 'uncrackable' if they're mislaid.

Logical Business Controls
CommandHub makes collaboration easy for contributors users while ensuring that your telco's business processes are followed. You can set controls for who can see, edit or save a file, who may move it and to where, how approvals and rejections apply, the exact sequence of these steps as well as version control, watermarking, file-locking and more.

Tailored To Your Exact Needs
With over 500 configuration settings, CommandHub can be fully tailored to how your telco operates. By simply turning on or off rules for files, access, use, formats and settings at any level, CommandHub ensures that your sensitive client data is fully protected, without impeding how your contributors work.

Ease of Setup, Use & Control
CommandHub was designed for setup and use without IT skills. After little training, your administrators will be able to arrange client data logically for contributors and apply controls to protect it. When reports or client relationships end, administrators can make the changes themselves. For contributors, the intuitive interface makes collaboration easy without IT support.

Proven In Situations Like Yours
CommandHub has been protecting sensitive content in the most demanding situations for over ten years, in Telecommunications, Banking and Insurance, Justice, Law Enforcement and Defence Contracting, and for Executive Committees elsewhere. Ask us about our case studies.

Contact us about how CommandHub can secure your sensitive collaborations.