CommandHub
securing sensitive information

CommandHub Use Case

Banking and Finance

How to Secure Collaboration on Sensitive Reports, Products and Strategies

USE CASE: Banking and Finance

How to Secure Collaboration on Sensitive Reports, Products and Strategies

Your Situation

You hold the role of CTO, CIO, Senior Business Executive, Legal Counsel or similar in a major financial institution based in Australia. Your services include banking, insurance, and superannuation. Yours is a proud institution of long standing; you employ thousands of people and serve millions of customers.

Your organisation employs hundreds of senior executives who need to work on highly sensitive financial content. This includes strategic plans, risk analyses, compliance reports, meeting minutes, responses to regulators and more. If this material fell into the wrong hands, it could directly impact your organization's competitive advantage, value and reputation.

Your Challenge

This sensitive content needs to be shared, discussed, commented on, revised and finalised, passing through executives' hands and those of their assistants for many iterations. This process raises the risk of leakage, loss or theft, given that C-level executives and their assistants are high value phishing targets for hackers.

Therefore, both your sensitive content and how it's shared must be well protected. Further, your safeguards must be stringent but not become barriers to collaboration. That means, they must be easy to set up and work with for senior business users who may not have advanced IT skills.

Many of your senior executives travel for their jobs, so they'll need to collaborate elecrtonically. Most of them use smartphones or tablets, which increases your exposure.

Apart from being less secure than fixed devices, mobile devices are prone to theft and being mislaid or lost. To enable collaboration without heightened risk, you need to protect your sensitive content and how it's used on mobile devices.

Your Options

If securing collaboration on sensitive content is critical for your institution, you have 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 be your choice if the data your executives share is not highly 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 open security gaps. This would be your choice if lowering rather than eliminating risk 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 and that user configurations require a great deal of IT help. This would be your choice if your content is not critical, mobile device use is not widespread and your IT resources are readily available.

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 content 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 sensitive content, 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. 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 to fulfil their roles. This negates the risk of a 'Chelsea Manning' type breach.

Patented End-to-End Protection
Providing the highest level of server security is the minimum; CommandHub also provides content protection in transit and in use. With patented HubVault technology, your executives can securely access and use your content on mobile devices including Apple iOS and OSX, Android and Windows-based, 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.

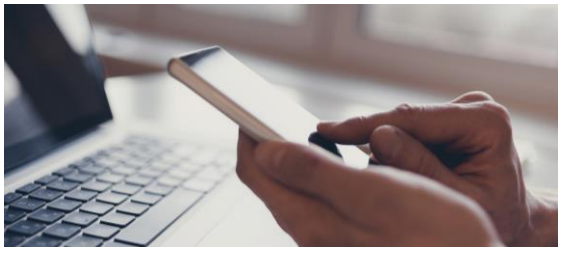
Logical Business Controls
CommandHub makes collaboration easy for executives while ensuring that your institution's processes are followed. You can set controls for who can see, edit or save a file, who may move it and to where, how approvals and rejections apply, the exact sequence of these steps as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

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

Ease of Setup, Use & Control
CommandHub was designed for setup and use without IT skills. After little training, administrators will be able to arrange the content structure logically for your users and apply controls to protect it. When meetings conclude or strategies alter, administrators can make the changes themselves. For your executives, 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 Banking and Finance, Telecommunications, Government, Justice, Defence Contracting, and for Executive Committees elsewhere. Ask us about our case studies.

Contact us about how CommandHub can secure your sensitive collaborations.



03 9653 9585 www.commandhub.com info@commandhub.com