Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Web Conferencing Security

APRIL 2020

Introduction

Web conferencing solutions (also commonly referred to as online collaboration tools) often provide audio/video conferencing, real-time chat, desktop sharing and file transfer capabilities. As we increasingly use web conferencing to keep in touch while working from home, it is important to ensure that this is done securely without introducing unnecessary privacy, security and legal risks. This document provides guidance on both how to select a web conferencing solution and how to use it securely.

Selecting a web conferencing solution

When selecting a web conferencing solution, it is important that organisations ask themselves the following questions.

Is the service provider based in Australia?

The use of offshore web conferencing solutions introduces additional business and security risks. For example, laws in other countries may change without notice and foreign-owned service providers that operate in Australia may still be subject to the laws of a foreign country. In addition, service providers who are located offshore may be subject to lawful and covert data collection requests and access an organisation's data without their knowledge.

What is the service provider's track record?

A service provider's actions in response to privacy issues and cyber security incidents is important, as is how quickly they disclose and take effective action to remediate security vulnerabilities in their web conferencing solution. Look for a service provider that actively and quickly engages with their customers, advocates for data privacy rights and proactively addresses cyber security issues, such as having a vulnerability disclosure program. Conducting research on a service provider's historical responses will help identify how seriously they treat these issues.

Are privacy, security and legal requirements being met?

Prior to agreeing to a service provider's terms and conditions, organisations should seek privacy, security and legal advice. Notably, the terms and conditions should include specific clauses that address organisations' legal, privacy and security requirements. Without privacy and security requirements being specified, organisations may not be able to verify a service provider's security claims or whether their information is being appropriately used or not. In particular, attention should be paid to whether a service provider claims ownership of any recorded conversations and content, metadata, or files that are created or shared when using their web conferencing solution. Finally, when seeking legal advice, organisations are less likely to inadvertently accept terms and conditions that breach financial or liability rules.

What information and metadata does the service provider collect?

Information and metadata can, and often will be, collected by a service provider. Such information can include (but is not limited to) names, roles, organisations, email addresses, and usernames and passwords of registered users, as well as information about devices they use. As this information may be sensitive, organisations may need to provide advice to staff as to the appropriate level of information they should disclose during the registration process. Knowing how this information will be used by a service provider will help inform organisations of the privacy, security and legal risks when using their web conferencing solution.

Does the service provider use strong encryption?

A service provider should be encrypting data both while it is at rest (being stored by the service provider) and while it is in transit (being transferred been different devices). This is to ensure that the data can't be read by others that don't have a need to know. One thing to specifically look for is whether a web conferencing solution use strong encryption, such as Transport Layer Security (TLS), to protect data while it is in transit. Web conferencing solutions that exclusively support TLS versions 1.2 and 1.3 inherently offer more protection for data transmitted across untrusted networks such as the internet.

What is the reliability and scalability of the service provider's web conferencing solution?

As the number of organisations and staff using a web conferencing solution increases, it can become overloaded. As such, it is important to ensure that any web conferencing solution will be both reliable and available in times of increased demand. Understanding the capabilities of a web conferencing solution, such as the number of simultaneous connections that can be supported, will ensure organisations and their staff are able to collaborate even during times of increased demand.

If an existing web conferencing solution does not meet business requirements in times of increased demand, organisations should consider increasing the capacity of the existing solution, or using alternative methods of relaying information, prior to looking for alternative solutions that may introduce additional privacy, security and legal risks.

Using a web conferencing solution

When using a web conferencing solution, it is important that organisations practice the following activities.

Configure the web conferencing solution securely

Review the service provider's documentation for the security features and recommended configurations related to their web conferencing solution. In doing so, note that default security settings in web conferencing solutions may need to be configured to meet organisational security needs. Furthermore, advise staff using the web conferencing solution on personal devices to ensure that they have applied all security patches for their devices and their devices are as secure as reasonably practicable.

Establish meetings securely

When hosting a meeting, consider how invitations, website links and access credentials will be distributed to participants. If permitting guests, send meeting details and access credentials separately via email or encrypted messaging apps. Do not share website links or access credentials on publicly-accessible websites or social media. Finally, remember to update any access credentials periodically, such as once a month, or after they have been provided to any guests. This will reduce the risk of guests joining other meetings they haven't been invited to.

Be aware of unidentified participants

Only allow invited participants to join a meeting, and once all participants are present, consider locking the meeting so no one else can join. However, in some cases, it may not be possible to identify individual participants, such as when they join via a telephone call. In such cases, take note of sounds or visual notifications indicating that participants are joining the meeting, and ask any unknown participants to identify themselves. If unknown participants are unable to appropriately identify themselves, they should be disconnected by the meeting host.

Be aware of surroundings

Using a private location for meetings will help maintain confidentiality. If a private location isn't possible, using headphones can ensure that when working in a shared location only approved meeting participants will hear the full discussions. In addition, muting the microphone when not actively speaking improves the meeting experience by eliminating unwanted background noises, such as keyboard typing sounds or audio feedback loops, and prevents accidentally broadcasting private or sensitive discussions that may be happening nearby.

Finally, with high definition webcams now the norm, participants may unwittingly broadcast private or sensitive details in their background. Where video is required for a meeting, try to position cameras so they only capture participants' faces. Alternatively, consider using background blurring features if they are available, noting these may be specific to certain service providers.

Be mindful of conversations

Be aware of the potential private nature or sensitivity of workplace conversations, and limit discussions in meetings to those approved to be conducted using a web conferencing solution. It is also good practice to set expectations prior to a meeting, for example, whether the contents of the meeting will be recorded or made public. For Commonwealth entities, consider what sensitivity or classification has been authorised for discussions over any web conferencing solutions.

Only share what is required

If sharing screen content for a meeting, it is best practice to share an individual application instead of a device's entire screen. Alternatively, a web conferencing solution may be able to select only a section of a device's screen to share. However, if screen sharing is not required, either disable the functionality or limit its use to only the meeting host. For similar reasons, capabilities that record and automatically transcribe calls, subtitle videos or share files can create a risk of inadvertently sharing more content than intended.

Further information

The ***Australian Government Information Security Manual*** (ISM) assists in the protection of information that is processed, stored or communicated by organisations' systems. It can be found at https://www.cyber.gov.au/ism.

The ***Strategies to Mitigate Cyber Security Incidents*** complements the advice in the ISM. The complete list of strategies can be found at https://www.cyber.gov.au/publications/strategies-to-mitigate-cyber-security-incidents.

When selecting web conferencing solutions, please see the ***Cyber Supply Chain Risk Management*** publication at https://www.cyber.gov.au/publications/cyber-supply-chain-risk-management.

Contact details

Organisations or individuals with questions regarding this advice can email asd.assist@defence.gov.au or call 1300 CYBER1 (1300 292 371).