Working from home: managing communication risks

Within the current context of remote working, video and audio conferencing tools have become an increasingly common way to conduct business meetings. However, there are a number of important factors that businesses should bear in mind when using third-party communications platforms:

Evaluating risk: No conferencing tool is completely risk-free, and each has pros and cons. In particular, when selecting a conferencing tool, businesses should be careful to consider the data protection and cybersecurity related risks inherent in the technology (considered further below) and the potential harm to the business if security was to be compromised. The more sensitive the communications that are taking place using conferencing tools, the more important it is to ensure that the right tools are selected.

The service provider's terms: Before selecting a conferencing tool, it is important to review the service provider's standard terms to understand what contractual obligations and liabilities each party is taking on. In particular, the service provider will almost certainly be processing personal data in the course of providing the conferencing services, so a GDPR processing agreement will be mandatory for businesses that are subject to EU law.

Access by the service provider: It is important for a business to understand the level of access (if any) that the service providers have to any calls or recordings, and the purposes of access. For example, some service providers monitor calls for quality purposes. Others use information from calls for data analytics purposes. Some reserve the right to share information from calls with law enforcement. Such practices could be particularly problematic where highly sensitive matters are being discussed, including legal advice.

End-to-end encryption: Not all conferencing tools provide equal levels of security. A key question when considering a conference tool is whether it provides end-to-end encryption (i.e., encryption at all stages of the transmission of data between devices). Conferencing tools that lack this feature inherently expose communications to a greater risk of eavesdropping and loss of confidentiality in the event of a security incident.

User authentication: Some conferencing tools require different levels of user authentication (e.g., requiring users to log in from a particular domain, using a password in addition to the meeting number, or verifying identity using an email address or phone number) while others merely allow anyone with access to a link or a call number to join. Businesses should ensure that any sensitive materials are only discussed among authenticated users. Employees should be instructed to notify IT security immediately should unidentified users appear on calls.

Device security: An unavoidable feature of working from home is that many employees will use their own devices, rather than work-issued devices, to communicate. Businesses should ensure that they have appropriate IT security policies in place to mitigate the heightened security risks associated with personal device use, and should also require that employees use systems that are correctly updated and have the latest patches applied.

Working from home: managing communication risks

Disciplinary measures: An essential component of data protection and cyber risk management is ensuring that employees are adhering to their responsibilities. Working from home should continue to be treated as work, and employees who violate applicable policies should be subject to disciplinary action where appropriate. Failure to take disciplinary measures may place the business at risk, if employees start ignoring their responsibilities in large numbers. Two often overlooked components of employee training for remote workers that are less problematic within office confines are: (i) physically securing business information (including documents and computer monitors visible to household members); and (ii) remaining mindful of who may be able to overhear their conversations.

Recording: Some conferencing tools include functions for recording conversations. If a business selects a tool that has recording functionality enabled by default, that business should ensure that employees are alerted to the relevant settings to disable it as needed. Companies also should address whether it is lawful and within company policy for employees to record conference calls without obtaining the prior consent of all participants (noting that there are potential criminal sanctions in some jurisdictions).

Periodic review: Businesses should regularly consider the conferencing tools that they have implemented, and re-evaluate risks as further information becomes available. Businesses should also conduct regular testing to evaluate the strength and effectiveness of the security measures they have in place.

Updating compliance documentation: Businesses should ensure that their compliance documentation and information security training programs are updated to reflect the use of conferencing tools. This typically includes amendments to employee-facing privacy notices, and updating data processing registers where required. Employee training documentation and materials should also be updated where necessary.

Cyber risk insurance: Businesses that are using new conferencing tools should review their cyber risk insurance coverage to ensure that they do not inadvertently void their cover by using tools that fall outside the scope of that cover.

Key contacts

Tim Hickman
Partner, London

T +44 20 7532 2517
E tim.hickman@whitecase.com

Detlev Gabel
Partner, Frankfurt

T +49 69 29994 1528
E dgabel@whitecase.com

Steven Chabinsky
Retired Partner of Counsel, Washington, DC

T +1 202 626 3587
E steven.chabinsky@whitecase.com

F. Paul Pittman
Counsel, Washington, DC

T +1 202 729 2395
E paul.pittman@whitecase.com

whitecase.com

LON0420012_03