SECURED COMMUNICATIONS

How can companies mitigate risk in a world where more people are working remotely?

8 September 2020

Covid-19 has changed how the world works. Large corporates are shifting from a workforce based in an office environment, to a large proportion of their staff working from home.

This has underscored the need for secure and reliable communications platforms. Which brings us to the question, *'How can companies mitigate risk in a world where more people are working remotely?'*

How can we ensure that our communications and data are truly secure?

A recent survey conducted by Forcepoint in partnership with WSJ Intelligence revealed that 71% of global CEOs said they were losing sleep over the prospect of their company's next security breach, and less than half (46%) regularly reviewed their cybersecurity strategy.

Ensuring that security protocols are in place and using trusted secure systems for business needs is the key. Many communications platforms that businesses have come to rely on during the pandemic were built for a social purpose, not corporate. They simply do not provide the level of security and enterprise support needed to ensure protection.

Over the past months, many security breaches have been reported including those where video conferences have been hijacked, inappropriate images have been distributed and there has been disruption to services. All of this carries with it a huge risk for a company's reputation.

However, in our new world and new ways of working, businesses have to find a way of staying connected whilst being satisfied that their information and data is secure.

Businesses must consider their needs carefully and understand the consequences of data breaches and the associated loss of productivity. Cost effective and secure systems are available that have a similar functionality to some of the well-known platforms but offer much higher levels of security giving businesses reassurance that their sensitive information and data is protected.

As we move towards remote working becoming the new normal, workers need to have simple but secure systems available to them. There is always a tendency to mix business with social needs when working from home and, if you're working on an insecure IT connection or platform, that presents a risk.

Bespoke systems that firewall business data from private information is vital, not only to ensure productivity, but to reduce the risk of opening a door to unwanted guests.

Mercury is a highly secure, encrypted video and audio-conferencing product based on technology which is already trusted by many law enforcement agencies and businesses around the world.

It is operated on a fully secure private cloud platform based entirely in the US and has been specifically designed for businesses to fulfil the critical need for a secure meeting solution. When you're in a Mercury meeting you are in a locked room that no-one can enter.

Unlike other companies, Mercury will never harvest and share user data or trade clients' privacy protection for a larger user base. Mercury offers similar features to other applications, but none can match it for its security through end to end encryption and enterprise level of support from the company.

It is important for businesses to have the reassurance that their information is protected and to conduct remote meetings in private, knowing that anything discussed or shared is not overheard or ever captured by anyone else.

John Parkinson OBE is a former Chief Constable of West Yorkshire Police and Senior National Counter Terrorism Coordinator. He is president of US tech company, Secured Communications, which recently launched its Mercury secure video conferencing, audio calling, messaging, file transfer platform in the UK.