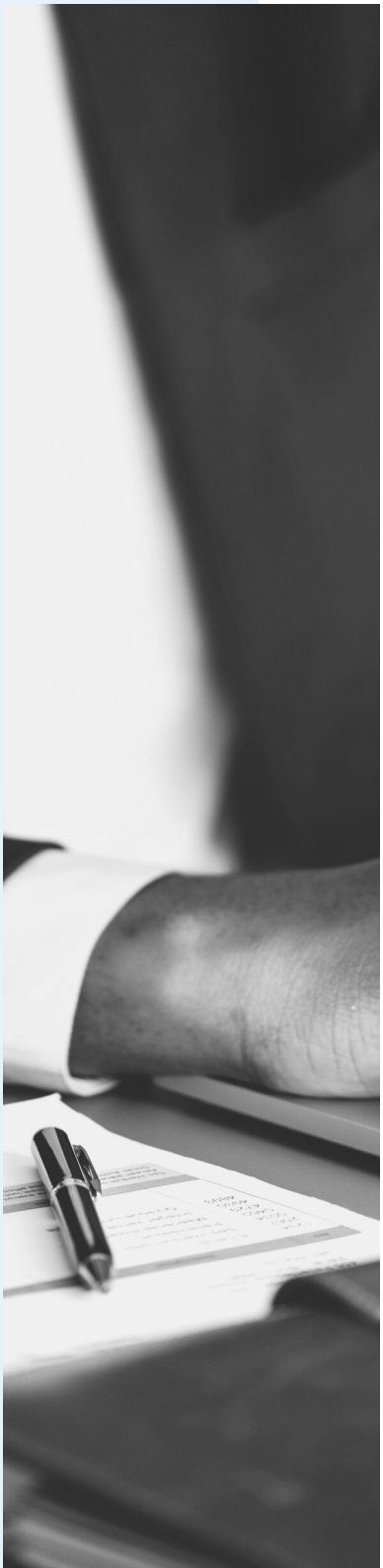
DekkoSecure // AUGUST 2020

What every CEO needs to know about the risks of information sharing and video conferencing that no-one has told them.

Jacqui Nelson
CEO, DekkoSecure

01



> Gartner research shows that CEOs are increasingly being blamed and punished as a result of cybersecurity-related events – even more so than IT executives.

Following the very public Equifax hack in 2017 that cost CEO Richard Smith his job and exposed the personal details and records of more than 140 million Americans, it was noted in the US House of Representatives subcommittee report released in 2018 that, “Equifax’s CEO simply did not prioritise cybersecurity.”

A recent discussion I had with a CEO from a global law firm further highlights the risk CEO’s face today in the wake of information privacy and security issues.

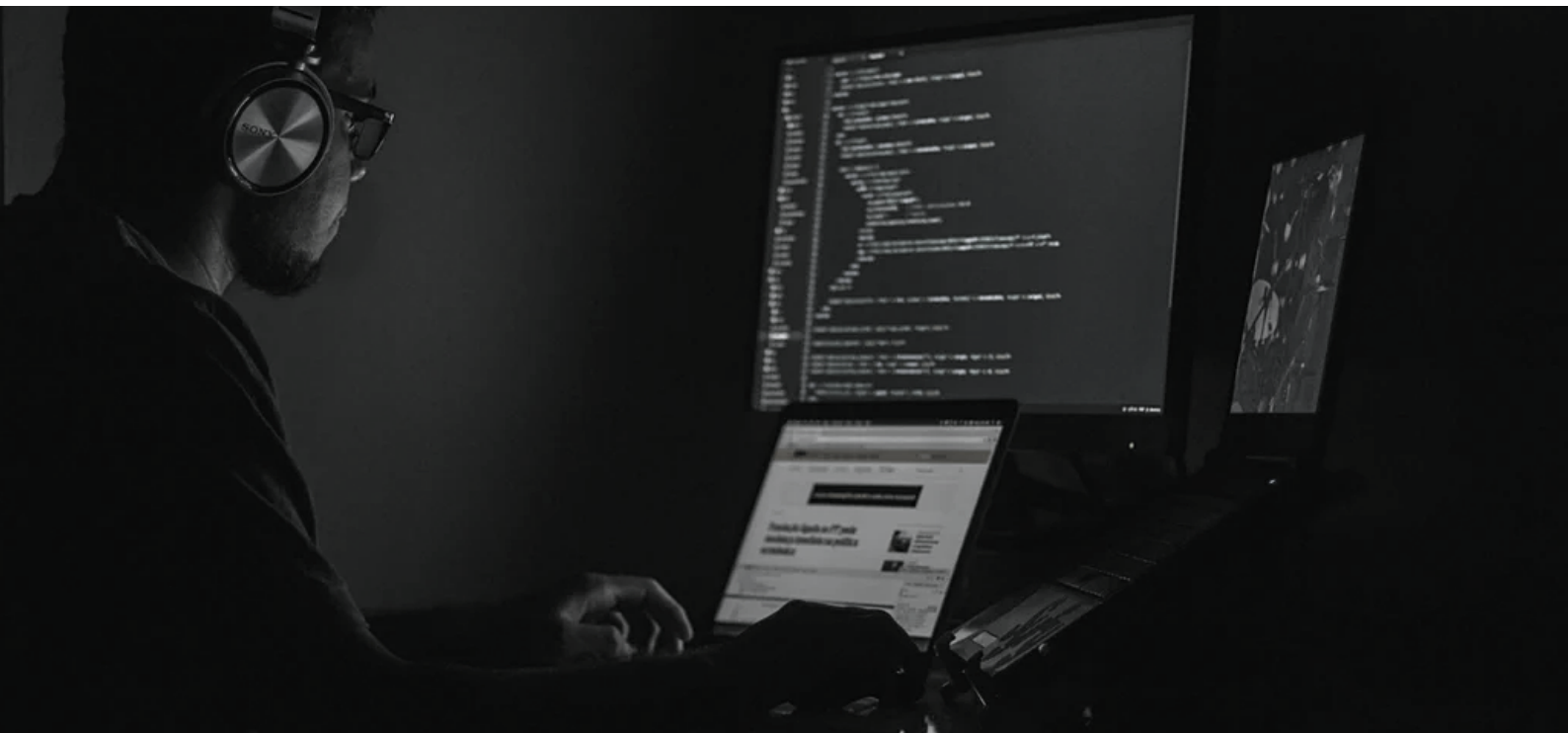
02

During our conversation it became apparent he, as well as many other CEOs, simply “don’t know what they don’t know” about the cyber risk profile of their organisation when it comes to information sharing and data storage.

This is in spite of the fact that some may have a team of cyber security specialists reporting to them.

The sobering fact is most organisations are routinely affected and have, or will experience, the theft of their intellectual property, important information or sensitive data sometime during their lifecycle.

Of particular concern is that cyber criminals including nation states, have become increasingly sophisticated and effective in their ability to bypass traditional security measures.



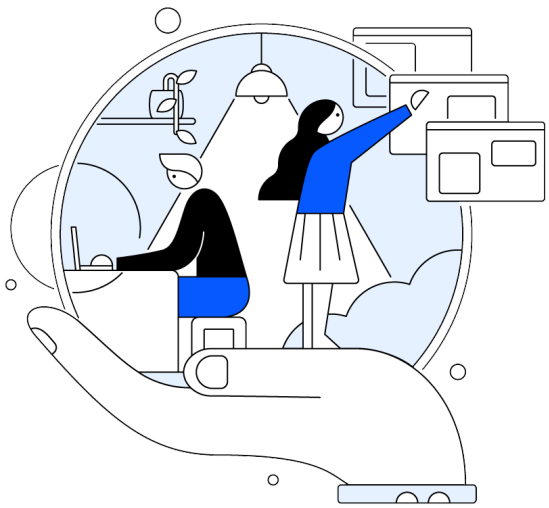
03

In the wake of a data breach financial loss is unavoidable, reputational brand damage is often impossible to recover from, and employee morale is seriously affected as staff must work harder to recover from the breach.

The risk is real and the potential costs can be catastrophic.

It is now abundantly clear that when it comes to the protection of your organisation's data, "near enough is simply NOT good enough", and ignorance or abrogated responsibility is not a valid defence.

The following are the key factors that CEO's must consider when analysing organisational security risk and the acquisition of the appropriate technology to mitigate that risk.



04

THE IMPORTANCE OF DATA SOVEREIGNTY

It is prudent to consider who hosts your company's data and in which jurisdictions it resides.

As the CEO, you need to know that data stored or hosted outside of your country is subject to the laws of the country in which the data resides and may be accessed by a foreign government. Furthermore, it is difficult to ensure that privacy regulations are being met if the data is stored in some jurisdictions.

Data sovereignty must be a key consideration in the technology acquisition process. If the data being stored is of a sensitive or protected nature it is prudent to store it in the jurisdiction of your choice to minimise risk.

If data sovereignty is a potential issue we strongly advise a thorough review of your provider's contract to determine where your information will be stored or hosted and consideration given to securing a guarantee that your data is and will be stored in the country of your choice.

05

THE RELEVANCE OF SECURITY BY DESIGN

If security has not been built into a technology from its foundation then it is inherently less secure.

Depending on the sensitivity of your data it is prudent to ask the question about the inherent security design of the technology you employ.

To use a popular phrase to illustrate the point, “You wouldn’t take a knife to a gun fight”.

If a high level of security is required for your data and information you would be well advised to evaluate and choose technologies that are built with security at the core.

Some popular data sharing and video conferencing solutions are feature rich but are designed with security as an afterthought and a “bolt on” feature. These providers have been called out by security experts for focusing on useability and scale over privacy and security.

06

If the risk of a data breach or intrusion is a critical factor they simply may not provide the surety and peace of mind you require.

If this is the case, when evaluating competing technologies, it is vital to question the validity of vendor's security claims and insist on a thorough competitive analysis around security design.

As an example, Dekko Secure is an Australian cybersecurity company with a deep pedigree in designing military grade security products. These products, designed with security at the core, are now commercially available for information sharing, collaboration and communication.

07

WHAT ABOUT GOVERNMENT REGULATION AND COMPLIANCE?

With the drastic increase in cyber security threats, nation states and state-sponsored actors and criminals are putting the privacy and security of our most important asset, our data, at risk.

This has forced governments to plead with organisations to take cyber security very seriously, and request that boards implement stringent cyber security guidelines.

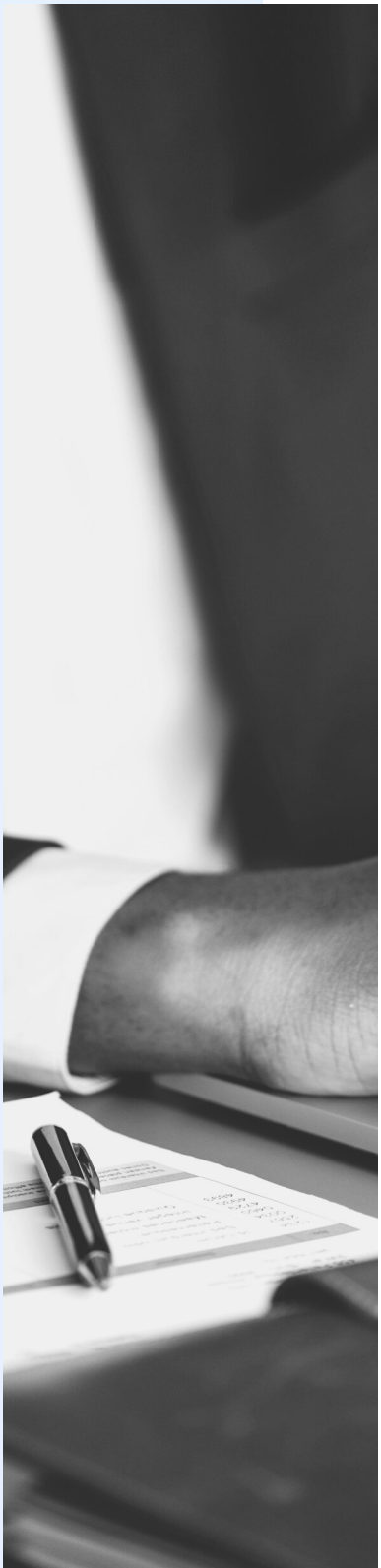
This has, at the very least, raised awareness of these important issues.

What it has also created is potential poor decision making as boards increasingly rely on “checking boxes”, buying into the misguided belief that compliance alone is the answer.

To put it simply, technical compliance does not equal cybersecurity protection.

At its worst, compliance forces you to spend where you may not need it and may stop you from investing where you definitely should.

08



WHAT YOU NEED TO KNOW ABOUT VIDEO CONFERENCING AND DATA SECURITY

Due to the pandemic the increase in the use of video conferencing as a means to communicate, meet and collaborate has been exponential.

This trend is unlikely to reverse now that remote working has become the new normal.

Conducting meetings and activities without the need to travel and meet face to face has provided unexpected benefits and efficiencies.

However, depending on the sensitivity of your meeting content and communications the following are the key factors to evaluate:

09

ENCRYPTION TECHNOLOGY

The majority of the popular video conferencing solutions claim to provide encrypted video calls. In fact, many of the existing solutions only encrypt video content between the user's device and the solution providers' servers.

What is not widely known, however, is that the call is decrypted at the server, which means that third parties have the ability to access, transmit, or even modify the content of the meeting.

This means the privacy and security of your meeting can potentially be compromised.

When absolute protection and privacy of information shared via video conferencing is required video content should be end-to-end encrypted, meaning that the data is encrypted and decrypted only at the user endpoints.

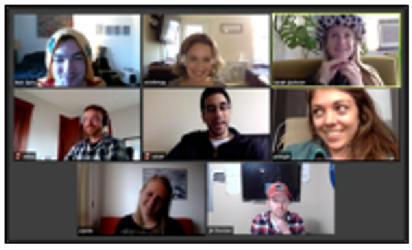
This completely avoids the possible compromise of the information in transit.

To date DekkoLynx is the only product on the market that employs end-to-end encrypted video conferencing in the browser and end-to-end encrypted call recording, storage and sharing.

10

REGULAR ENCRYPTION

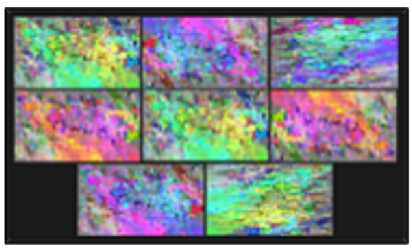
The two most common methods are 'at-rest' and 'in-transit'. Using these methods your data is encrypted as it leaves your computer but can be decrypted then re-encrypted again at numerous points as it travels to its end destination, as the service provider holds the key to the content. Each time the data is decrypted it has potential to be exposed or altered.



What the server sees

END-TO-END ENCRYPTION

Using end-to-end encryption, only you and the desired users have access to the keys to unlock your data. It is never decrypted at any point before the destination. This means no third-party, not even the server or your internet provider can view or alter this data.



What the server sees

DATA TRANSPARENCY AND TRACEABILITY

As mentioned above, due to the nature of the encryption method used, many of the popular video conferencing providers have unlimited access to the content of your meetings.

According to their privacy policies, they can collect data during the call by accessing audio transcripts or conducting spot checks on video conference quality for product development purposes.

Of particular concern is the mining of personal data to build consumer profiles and / or to sell the information.

To understand the likelihood of risk, it is essential to conduct a due diligence process and trace the data lifecycle to identify the levels of access and security in place and its storage location.

12

HUMAN ERROR, TRANSGRESSION AND SOCIAL LOAFING

It is a startling fact that just under 40% of all organisational leaks and breaches today are attributed to human error.

Misaddressing of emails that contain sensitive and highly confidential company information are too often sent to the wrong person either accidentally or with malicious intent.

The Department of Home Affairs accidental release of a key whistleblower's identity and disclosure details illustrates the stark and devastating consequences of human error and an accidental misaddressing of an email.

The leaking or loss of sensitive information is also of increasing concern for business.

As an example, we were contacted recently by a company COO seeking assistance after it was accidentally discovered that an employee was being paid to provide highly confidential and market sensitive information to a competitor.

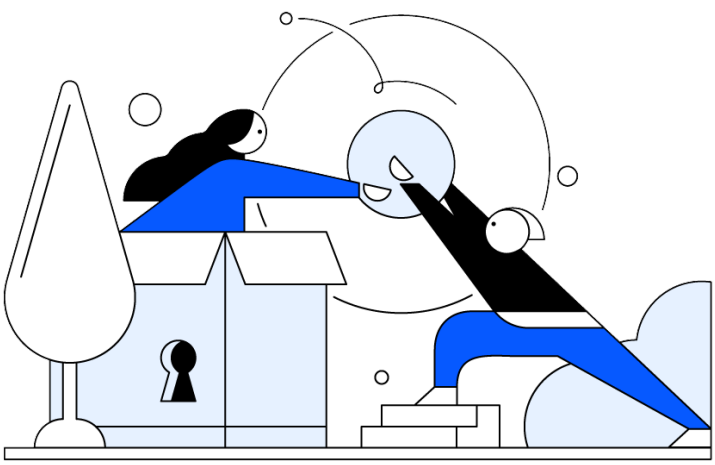
13

There have also been numerous cases of employees carelessly leaving USB's with sensitive data lying around, or not locking the device, or not disposing of them in the recommended manner. In some instances, vital information is being withheld and not shared due to the high level of risk associated with unsecured sharing.

The sociological concept known as social loafing partly explains the high incidence of costly human error and carelessness.

Social loafing is defined as, "The phenomenon of a person exerting less effort to achieve a goal when they work as part of a group than when working by themselves."

The key consideration for CEOs is the importance of being aware that employees working in teams often assume it is the responsibility of company leaders to drive security initiatives.



14

This issue alone demands that CEOs thoroughly investigate the inherent design of the chosen security technology.

Choosing a technology that has security “by design” means efficiency and total protection from employee error by ensuring that your employees never have to opt in to initiate security measures, nor can they ever opt out.

In simple terms, the security door is “fully self locking” and protected from the risks of human error, carelessness and human transgression.

15

This document has addressed some of the key issues that affect the security and privacy of your organisation's valuable information and data. We hope that it assists your efforts to keep your valuable and private data safe and secure.

Jacqui Nelson is the CEO of DekkoSecure, an Australian cyber security specialist. She is a finalist in the 2020 Australian Women in Security Network Award for Australia's most outstanding woman in IT security.

Dekko has pioneered the employment of military grade security technology to affordably safeguard the data of Government, Enterprise and SMB's across the globe. The Dekko platform enables totally secure storage, information sharing, document approval and video conferencing.

For further information please contact Jacqui Nelson, jacqui.nelson@dekkosecure.com.