Cyber-Risks and Liabilities

July/August 2020

Protecting Your Privacy While Using Video Conference Software

During the COVID-19 pandemic, technology has proven to be invaluable in allowing organisations to stay as connected as possible. Video chat software and apps have been particularly useful, as employees have been able to continue to attend virtual meetings and feel a sense of connection to their co-workers while working remotely.

But, while video conferences have been useful for many organisations across a wide variety of industries, the increased use of technology also means increased cyber-risks. With employees working from home, and therefore potentially lacking the same cyber-security protections that your workplace may have, it is important that your organisation take precautions to ensure that the use of video conference software is safe. Take these steps in order to protect the data of your employees and your organisation:

- **Establish protection**—When selecting which video software to use, consider whether a service is included in your current business software package. If so, this will help staff familiarise themselves with the program and allow you to use your existing authentication provider. If applicable, use single sign-on in order to integrate video conferencing with your other corporate systems. As a result, your video software will have the same protections as other company services.
- **Understand privacy settings**—While using video conference software, be aware of what data your employees may be sharing, how it is being processed and with whom it is being shared. Take the time to understand the privacy and security settings for your organisation's video software of choice. These settings may include the ability to password protect meetings, control when certain parties are allowed to join meetings and determine who is allowed to share their screens.
- **Avoid phishing**—Phishing attacks are common methods used by sending cyber-threats via email and text, but these threats might also show up during video chats. If you are using a live chat feature, an unwelcome party may attempt to slip in an attack. Instruct your employees to avoid clicking on links or attachments that were unexpected or shared by an unknown party.
- **Stay updated**—Regardless of what software is being used, or whether employees are working from home or not, one of the most important cyber-security measures that must be taken is keeping software updated. If employees are using a web browser to run their video chats, it is imperative that you instruct them to keep the browser up to date as well.

As technology becomes more integrated into the workplace, good cyber-security practices are increasingly important. Contact us today to learn about cyber-insurance solutions.

Crendon Insurance Brokers Ltd
0121 45 45 100
www.crendoninsurance.co.uk
enquiries@crendoninsurance.co.uk

Crendon Insurance Brokers

Supreme Court Rules on WM Morrisons Data Breach

On 1st April 2020, the Supreme Court handed down a ruling that could influence the future of group litigation stemming from data breaches.

In the case of Various Claimants versus WM Morrisons Supermarkets, the court ruled that the company was not vicariously liable for a 2014 data breach that exposed the personal details of nearly 100,000 employees. The breach was caused by a former employee, who posted the information online.

Previously, the High Court had found that Morrisons was vicariously liable for the breach, but not directly liable. Under established law, an employer is vicariously liable for actions committed by an employee who was acting within their 'field of activities'.

However, upon appeal, the Supreme Court overruled that decision, finding that the employee in question had not been acting within their normal duties, and had instead been carrying out a personal vendetta.

It is worth noting that this data breach occurred prior to the 2018 implementation of the General Data Protection Regulation (GDPR). While the Morrisons case was ruled upon based on the Breach of the Data Protection Act 1998 (DPA 1998), for future cases and those occurring after 25th May 2018, the GDPR will apply.

Regardless of the recent ruling, it remains of the utmost importance that employers take the necessary steps to protect their data. In Morrisons' case, lower courts found no fault in their cyber-security measures. As such, the case was judged entirely based on the actions of the employee. However, had the organisation's security measures been found to be faulty, the outcome of the case may have been different.

Ensuring Cyber-security by Managing Access and Privileges for Users

Your organisation's data and intellectual property are invaluable resources, but they also present a tempting target for cyber-attacks. If your systems are compromised, there may be irreparable harm done to your organisation's finances, reputation and future. One of the most important steps in addressing cyber-risks is regulating what information is accessible, and by whom.

Many cyber-attacks occur due to a user's account being hacked or compromised. With that in mind, your organisation should take steps to limit how much access each user on your network has. By doing this, employees and other users will not be able to access information that they should not be privy to and, if hacked, the attacker will not have as much access to your systems.

Take the following steps in order to maintain proper user access:

- **Account management**—Accounts and their respective access permissions should be managed and updated regularly. Redundant accounts provided for testing or temporary staff should be deleted or inactivated after having served their purpose.
- **Authentication policies**—Organisations should establish a password policy that ensures employees will be using strong passwords in order to access data. For accounts with certain permissions, additional authentication steps should be considered.
- **Limited access**—All users should only be granted access and permissions that are necessary to perform their job.
- **Limited privilege**—The number of accounts with in-depth access to important systems and sensitive information should be strictly limited. Administrative accounts with a high amount of access should be used sparingly. Those with access to them should also have normal accounts that are used for everyday business.
- **Surveillance**—It is important to be aware of what is going on in your network. Monitor the activity of users and respond to any suspicious activity.
- **Separate logs**—Access to activity logs should be limited. Activity logs should be sent to an accounting and audit system that is kept separate from your core network.
- **User awareness**—Make sure that your users are aware of how they are allowed to use their accounts, what permissions they have and their personal responsibilities as they pertain to the organisation's overall cyber-security.

Crendon Insurance Brokers