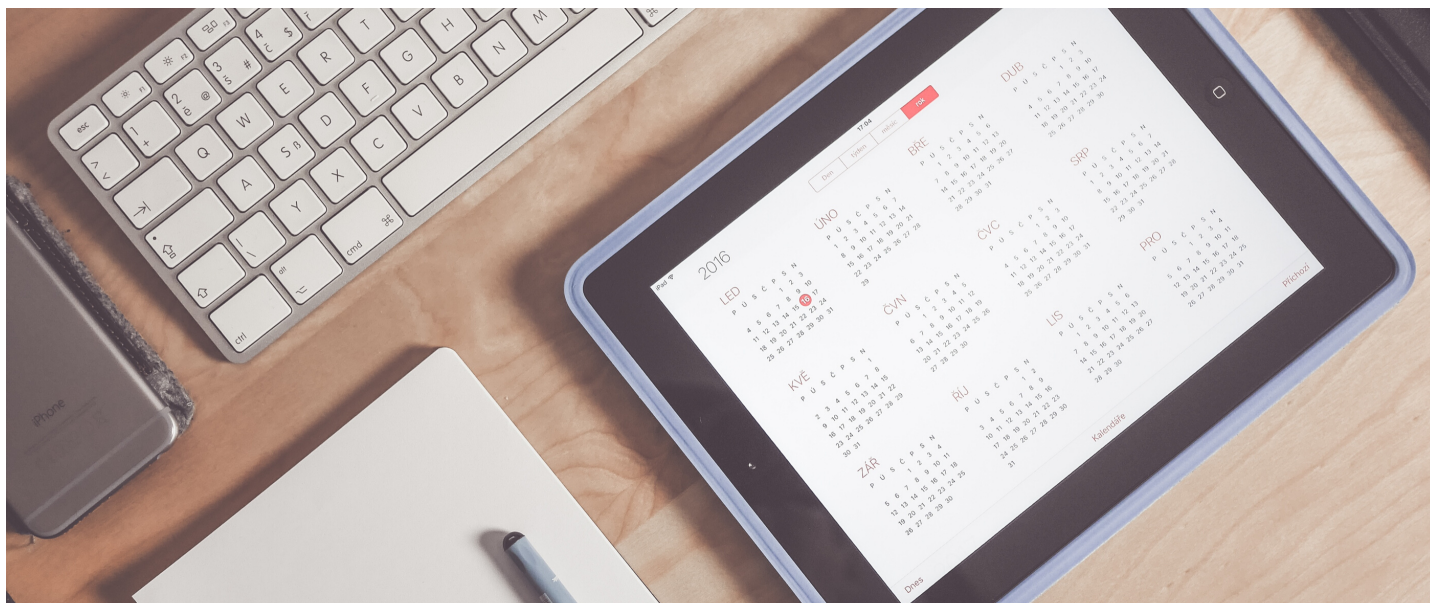


LOGICAL IN LOGISTICS NEWS



NOVEL CORONAVIRUS (COVID-19) & WORKING FROM HOME

Many logistics businesses in Australia are looking for ways to protect their staff from the COVID-19 pandemic.

One way of minimising the spread of the virus is for businesses to instruct their staff to work remotely, i.e. work from home. However, whilst we are all trying to curb the spread of this human virus, attention should also be paid to viruses spread in the information technology realm because remote work arrangements can have security implications and cybercriminals are attempting to take advantage of this.

Logistics businesses are starting to report COVID-19 scams being transmitted via email and text messages. Some examples include fake COVID-19 apps which, when accepted, give access to the data on the victim's mobile devices &/or computer. Others, such as the Maze ransomware, relate to hackers stealing files from their victims before locking the devices with ransomware-based encryption. The stolen files are then used as leverage by the Maze hackers, who threaten to make the data public unless the victims pay the ransom.

As can be seen, the cyber risks of flexible work arrangements could include malware infection, unauthorised information systems access, data security, and insecure devices used by your staff.

That's why it is important that logistics businesses and their staff ensure that remote access to business networks are secure, so they aren't vulnerable and valuable business information isn't exposed.

How does a logistics business go about ensuring that good cyber security measures are in place to address these cyber threats?



JAMES COTIS

Principal at Logical Insurance Brokers

To help answer that question, the Australian Signals Directorate's Australian Cyber Security Centre (ACSC) has produced some great advice to help businesses stay secure from cyber threats whilst managing a remote workforce, particularly their recently published threat update, COVID-19 Malicious Cyber Activity.

ACSC's advice includes:

- review your business continuity plans (BCP) and procedures;
- ensure that your systems, including Virtual Private Networks (VPN's) and firewalls, up to date with the most recent security patches;
- implement multi-factor authentication (MFA) for remote access systems and resources (including cloud services);
- ensure that your staff and stakeholders are informed and educated in safe cyber security practices, such as identifying socially engineered emails and messages;
- ensure your data is backup daily and automatically;
- increase your cyber security measures in anticipation of the higher demand on remote access technologies by your staff, and test them ahead of time;
- if you use a remote desktop solution, ensure it is secure;
- make sure staff working from home have physical security measures in place. This minimises the risk that information may be accessed, used, modified or removed from the premises without authorisation;
- ensure your work devices, such as laptops and mobile phones, are secure;
- ensure that you are protected against Denial of Service (DoS) threats.

We recommend that you carefully review this advice and compare it with your business's current arrangements.

Governments across Australia keep reminding us that we are living & working in unprecedented and challenging times and it is up to us as business owners to keep our people and IT systems safe.

We understand that business cashflows are currently under severe pressure. However, it is worth considering arranging Cyber insurance coverage. Quality Cyber insurance policies are designed to include staff working remotely. If a cyber event emanates from a computer, laptop or other device being used at home, these policies will respond to cover the cyber event, response costs, loss of profits and any potential litigation which may arise.

Who we are:

James and the team at Logical Insurance Brokers provide specialist risk management and insurance solutions to the logistics industry. Logical is delighted to be associated with the Freight and Trade Alliance (FTA) and is proud to be their appointed insurance adviser since its inception in 2012. James is also a regular presenter at FTA professional development events.

If you would like more information about how a carefully constructed insurance program and business continuity plans can help protect your business, please feel free to contact James on 02 9328-3322, email jamesc@FTAlliance.com.au or visit the Logical Insurance Brokers website at www.logicalinsurance.com.au/logistics.

Disclaimer: This article is general in nature and is designed to provide helpful general guidance on some key issues relevant to this topic. It should not be relied on as legal advice. It does not cover everything that may be relevant to you and does not take into account your particular circumstances and you use it at your own risk. Logical Insurance Brokers specifically disclaims any liability, whether based in contract, tort, negligence or otherwise, for any direct, indirect, incidental, punitive, consequential or other damage arising out of or in any way connected with the use of or reliance on the content of this article. It is only current as at the date of release. You must ensure that you seek appropriate professional advice in relation to this topic as well as to the currency, accuracy and relevance of this material for you.