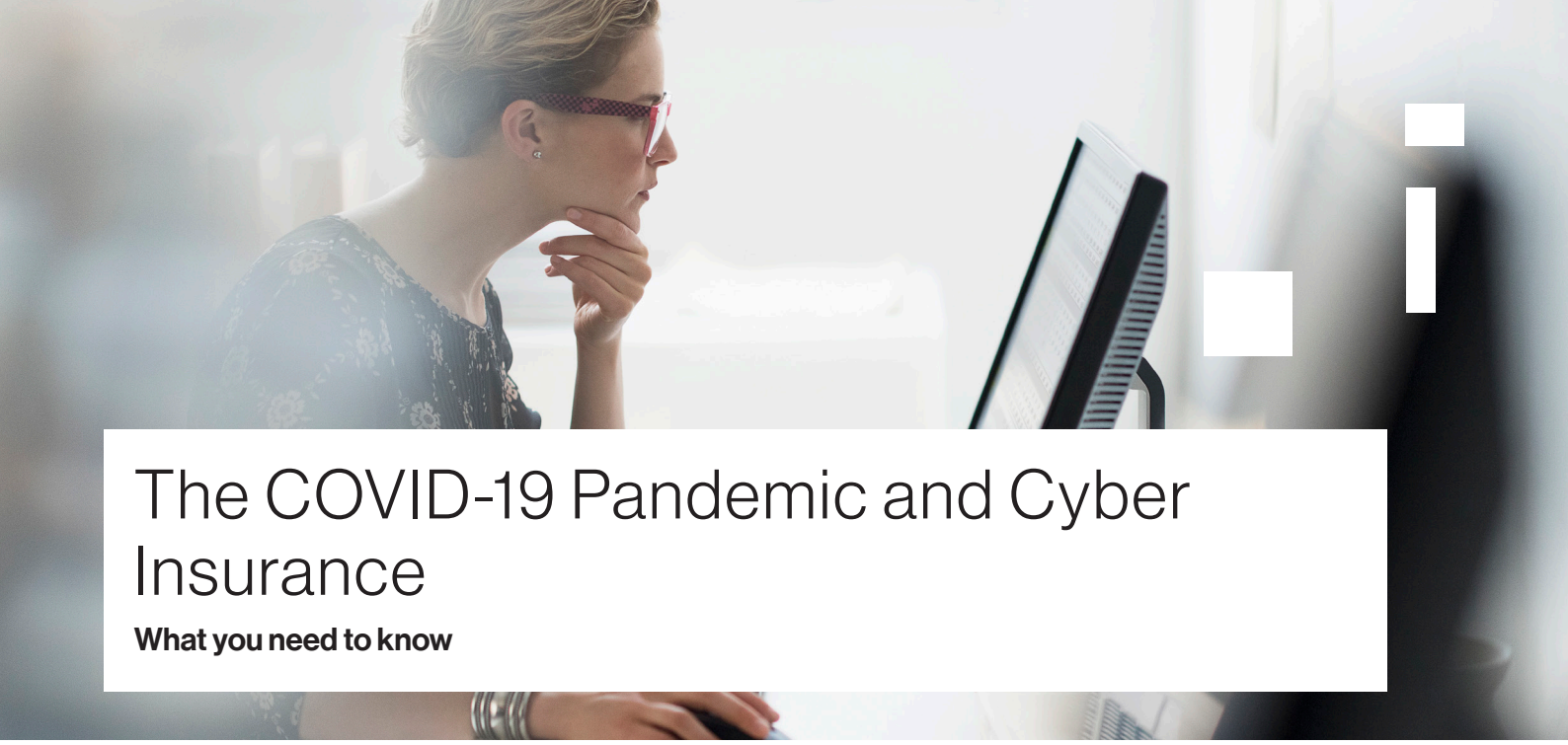

The COVID-19 Pandemic and Cyber Insurance

What you need to know

The unprecedented coronavirus (COVID-19) pandemic has impacted every major economy and industry and the local and global insurance market is no exception. The immediate challenges associated with the pandemic and the resultant economic downturn are likely to bring lasting effects to the insurance marketplace. Insurers are reviewing the coverage provided under their range of products and governments are introducing new laws which directly and indirectly impact risk and insurance. The situation is constantly evolving and Willis Towers Watson is collaborating globally to consider the insurance implications.

Numerous forms of ransomware and social engineering attacks are using COVID-19 fears to coerce employees into downloading malicious documents or visiting unsecure internet locations. Many of these attacks are designed to look like official communications from bodies such as the World Health Organisation, the Center for Disease Control and Prevention and various Health Insurers.

Where these attacks are successful they can result in password stealing, ransomware compromises, data exfiltration and system compromises.

COVID-19 is also causing changes in business processes which are increasing the attack surface for organisations. Many management procedures and business continuity plans require employees to work remotely, and to access systems using potential insecure personal devices.

Where workers are unable to attend offices in person, organisations require robust infrastructure to support continued operations which must also address identity management and information security requirements. Remote desktop services are a particularly common form of vulnerability that must be carefully secured and support with strong password management.

Third party intruders will also commonly use periods of business stress, or times when a business' IT resources are under strain to commit sophisticated attacks, given the company's underlying detection capabilities are likely to be compromised.

Any organisation which experienced a significant COVID-19 incident is likely to become a more attractive target for data system compromises.

Cyber hygiene will be particularly important for organisations at this time and consideration should be given to strategies which are in place to manage:

remote working conditions including how corporate laptops and other devices are encrypted and secured, patching and software vulnerability, identity management and data segregation;

the management of key data assets, and the extent to which they require additional protection;

the use of virtual private networks, as well as multi-factor authentication, automated logoff processes, geo-blocking and related security controls.

What is typically covered?

COVID-19 related risks are only likely to engage a cyber policy, where the underlying circumstances result in some breach of compromise of a sensitive data record in the care, custody or control of the organisation.

Where such a cyber event arises coverage is likely to be available, subject to the specific circumstances involved.

Willis Towers Watson

Organisations that sustain a data or system security event will generally seek the following support and cover under their cyber insurance policy:

- Cyber incident response costs such as:
  - those incurred for forensic investigations
  - legal advice on how to response to an event
  - notifying customers
  - notifying the regulator
  - public relations and
  - restoring or recreating data;
- the costs and payments necessary to end a ransomware event;
- loss of business income and extra expenses resulting from either:
  - a business or network interruption due to a cyberattack
  - a voluntary shutdown of a network to mitigate the impact of a pending or ongoing attack or
  - a system failure;
- regulatory costs relating to a data security event; and
- defence and settlement of a third party claim ultimately brought as a result of a cyber incident.

What is not covered?

Cyber wordings will generally not cover physical damage (fire, flood etc) resulting from a cyber-attack, or the extent to which a cyber-attack results in personal injury. Physical damage and personal injury however rarely result from cyber incidents.

Cyber policies contain a broad range of exclusions, which are unlikely to be directly engaged following a COVID-19 related event. Potential exclusion clauses that could be engaged include:

- reckless, criminal or wilful violation of any privacy laws or privacy regulations;
- employee and employer related disputes;
- breach of contract provisions or liability you have assumed;
- power outages or any failure of any system, infrastructure or network over which you have no direct control;
- physical injury or illness of any person (including death sustained as a result of such) except in relation to mental anguish or emotional distress;
- physical damage or destruction of any tangible property including resulting loss of use; or
- an act of terrorism by any person or group (cyber terrorism will however generally be covered by a cyber wording).

A reminder about claims

With business changing rapidly in response to the COVID-19 crisis, it is worth remembering that this type of insurance is written on a "claims made and notified" basis.

This means an organisation must notify their insurer of any known claim or any circumstance that could give rise to a claim before the policy period expires. Once the policy has expired, no claims or circumstances can be notified under it.

Please contact your insurance broker for further guidance on how to notify a claim or a circumstance that could give rise to a claim.

For further information

The Willis Towers Watson FINEX team can assist in interpreting coverage and help you manage this risk within your organisation. Please get in touch with your broker or consultant for further information.

About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has 45,000 employees serving more than 140 countries and markets. We design and deliver solutions that manage risk, optimise benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas — the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.

Information correct as at 3rd April 2020

Willis Australia Limited | ABN 90 000 321 237 | AFSL No. 240600
Willis New Zealand Limited | Company No. 111584 | FSP No. FSP37782
CKA Risk Solutions Pty Ltd | ABN 33 109 033 123 | AFSL No. 276915