# Advancing cyber resilience in a COVID-19 world

The COVID-19 pandemic has completely disrupted organisational perception and planning around strategic, operational, technological and financial risks. A key threat that is emerging is that of cyber risk. This is undoubtedly a time for organisations to remain alert given the increased opportunities for hackers due to work-from-home policies being stretched to unplanned levels.

Most organisations and their employees will find working from home to be an untested and uncertain environment. Why not log in via an accessible open network while your children are using all your home bandwidth on their devices? Or simply use one of the alternative conferencing tools or collaboration platforms out there which are free for download. Will the organisation's VPN be able to manage potentially thousands of remote log-ins, and will employees be able to identify social engineering campaigns which prey on their curiosity to know more about the virus?

This pandemic has brought to the forefront numerous risk considerations for both individuals and organisations across all industries, and questions on whether existing cyber insurance policies are adequate.

**Opportunity for hackers**

According to the United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the United Kingdom's National Cyber Security Centre (NCSC), Advanced Persistent Threat (APT) groups and cybercriminals are likely to continue to exploit the COVID-19 pandemic over the coming weeks and months. Key threats observed include:

- Phishing, using the subject of coronavirus or COVID-19 as a lure;

- Malware distribution, using coronavirus or COVID-19-themed lures;

- Registration of new domain names containing wording related to coronavirus or COVID-19; and

- Attacks against newly and often rapidly deployed remote access and teleworking infrastructure.

Most notably, these threats are commonly administered via basic social engineering techniques targeting employees by enticing them with COVID-19-related information to click on links and attachments containing malicious payloads.

**Mitigating cyber risk when working from home**

High volumes of employees logging in remotely may make it easier for cyber criminals, infiltrating a network through remote desktop services, to stay hidden in an attempt to identify and access systems with sensitive data. One has to wonder whether an organisation's crisis response, in the event of an actual cyberattack, will be compromised with less employees on site.

The advice to offer employees working remotely due to coronavirus concerns is no different than what has been offered previously when it comes to general cybersecurity hygiene. Anyone working remotely should ensure corporate laptops and other devices are locked when in public places and are using patched and updated software and operating systems, encrypted hard drives and automatic screen locks. Organisations should urge their employees to use a virtual private network (VPN) whenever working remotely, as well as multi-factor authentication to log into work-related services.

**Organisational response**

Organisations need to start adopting a holistic cyber risk management strategy which prioritises 'Resilience' while giving due importance to 'Security'. Cyber resilience can only be achieved with active engagement from the CEO and other members of the senior-management team. Cyber resilient organisations focus on an all-encompassing strategy that address the ‘People’, ‘Process’ and ‘Technology’ elements of cyber risk.

Key risk management considerations for organisations in the current times should include the following:

- Willis Towers Watson’s cyber insurance claims data shows that most cyber breaches are caused or enabled by employee negligence or malfeasance. Companies should review and revise their security policies and practices, ensuring a focus on employee training. Such training should remind them of phishing and social engineering threats.
- Ensure robust password requirements (complexity, length, diversity)
- Enforce the use of company-approved communication services (email, messaging, and conferencing via audio, web, and video) and prohibit the use of free online services.
- Implement and monitor intrusion detection system filters.
- Ensure user segmentation is in place, so employees have access to data and systems directly related to their specific tasks or departments.
- Monitor the vulnerabilities of third-party service providers used by remote workers.
- Consider transferring some of the risk exposure to a cyber risk insurance policy to mitigate potentially catastrophic incidents.
- Charting appropriate Business Continuity Strategy/IT Disaster Recovery Plans.

**How would cyber insurance apply?**

We expect cyber insurance coverage would be in place for claims and losses arising due to security failures and privacy events caused by the increased risk environment created by the pandemic situation. For example, a ransomware event or other cyberattack could undoubtedly lead to a plethora of costs, including as business interruption losses, forensic investigations, legal advice on how to respond to an event, notification costs, public relations and costs to restore or recreate data. For such events, we do not foresee any coverage issues caused primarily by the new pandemic environment.

On the other hand, limited coverage would be provided by a cyber insurance policy for a slowdown of company network due to difficulties supporting the increased demand arising from telecommuting arrangements. “Overuse” of the network would not likely constitute an unintentional or unplanned outage, administrative error, or programming error, and therefore the insurance policy would not be triggered.

Similarly, any elective coverage purchased for the voluntary shutdown of systems must be for the purpose of limiting the potential loss following the discovery of a security or systems failure. Therefore, any general shutdown of business operations due to the pandemic would not be covered by the organisation’s cyber insurance policy.

As companies navigate new ways of working during COVID-19, those with a strategic view of technology will find themselves with a competitive advantage during this challenging period.

[1] Alert (AA20-099A) COVID-19 Exploited by Malicious Cyber Actors - https://www.us-cert.gov/ncas/alerts/aa20-099a

## About the Authors:

**Jessica Wright**
Regional Associate Director, Cyber – Asia,
Willis Towers Watson
jessica.wright@willistowerswatson.com

**Sunny Goel**
Head of Financial and Executive Risks,
Willis Towers Watson India Insurance Brokers
sunny.goel@willistowerswatson.com

## 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 over 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.