Client Alert:

Cyber risk, coronavirus and insurance coverage

The outbreak of COVID-19 leaves many organizations vulnerable to cyberattacks. Now is as good a time as ever to review your cyberinsurance policy.

The outbreak of the COVID-19 (Coronavirus) over the past few months has brought to the forefront numerous risk considerations for both individuals and organizations across all industries. While the health and travel insurance markets may be more directly impacted in the near term, the impact on financial lines insurance should not be overlooked. With the expanding breadth of coverage available under traditional cyberinsurance policies, it is getting more difficult to find a risk that does not present a claim or loss scenario that potentially triggers a cyber policy.

Opportunity for hackers

While the inclusion of a bodily injury exclusion is standard on cyber policies, there are a number of different cyber exposures that the coronavirus could present. First and foremost, cyber criminals are already preying on the widespread fear that the coronavirus, now classified as global emergency by the World Health Organization, has created.[1] It is a perfect opportunity for hackers, adept when it comes to identifying vulnerabilities in infrastructure and defenses, to spread ransomware infections, malware and launch other cyber threat campaigns.

Indeed, malicious infections in the name of Wuhan coronavirus have already been reported to be in circulation in the U.S. and U.K. with similar threats on the horizon. Kaspersky's technologies have found malicious .pdf, .mp4 and .docx files disguised as documents relating to the coronavirus. Although the file names suggest that they include virus protection instructions, current threat developments and virus detection techniques, they actually contain a number of malware samples, such as Trojans and worms that could damage or encrypt data.

Work-from-home policies could increase vulnerability

In addition to an organization being more susceptible to a cyberattack due to employees' coronavirus fears, it is also possible that an organization's technological defenses will be more vulnerable than usual. As the coronavirus is causing more employees to work remotely, it is possible that those individuals are logging in remotely from a less secure network and perhaps using less secure hardware.

Further, 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

[1] https://usa.kaspersky.com/blog/coronavirus-used-to-spread-malware-online/20213/

sensitive data. One has to wonder whether an organization'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. Organizations 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.

Would cyberinsurance apply?

It is important to recognize that an organization would likely be protected for the above-referenced exposures by a stand-alone cyberinsurance policy. The costs and payments necessary to end a ransomware event would likely be covered under a policy's cyber extortion section. A ransomware event or other cyberattack could undoubtedly lead to a plethora of cyber incident response costs, such as those incurred for forensic investigations, legal advice on how to respond to an event, notifying customers, public relations and restoring or recreating data.

There would also likely be coverage for the 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, which would not require an actual cyberattack. Lastly, a cyber policy's network security and privacy liability insuring agreement would be available to defend third party claims brought as a result of the cyber incident.

Each applicable policy of insurance must be reviewed to determine the extent, if any, of coverage for COVID-19. Coverage may vary depending on the jurisdiction and circumstances. For global client programs it is critical to consider all local operations and how policies may or may not include COVID-19 coverage.

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, optimize 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.

Contact

Jason Krauss
FINEX Cyber/E&O
Thought and Product Leader
+1 212 915 8374
jason.krauss@
willistowerswatston.com

willistowerswatson.com/social-media