wotton kearney

Client Update

Shaping the future of insurance law

Preying on the vulnerable – cyber claims predicted to rise due to COVID-19

31 MARCH 2020

AT A GLANCE

- Insurers are likely to see an increase in cyber claims in the upcoming months due to the impact of the coronavirus on businesses.
- Businesses have had to accommodate remote working rapidly, leaving many with a range of increased cyber security exposures.
- Other businesses have been forced to close their doors temporarily or permanently, which makes them a prime target for cyber criminals.
- There are already phishing scams using COVID-19 related messages to lure anxious individuals and the number of these is expected to rise.
- OAIC has recently provided guidance to remind businesses of their privacy obligations and ensure compliance with legal obligations given the challenges faced with COVID-19.

Coronavirus (COVID-19) is potentially the largest ever cyber-security threat to face businesses and consumers. The new norm is leaving businesses – which are already under pressure – more vulnerable to attacks than ever before. As businesses adjust, COVID-19 related cyber claims will spike in the weeks to come due to three key cyber vulnerabilities facing businesses: remote working, targeting of key organisations, and phishing scams.

REMOTE WORKING

System vulnerabilities

Many businesses are underprepared to have the majority (if not all) of their workforce working remotely. They have been forced to adapt their systems quickly to enable their employees to safely work from home. CNBC recently conducted a survey with its technology executive council, comprising senior technology executives within large companies, government and non-profit organisations. Of particular note, 53% said their firms had never stress-tested their systems for an event like COVID-19 that requires their entire workforce to work from home.[1]

In the haste to adapt systems for remote working, security policies may not have been properly implemented. There could be issues with technical and administrative controls, such as improper VPN configurations, installation of less robust versions of software, and failure to install regular updates and patches, particularly considering IT departments are currently overwhelmed and stretched.

[1] https://www.cnbc.com/2020/03/20/phishing-spam-spike-as-hackers-use-coronavirus-to-hit-remote-work.html

Employees are also now accessing company data from a range of devices, including personal devices. This creates an increased risk of exposure for organisations if personal devices and accounts are compromised. There has also been a surge in the use of third-party virtual conferencing and other collaboration tools, all of which are likely to attract opportunistic cyber criminals. Zoom, in particular, has been publicly criticised recently for its security vulnerabilities at a time where its usage is surging.[2]

In a 2019 study published by data storage solutions provider Apricorn, one third of IT decision-makers admitted their organisations had suffered a data breach as a result of remote working.[3] The biggest problem cited was the complexity of managing all the technology employees require for remote working, and a lack of control over where company data is stored. Notably, this was before COVID-19 when a much smaller portion of employees were working remotely.

The Australian Cyber Security Centre (ACSC) issued guidance on working remotely in connection with COVID-19. It recommends a number of security measures to prevent cyber threats, including implementing multi-factor authentication for remote access systems and ensuring systems are up-to-date with the most recent security patches.

Insight from W+K:

2020 has already seen an increase in ransomware attacks with higher ransoms being demanded in conjunction with data exfiltration threats.

We predict this trend will continue to grow at an even faster pace, with hackers targeting system vulnerabilities of remote workers, exploiting either business or home network vulnerabilities.

We foresee a further increase in ransomware attacks preying on the increased vulnerability and anxiety of companies with a continued increase in higher ransom demands.

Based on our experience in handling cyber claims over a number of years, many businesses big and small do not yet have in place the security measures recommended by the ACSC. Working from home provides an even larger attack surface for hackers.

Smart home technologies

The existence of smart technologies in people's homes increases the risk and vulnerability to attack by cyber criminals. It also increases the risk of a data breach via the inadvertent disclosure of sensitive business information.

While providing convenience within the home, for example allowing you to order toilet paper when you run out (although perhaps more difficult at the moment), listening devices like Amazon's Alexa or Google's voice assistant present a risk of confidentiality breach or data leakage when working from home.

Voice assistants are not the only risk as video products, such as Ring, baby monitors and closed-circuit TVs, all run the risk of causing inadvertent disclosure of data as well as historically being vulnerable to attacks. At a more basic level, sensitive files or client information could be visible in the background when videoconferencing.

TARGETING OF KEY ORGANISATIONS OR SECTORS

Business closures

Many businesses, including restaurants, pubs, casinos, cinemas, retail stores and gyms, have been forced to close by the government as a result of COVID-19. These forced closures provide a perfect blueprint for industries to target as businesses are mothballed, systems are left unattended, and employee reaction time is much slower.

For the businesses that close permanently, a cyber-attack would be concerning for creditors who may be unable to recoup monies owed to them in the future.

For businesses that have closed temporarily and have already been impacted financially by COVID-19, dealing with the financial and reputational damage that arises from a cyber-attack could be the difference between a temporary break and permanent closure.

[2] https://www.bbc.com/news/technology-52033217
[3] https://www.continuitycentral.com/index.php/news/technology/4022-almost-two-thirds-of-data-breaches-are-a-direct-result-of-human-error

Insight from W+K:

As a result of COVID-19, we expect a significant increase in business email compromise (BEC) scams and invoice fraud, particularly as businesses close and become more desperate for cash flow with money outstanding to suppliers or owed by customers.

This creates the perfect storm for social engineering with businesses chasing down payments before their doors are closed for lockdown.

Targeted sectors

According to a report from global insurer Beazley, 2019 saw a 131% rise in the number of ransomware attacks compared with the previous year. Of the ransomware incidents in 2019, the healthcare sector suffered 35% of attacks, more than any other sector. Financial institutions were targeted in 16% of the attacks, while 12% targeted the education sector and 9% occurred in professional services.[4]

The potential for further ransomware and other cyber-attacks on our already stretched healthcare sector in 2020 looms large. Some ransomware operators have publicly stated they will not target health and medical organisations during the COVID-19 outbreak, although it remains to be seen whether this was the voice of a couple or many.[5] In fact incidents have already been reported since the outbreak of COVID-19.

On 14 March, Hammersmith Medicines Research, a UK medical facility on standby to help test a COVID-19 vaccine, suffered an attempted ransomware attack.[6] On 15 March, the US Health and Human Services Department suffered a cyber-attack on its computer systems.[7] The World Health Organisation (WHO) also reported a two-fold increase in cyber-attacks this month.[8]

Public authorities may also be targeted in the upcoming weeks. Although the reported denial of service (DoS) attack on the MyGov website on 23 March was later determined as false, increased dependency on online services is likely to lead to a rise in DoS attacks. Australians will remember the attack on our first ever online census in 2016, which caused much embarrassment for the government at the time. Accordingly, websites providing information or assistance expecting an increase in visitors are a key target.

PHISHING SCAMS USING COVID-19 RELATED MESSAGES

A surge of COVID-19 themed phishing campaigns has been detected since January 2020, including malicious messages purportedly sent on behalf of the Australian Medical Association and global bodies such as the WHO. Crowdstrike has reported a surge in phishing campaigns using COVID-19.[9] Crowdstrike CEO, George Kurtz noted "now is the time, when there's chaos and there's fear and people are worried about their family [and] they're not in the office ... they're going to strike."

The Australian Competition and Consumer Commission's (ACCC) Scamwatch has received 94 reports of COVID-19 related scams since the beginning of this year and, concerningly, warns the figures are climbing.[10] Phishing scams, sent via email or text message, claim to be providing official information on COVID-19 but are attempts to "phish" for personal information.

Multiple reports to Scamwatch related to a text message appearing to be sent from 'GOV', which included a link to find out when to get tested in their area for COVID-19. If the link was clicked on, malware was installed, designed to steal user's bank details. Another reported scam was an email that requested the user to provide certain credentials to receive government benefits.

[4] https://www.cyberscoop.com/ransomware-beazley-insurance-claims/
[5] https://www.teiss.co.uk/hacker-groups-wont-target-healthcare-organisations/
[6] https://www.forbes.com/sites/daveywinder/2020/03/23/covid-19-vaccine-test-center-hit-by-cyber-attack-stolen-data-posted-online/#3be7ed2718e5
[7] https://tech.newstatesman.com/security/us-health-human-services-department-cyber-attack
[8] https://www.forbes.com/sites/daveywinder/2020/03/25/hackers-target-world-health-organization-as-cyber-attacks-double-during-covid-19-pandemic/#165f14a72e5c
[9] https://www-cnbc-com.cdn.ampproject.org/c/s/www.cnbc.com/amp/2020/03/20/crowdstrike-sees-phishing-attack-uptick-during-coronavirus-crisis.html
[10] https://www.scamwatch.gov.au/news/warning-on-covid-19-scams

Insight from W+K:

The majority of BECs and ransomware attacks are perpetrated by phishing emails. These emails need to be convincing enough for the user to either open a document or enter their log-in credentials into a website.

COVID-19 provides the perfect platform for hacker email credibility, playing on an increased anxiety and curiosity about COVID-19 leading to an increase in rate at which documents are opened and credentials are entered.

Businesses are now at a heightened risk of phishing scams. In an office environment, employees often check with their colleagues on the legitimacy of suspicious emails. With no colleagues present when working from home, combined with the emotional toll of the global health pandemic, employees are much more likely to fall victim to these scams.

There have been reports of cybercriminals targeting users of online videoconferencing platform Zoom, with malicious files being sent from fake Zoom domains.[11] As a result, users are being advised to carefully inspect any Zoom links or documents messaged to them via the platform, to ensure they are genuine.

Once a cyber-criminal obtains an employee's credentials, they typically use them to monitor emails and commit financial and social engineering fraud. Once the back door is open and the systems vulnerable, cyber criminals also have the opportunity for lateral movement around the business' network potentially leading to more opportunity to steal sensitive corporate and personal information, and ransomware.

The OAIC has recently provided guidance to help businesses understand their privacy obligations in the context of COVID-19 and ensure ongoing compliance despite the challenges faced.

Businesses should continue to be mindful of their notification obligations in Australia under the *Privacy Act 1988* (Cth) and in other jurisdictions, as businesses will still need to comply with such legal obligations during this pandemic.[12]

KEY TAKEAWAYS FOR INSURERS

Insurers are likely to receive an increase in cyber claims in the upcoming months. Numerous COVID-19 related attacks have already been reported since the outbreak, and the numbers will continue to rise with increased numbers of employees working from home and the temporary closure of numerous businesses already susceptible to attack.

Now more than ever, businesses need to be mindful of their processes and procedures, ensuring they are adaptable to remote working environments and that established verification procedures of emails and payments remain in place so that the financial risks posed by COVID-19 are not exacerbated.

“There have been reports of cybercriminals targeting users of online videoconferencing platform Zoom, with malicious files being sent from fake Zoom domains.

[11] https://thehackernews.com/2020/03/zoom-video-coronavirus.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Cyber+Security+Blog%29&m=1

[12] https://www.oaic.gov.au/privacy/guidance-and-advice/coronavirus-covid-19-understanding-your-privacy-obligations-to-your-staff/

Need to know more?

For more information please contact us.

Kieran Doyle
Partner & Cyber Leader, Sydney
T: +61 2 8273 9828
E: kieran.doyle@wottonkearney.com.au

Eden Winokur
Special Counsel, Sydney
T: +61 2 8273 9942
E: eden.winokur@wottonkearney.com.au

Ellie Brooks
Associate, Melbourne
T: +61 3 9604 7987
E: ellie.brooks@wottonkearney.com.au