HERBERT SMITH FREEHILLS

COVID-19: PEOPLE: FIVE PRACTICAL STEPS TO MANAGING YOUR CYBER SECURITY RISK DURING A CRISIS (GLOBAL)

24 March 2020 | Global
Legal Briefings – By **Julian Lincoln, Partner, Michelle Curran, Senior Associate and David J Ryan, Senior Associate**

The COVID-19 pandemic has created a range of unexpected technology, intellectual property and data related challenges for all businesses. Organisations are doing everything they can to face these risks head on while maintaining business continuity.

The security of organisations' networks and their valuable IP rights, confidential materials and personal information is one of these challenges and runs across the entire landscape of businesses' operations. Organisations must respond early and with vigilance to manage and mitigate these risks, to ensure that information they hold, their reputations and their networks are protected.

With working from home now the status quo, organisations face increased cyber security risks, including greater exposure to data vulnerabilities and data breaches and heightened activity of malicious threat actors capitalising on the uplift in the use of remote access technology.

All organisations can take the following practical steps to improve their cyber security posture in the context of the impacts of COVID-19.

PREPARE FOR EMAIL-BASED ATTACKS

Phishing emails containing COVID-19 related information, purportedly being sent by legitimate global organisations, are being targeted at remote workers. Individuals who work from home may be doing so from their personal computers, rather than organisation provided devices, increasing the likelihood that these attacks may circumvent an organisation’s security controls. Today’s cyber actors use sophisticated malware which, when clicked on, can lead to the disclosure of large amounts of confidential and personal information and the theft of remote access logins.

- *Have you provided guidance to your personnel on phishing emails? For example, personnel should be advised to:*

- *Watch out for unexpected or poorly written emails*
- *Check the email addresses of any unknown or unusual senders*
- *Avoid clicking on any embedded links*
- *Immediately report and delete suspected phishing emails*

EDUCATE PERSONNEL ABOUT CYBER SECURITY RISKS

Cyber criminals thrive on crisis situations, which means that remote access scams will no doubt be on the rise, and, if successful, could have a devastating impact on an organisation's business. Personnel should be made aware of the potential for threat actors to steal remote access user credentials, including less sophisticated methods like contacting the employee and pretending to be a member of their IT department. As part of their cyber security framework, organisations should ensure that robust remote working procedures are implemented.

- *Have you reviewed your cyber security policies to assess whether they appropriately address the risks related to large scale remote working?*

- *Have you established IT support tailored for remote working and advised your personnel how they can securely deal with IT related issues that require external support?*

CYBER SECURITY TRAINING

It is standard practice for organisations to require personnel to carry out annual cyber security training. Organisation-wide awareness of heightened cyber security threats is critical to combating cyber risk and being able to respond rapidly to any events that occur.

Personnel who are well educated on the importance of cyber security and what they can practically do (and not do) to ensure organisations are protected, are a key component of mitigating cyber security risk.

- *Have you required personnel to undertake a refresher of cyber security training?*
- *Have you circulated your information security policies and procedures to all personnel as you move to a remote working operating model?*
- *Do your personnel know who to contact if they become aware of a cyber threat or data breach?*

CYBER SECURITY PRACTICES

The Government authorities and cybersecurity standards bodies are reminding organisations of the importance of incorporating cyber security into contingency planning. This includes increasing cyber security measures, testing remote access technologies ahead of time, ensuring that all systems are updated with the most recent security patches, and making sure that all work devices are adequately secure.

- *Do you need to update cyber security protocols and practices to meet new information security risks presented by COVID-19?*

It is also crucial that organisations remain across official cyber security updates and implement proactive not reactive measures to address emerging and increased risks.

- *Is your Cyber Security team implementing enhanced monitoring of cyber threat activity across your network and engaging with updates from external information security authorities?*

PHYSICAL SECURITY MEASURES

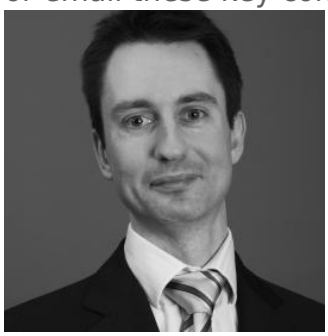
Although organisations should be discouraging personnel from removing commercially sensitive and confidential information from the office, or printing documents at home, the reality is that this will be difficult to enforce. To mitigate the risk of unauthorised access, organisations should implement robust physical security procedures and plan for how personnel will destroy this information once it is no longer required.

- *Have you notified your personnel of policies regarding protection, secure storage and destruction of any physical documents they hold in the context of remote working?*

Taking practical steps like those outlined here will help ensure that your organisation is well equipped to proactively plan for and respond to COVID-19 related cyber security threats. This ability to effectively and swiftly mitigate and respond to cyber risks as they arise, will enable you to maintain focus on running your business in these challenging times.

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.



JULIAN LINCOLN
PARTNER, HEAD OF TMT & DIGITAL AUSTRALIA, MELBOURNE

DAVID J RYAN
SENIOR ASSOCIATE, MELBOURNE
+61 3 9288 1831
david.j.ryan@hsf.com

PETER JONES
PARTNER, SYDNEY
+61 2 9225 5588
peter.jones@hsf.com

KAMAN TSOI
SPECIAL COUNSEL, MELBOURNE
+61 3 9288 1336
kaman.tsoi@hsf.com

+61 3 9288 1694
Julian.Lincoln@hsf.com

MERRYN QUAYLE
PARTNER, MELBOURNE
+61 3 9288 1499
merryn.quayle@hsf.com

NICK PANTLIN
PARTNER, HEAD OF TMT & DIGITAL UK & EUROPE, LONDON
+44 20 7466 2570
Nick.Pantlin@hsf.com

ANDREW MOIR
PARTNER, INTELLECTUAL PROPERTY AND GLOBAL HEAD OF CYBER & DATA SECURITY, LONDON
+44 20 7466 2773
Andrew.Moir@hsf.com

LEGAL NOTICE