Cybersecurity and COVID-19: Opportunities for change in the face of challenge

March 2020

COVID-19 is not the first and will not be the last pandemic, but it is the first one that has brought the importance of cyber resilience and adaptability in the era of global trade to the forefront of many businesses' minds.

Many businesses have been understandably focused on continuing to trade. While this is obviously a critical concern there could be a risk that it distracts from ensuring that appropriate security measures are put in place to protect personal and commercially sensitive data. The National Cyber Security Centre (NCSC) report that malicious actors across the globe are already trying to capitalise.

In the UK, the National Fraud Intelligence Bureau (NFIB) has identified multiple reports of fraud involving coronavirus links to date, with losses to victims totalling close to £1m. This is likely the tip of the iceberg both because victims are not obliged to report to NFIB and because the UK has only experienced the first few weeks of what is predicted to be a significant period of disruption.

Some of the most common sources of risk, particularly where commercial or IT decisions are being made at a rapid pace are:

- Phishing emails referring to the need to use new access protocols which request employees' login credentials and emails relating to virtual signing services in the absence of being able to provide "wet ink" signatures.

- Payment misdirection and social engineering emails appearing to originate from a genuine colleague or supervisor's account (such account already having been compromised) to share information or make a payment, particularly in relation to a time-sensitive commercial matter.

- Employees being provided with hardware (or being allowed to purchase their own to be reimbursed) to enable them to work more effectively from home but where those devices have not been set up with the same security measures (eg thumb drives, laptops).

- IT teams having to quickly establish or expand remote access solutions where there are limited tokens of VPN access leading to insecure access/file sharing methods being used without, for example, implementing multi-factor authentication.

- Unsecured remote data ports being created or left open which may allow malicious actors access to a business' system.

Risk Mitigation

In order to deal with data security breaches quickly and effectively, recovery plans should ideally be developed and tested in advance. Managerial and technical staff should be aware of their different roles and responsibilities and the steps that need to be taken in the event of a breach. Data breach prevention and planning to reduce the risk of an incident and to ensure readiness to respond should a breach occur could prove to be significant. Some suggestions follow:

- Review insurance policies for cyber cover.

- Ensure incident response plans take into account remote working procedures and contains a list of up-to-date vendor-contacts (e.g. insurance broker, external legal counsel, forensic IT, PR)

- Ensure contact details are exchanged and updated effectively in order to be able to respond to an incident quickly; consider using a call tree/waterfall as part of this.

- Communicate with employees about the policies and procedures that apply to remote working and stress the need for increased vigilance, especially around outgoing and incoming payments and requests for changing or sharing credentials. As part of this, consider putting in place, or refreshing, training for employees on cyber security. The NCSC guidance pages are a good place to start.

- If someone is working remotely, they are working on a network not directly controlled by their business, so consider implementing multi-factor authentication, access to networks and servers via VPN and encryption of thumb drives.

- Assess your data backup solution to ensure it will be capturing all data as required but also that the backup is not itself vulnerable to attack.

Our US partners, Hinshaw, have also produced guidance which contains further risk mitigation steps and can be accessed here.

Taking the opportunity to recalibrate

The silver lining is that, whether by virtue of wanting to be proactive or as part of a post-cyberattack recovery and improvement plan, those businesses that capitalise on the opportunity to invest the time and financial resource to deploy secure, workable, long-term remote-working solutions for their workforce, stand to benefit in the long term. Attitudes to home working might change considerably following the current disruption and having flexible but secure infrastructure options could be a longer-term commercial advantage.

Contacts

RPC

Richard Breavington
Partner
+44 20 3060 6341
Richard.breavington@rpc.co.uk

Daniel Guilfoyle
Senior Associate
+44 20 3060 6912
Daniel.guilfoyle@rpc.co.uk

Ridvan Canbilen
Associate
+44 20 3060 6314
Ridvan.Canbilen@rpc.co.uk