Mitigating the Risk of COVID-19 on Your Cyber Security
The World Health Organisation (WHO) has declared COVID-19 a global pandemic.

We are living in unprecedented times. The outbreak of coronavirus has caused immeasurable damage and disruption to businesses worldwide. Many of us are fortunate enough to be able to work from home, which slightly mitigates this disruption.

However, moving to remote working at such a pace brings its own challenges – particularly relating to cyber security.

Amidst the fear and uncertainty, we’re seeing a rise in cyber attacks from phishing to ransomware. If businesses do not communicate and collaborate effectively, cyber criminals will use this to pass through the gaps in communication and continue to infiltrate businesses.

This document is aimed at helping coordinate an international response to cyber threats to businesses during this uncertain period, and to offer advice on how you can mitigate risks to your business.

We’ve identified three key steps to mitigate risk and bolster your cyber security:

**Security**
- Lock down security in your employees remote working environments.

**Proactivity**
- Put the solutions and procedures in place to prevent sophisticated cyber activity.

**Continuity**
- Ensure your data backup plan is robust enough to meet the demands of remote working.
Contents

Potential Threats to your Business ............................................... 1 - 2
The Far-Reaching Implications .................................................. 3 - 4
How Businesses Can Mitigate Risk ........................................... 5 - 8
Resources ...................................................................................... 9

If you would like to find out more, we would be delighted to hear from you on 01283 753 333 or at hello@neuways.com.
Potential Threats to Your Business

Operations Over Security

Many businesses are trying to provide their customers with the expected level of support to keep them going, whilst also dealing with potentially terminal financial and operational challenges. Unfortunately, security can be pushed further down the priority list, meaning that critical cyber resilience measures are passed by. This, in turn, increases risk.

Lack of IT Resources

As the rate of infection rises, and staff self-isolate for precautionary measures, many departments will find themselves stretched due to employee absence. The rapid shift to mass remote working is likely to affect cyber risk management, with IT departments resourced to cope with both internal setup issues.

Breakdown of Supply Chain

The flow of the supply chain is delicate. If supply breaks down at one point, it will cause a ripple effect on many businesses. This is especially true in the IT sector where stock has been scarce.
Lack of Familiarity with Technology

With the move to mass remote working, many employees are being asked to work in ways they might not have worked before. Remote working is routine to plenty of people, but many more have never done it before. Lack of knowledge when it comes to using a VPN or other remote access technologies can, and will, impact productivity. This again, will have a direct impact on the ability for a business’s technical team to address security issues.

Targeted Cyber Crime

Cyber criminals are taking advantage of the fear and uncertainty surrounding COVID-19, using all manner of means to trick victims. Whether it’s impersonation of the World Health Organisation (WHO), or other trusted authorities such as local and national government, there are a range of COVID-19 scams in circulation that are causing severe disruption to businesses.
The Far-Reaching Implications

As businesses scramble to mitigate the financial impacts of COVID-19, security will suffer. This doesn’t guarantee that an organisation will suffer a cyber attack. However, it does increase the risk of being targeted due to a combination of emerging attack methods and the limited capacity for an organisation to respond.

Gaps in cyber security regime

Patch hygiene is something that some businesses struggle to keep on top of in ordinary times, either due to apathy or lack of awareness. However, it’s even more important that organisations continue to update their software and devices with patches. Failure to do this will increase risk of cyber security breaches in a significant way.

Another threat could come from inside businesses. With many organisations having to lay off swathes of their workforce in order to stay afloat, rogue employees at risk of redundancy could seek to cause damage on their way out. Unlikely as it might seem, people can get desperate in times like these – and some just want to cause long-lasting damage for perceiving to have been wronged.

Downtime

The cost of cyber crime is already enormous, with downtime comprising of much of the cost. In fact, downtime alone is costing businesses around £250,000 per hour (on average). With IT resources stretched and budgets slashed, downtime is far more likely, if an organisation has not equipped its staff with the means to fulfil their role.

Lack of awareness

If businesses don’t maintain and review clear Remote Working IT Guidelines, or fail to provide staff with the knowledge required to use software or equipment securely, they’re at risk of being exploited by a cyber criminal.
Severe financial implications

With potential downtime and gaps in cyber security comes a cost. Organisations are understandably trying to save money in order to keep running, but without the right IT infrastructure in place, businesses could find themselves going bankrupt.

Ransomware, for example, can cripple businesses in normal circumstances, if they don’t have a sufficient backup and business continuity plan, but the current threat landscape puts businesses under intense operational pressure. Sustained downtime could lead to bankruptcy.
How Businesses Can Mitigate Risk

In short, businesses can take three key steps to mitigate emerging risks to cyber security.

Security

1. Secure sensitive data
   Ensure all corporate devices are encrypted. This means that if they are lost or stolen, nobody can access the information stored on the device. If staff are using mobile devices, then implement a Mobile Device Management (MDM) policy with remote wiping. This allows data to be wiped remotely by the administrator, in the event that a mobile device or tablet is lost or stolen.

   Implement the Principle of Least Privilege (PoLP) for all staff. PoLP means limiting staff access to only the data and services they require in order to perform their job. This is a prudent data security technique because it prevents employees from accessing sensitive corporate data, if they don’t need to. This means that if a staff member’s account becomes compromised, there is very little the hacker can do.

   Staff will be required to work more collaboratively in the absence of an on-premises location. This means that all staff members must have the ability to share files and documents securely.

Continuity

24/7

Proactivity

Lock down secure remote environments for all staff
Administrators must also maintain a data access audit, ensuring that they’re aware of who is accessing corporate data, when they accessed it, and what was altered.

2. Secure Endpoints
Make sure all devices are patched and fully up-to-date, including critical functions such as endpoint and network security solutions. These must be administered centrally, ensuring that all staff benefit from these updates.

Distribute collateral to staff on how to spot phishing attacks, if possible. This will protect them, and the business as a result.

Roll out multi-factor authentication (MFA) for all solutions that are connected to the internet. Staff can be enrolled to receive ‘tokens’ via text or email, or a notification to their mobile device. MFA is proven to prevent up to 99% of account-based breaches, so it must be a priority.

All home users must use WPA-2 protection on their home WiFi network. Many home networks are set to WPA-2 as standard, but not all. Implementing this extra security measure makes it much harder for criminals to access the home network and steal corporate data.

Maintain Continuity of Cyber Security Functions

1. Have a Pandemic Preparedness Plan
A Pandemic Preparedness Plan is usually part of an organisation’s wider business continuity plan. Through this, organisations can identify the key contributors to downtime, and the services required to keep the business running as normal.

The full business must be aware of the Pandemic Preparedness Plan, and its procedures, in order to fully benefit.

2. Ensure automated processes are running correctly
If patching or backup procedures are set up to function ‘by exception’ (only notified if something is wrong), then do a periodic manual check to verify that all is working as it should be.

This also includes ensuring that patches can be delivered remotely to staff that are not on the internal network.
3. Make Staff Aware of the Incident Response Plan

A strong incident response plan can be the difference between a minor situation that is handled swiftly and costly downtime. All staff must be aware of who to inform if they have an issue, and what their responsibilities are.

Be proactive with cyber security (where possible)

1. Guidance and Awareness for Employees

Issuing clear guidance to employees on what not to do if they receive an email they’re not expecting, requesting payment. With staff working remotely more frequently as a result of the outbreak, cyber criminals are using social engineering methods to move between the lines of communication and trick employees.

Knowledge really is power. Equip all staff with official guidance on how to spot phishing emails, encourage a culture of communication so people feel able to report suspected cyber attacks, and ultimately – be clear on all cyber security procedures.

Whilst this isn’t a priority in the first few weeks of remote working, organisations that empower their staff to actively following best practices will be far more secure in the long term. Make sure that information and advisories reach staff as they are published.

2. Enhanced email filtering

Ensure that email filtering is set up to be highly discriminate.

This will prevent ransomware-borne emails, and some phishing attempts, from reaching end users. Many solutions offer the ability to ‘sandbox’ incoming communications that might be suspect, allowing staff to view the email in a safe and controlled environment, before deciding whether it’s a threat or not.
3. **Invest in a MSP with threat detection and remediation**
   Many businesses now find it far more expedient to outsource their cyber security to a MSP (managed service provider) on a co-managed IT basis. This means that an organisation’s internal IT have the support and experience of a dedicated cyber security team on hand.

   It also means that the internal IT team can concentrate on getting staff set up securely, and dealing with any queries, whilst the MSP function scopes out potential threat to cyber security.

4. **Identify Internal Threats**
   Identify ‘at risk’ employees. This might be staff who are soon to be made redundant, who the business has reason to suspect might be disgruntled. It could also be less cyber security-savvy staff who are less inclined to follow protocol.

   You may consider putting additional data loss prevention policies and restrictions in place for the ‘at risk’ category, as a secure measure.
Resources

In the meantime, we’ve compiled some resources to help you adjust to remote working, and to keep you safe.

- Getting Started with SharePoint
- Setting up Meetings with Teams
- Small Business Cyber Security Guide
- Microsoft Teams: 10 Tips to Tackle Your Day
- What is Your Remote Working Data Backup Plan?
- Your Guide to Multi-Factor Authentication
- Who is responsible for your data security in the cloud?
- Your Coronavirus Pandemic Preparedness Plan
- Security Guidelines for Remote Workers
What next?

The Security Experts at Neuways can help you secure your business.

Speak to one of our consultants today to find out more:

www.neuways.com

01283 753 333