Impacts of COVID-19 on cyber security:

Managing a remote working environment.

pwc

Managing a remote working environment

The COVID-19 outbreak has been declared a pandemic by the World Health Organisation, causing huge impact on people's lives, families and communities. This has had an immediate effect on organisations, changing the ways employees work and bringing with it new cyber risks.

As the international response continues to develop, we know that organisations are facing potentially significant challenges to which they need to respond rapidly. Many organisations and employees need to rethink ways of working in light of considerable operational and financial challenges. Without appropriate consideration, this could fundamentally increase the risk of cyber security attacks.

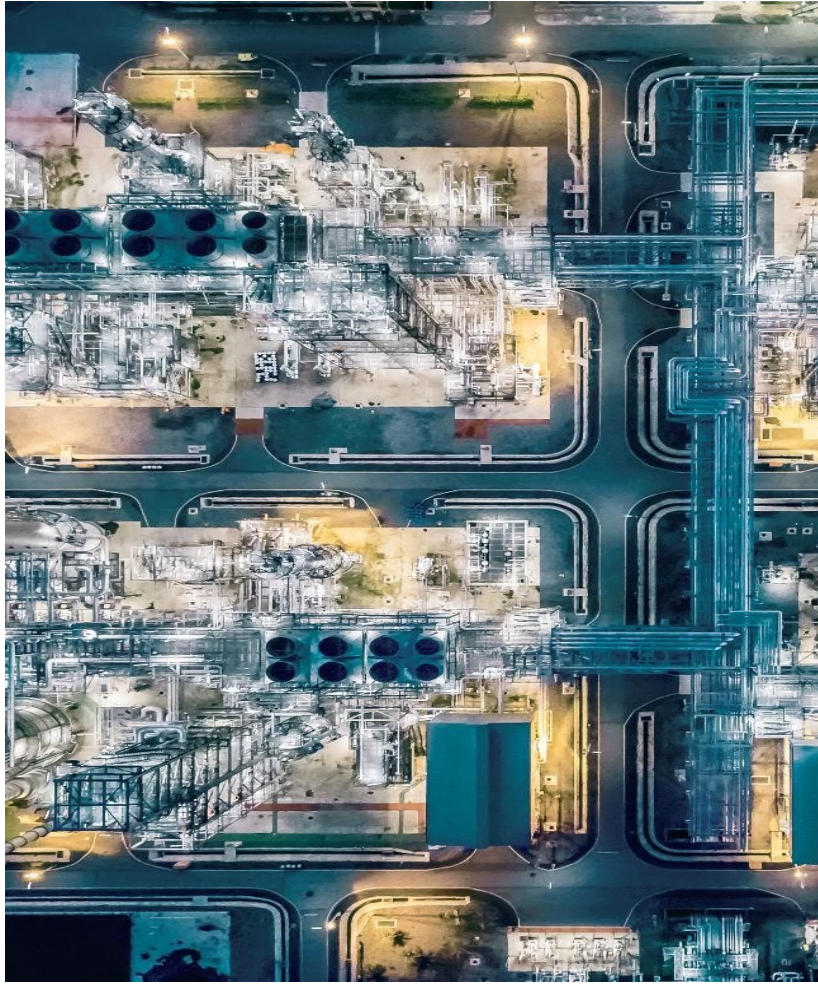
We are seeing both the likelihood and impact of cyber attacks increasing and cyber security good practices falling by the wayside as organisations become more technology dependent than ever. We are also beginning to see the nature of the threat changing, as attackers exploit uncertainty, unprecedented situations, and rapid IT and organisational change.

Organisations should take three key actions to mitigate these emerging risks:

Secure their newly implemented remote working practices **1**

Ensure the continuity of critical security functions **2**

Counter opportunistic threats that may be looking to take advantage of the situation **3**



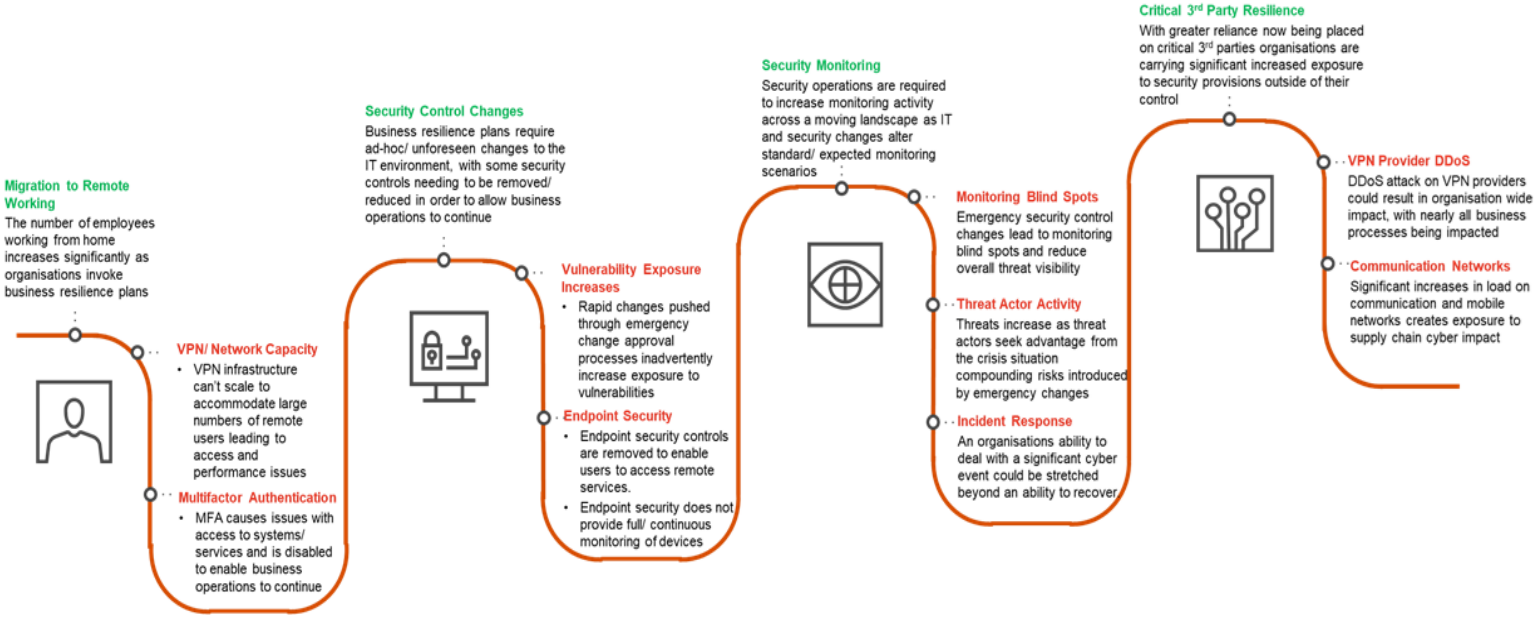
Early challenges as organisations migrate to a remote working environment

We see three key emerging cyber security risks as a result of COVID-19:

A shift to remote working and prioritising business operations has brought some immediate cyber challenges info focus

Disruption to the workforce and suppliers will increase vulnerability to old risks

Going forward this will change organisations' cyber security risk landscape



As organisations are shifting their workforce to remote working, the potential impact on their IT Infrastructure requirements and the attack surface

We see three key emerging cyber security **risks** as a result of COVID-19:	Indicative repercussions of the new remote working environment:	Organisations should take three key **actions** to mitigate these emerging risks:
A shift to remote working and prioritising business operations brings immediate risks	• Hasty deployment of new tools downgrading security controls. • Existing security controls may not be effective in a remote environment. • Employees may introduce free and unsanctioned tools in an effort to become efficient.	**Secure their newly implemented remote working practices**
Disruption to the workforce and suppliers is increasing vulnerability to old risks	• Regular security procedures may be neglected, i.e. Patching. • Security alerts may remain uninvestigated. • Detection may be degraded as Managed Service Providers may be unavailable.	**Ensure the continuity of critical security functions**
Going forward this will change organisations' cyber security risk landscape	• Upon returning to normal business, technology deployed to remote workforce may no longer adhere to security standards. • As remote working becomes the new norm, organisations are likely to shift more applications to the cloud.	**Counter opportunistic threats that may be looking to take advantage of the situation**

Mitigating emerging Cyber Risks

Secure their newly implemented remote working practices — 1

- Monitor for Shadow IT
- Secure Remote Access
- Implement Multi Factor Authentication
- Review On-premise Security Controls
- Enhance Security Monitoring
- Adapt Cyber Response

Ensure the continuity of critical security functions — 2

- Assess Critical Security Services
- Enhance Endpoint Security
- Implement Critical Security Control Change Freezes
- Review Privileged Access Management
- Review Security Architecture
- Monitor Asset Movement

Counter opportunistic threats that may be looking to take advantage of the situation — 3

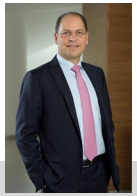
- Enhance Threat Intelligence
- Issue User Communications
- Monitor Insider Threat
- Monitor Phishing Activity
- Run Vulnerability 'Find & Fix'
- Implement 'Quick Win' Controls

Useful Tips for Remote Working Security

- Ensure your personal workstation/laptop/mobile are up to date with the **latest security patches** (and Operating System if possible) and the **local firewall** is enabled.
- Use corporate **VPN without split-tunneling**. (Restrict HTTP/S, DNS and SMTP access to the internet)
- **Enhance Monitoring capabilities**.
- Enforce **strong password** policy and implement **Multi-Factor Authentication** on all systems and applications where possible.
- Review your **business continuity** and **disaster recovery** plan and procedures
- **Educate your staff** in cyber security practices (e.g. how to handle phishing emails).

Let’s talk

For a deeper discussion on how the emerging Cyber risks might affect your business, please contact:



Philippos Soseilos
Partner
Advisory, Business Consulting
philippos.soseilos@pwc.com

Tassos Procopiou
Partner
Advisory, Business Consulting
tassos.procopiou@pwc.com

Minos Georgakis
Director
Advisory, Business Consulting
minos.georgakis@pwc.com