Impacts of COVID-19 on cyber security:

Managing a remote working environment.





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 cvber 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

Ensure the continuity of critical security functions

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

situation



March 2020

PwC

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

Migration to Remote Working

The number of employees working from home increases significantly as organisations invoke business resilience plans



 MFA causes issues with access to systems/ services and is disabled to enable business operations to continue

Security Control Changes

Business resilience plans require ad-hoc/ unforeseen changes to the IT environment, with some security controls needing to be removed/ reduced in order to allow business operations to continue

Vulnerability Exposure Increases

 Rapid changes pushed through emergency change approval processes inadvertently increase exposure to vulnerabilities

Endpoint Security

- Endpoint security controls are removed to enable users to access remote services.
- Endpoint security does not provide full/ continuous monitoring of devices

Security Monitoring

Security operations are required to increase monitoring activity across a moving landscape as IT and security changes alter standard/ expected monitoring scenarios

Monitoring Blind Spots

Emergency security control changes lead to monitoring blind spots and reduce overall threat visibility

· · Threat Actor Activity

Threats increase as threat actors seek advantage from the crisis situation compounding risks introduced by emergency changes

·· Incident Response

An organisations ability to deal with a significant cyber event could be stretched beyond an ability to recover

Critical 3rd Party Resilience

With greater reliance now being placed on critical 3rd parties organisations are carrying significant increased exposure to security provisions outside of their control :



processes being impacted Communication Networks

Significant increases in load on communication and mobile networks creates exposure to supply chain cyber impact

March 2020

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:

A shift to remote working and prioritising business operations brings immediate risks

Disruption to the workforce and suppliers is increasing vulnerability to old risks

Going forward this will change organisations' cyber security risk landscape Indicative repercussions of the new remote working environment:

- 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.
- 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.
- Upon returning to normal business, technology deployed to remote workforce may no longer adhere to security standards.

 A second of the control of the
- As remote working becomes the new norm, organisations are likely to shift more applications to the cloud.

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

Secure their newly implemented remote working practices

Ensure the continuity of critical security functions

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

March 2020

Mitigating emerging Cyber Risks











































March 2020

PWC

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:



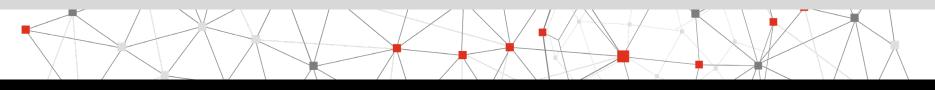
Philippos Soseilos Partner Advisory, Business Consulting philippos.soseilos@pwc.com



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



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





© 2020 PricewaterhouseCoopers Ltd. All rights reserved. PwC refers to the Cyprus member firm and may sometimes refer to the PwC network.

Each member firm is a separate legal entity.

Please see www.pwc.com/structure for further details.