Impacts of COVID-19 on cyber security: Focus on securing remote working

PwC Cyber Security

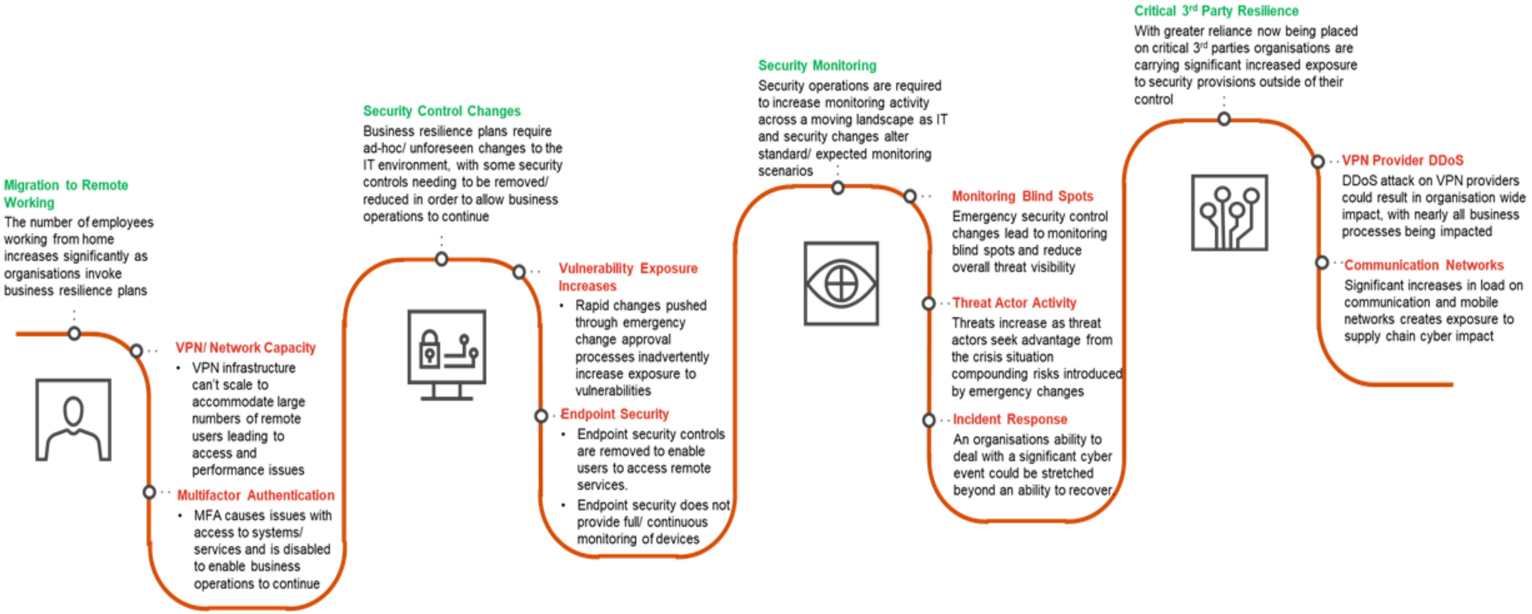
Early challenges - areas that clients have flagged as immediate difficulties

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

Going forward this will change organisations' cyber security risk landscape

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



Migration to Remote Working

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

VPN/ Network Capacity

- VPN infrastructure can't scale to accommodate large numbers of remote users leading to access and performance issues

Multifactor Authentication

- 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

VPN Provider DDoS

DDoS attack on VPN providers could result in organisation wide impact, with nearly all business processes being impacted

Communication Networks

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

Securing newly implemented remote working practices

1 Focus Area	Monitor for Shadow IT	Secure Remote Access	Implement Multi Factor Authentication	Review On-premise Security Controls	Enhance Security Monitoring	Adapt Cyber Response
2 Tactical Remediation	Expand endpoint and network monitoring to identify new devices	Expand VPN capacity (existing capability/ augmented via supplier)	Track / record MFA exceptions	Tighten data security access & related controls	Increase security monitoring capabilities (compensating control)	Ensure third-party incident response capabilities are on standby
	Monitor spend thresholds and expenses for authorisations of services	Monitor remote access systems & Active Directory for anomalous logins	Reconfigure gateways to enable MFA into on premise systems	Review critical security controls/ processes to determine gaps	Move SOC to a high risk footing & implement 24x7 / shift rotation	Focus threat intelligence to identify COVID-19 specific threats (e.g. phishing)
	Reassess web proxy filtering and consider implementing CASB	Extend/ implement DDOS mitigation	Switch to cloud applications with native 2FA (where possible)	Establish minimum security operating requirements to maintain consistency	Augment with third party suppliers to manage load on internal staff	Update processes to reflect contingency and alternative working practices
3 Strategic Remediation	Implement/ expand CASB to enable holistic shadow IT monitoring	Move away from VPNs completely (e.g., Google's BeyondCorp model)	Migrate to a zero trust based model	Implement a dynamic/ adaptive security control model	Define people/ process/ technology for SOC surge capacity	Expand cross industry support to increase market resilience
	Automate workflow approval to monitor for all IT related services		Implement passwordless authentication		Implement SOAR to decrease reliance on scaling staff	

Ensure the continuity of critical security functions

1 **Focus Area**	**Assess Critical Security Services**	**Enhance Endpoint Security**	**Implement Critical Security Control Change Freezes**	**Review Privileged Access Management**	**Review Security Architecture**	**Monitor Asset Movement**
2 **Tactical Remediation**	Assess the impact of recent changes on critical security services Repurpose IT staff to supplement critical security process Identify business impacts of re-prioritised critical security services	Confirm patching processes are operating for remote connected devices Implement out of band patching for endpoints & critical systems (inc. VPNs) Check BYOD device configurations (e.g. dual homing, AV etc)	Assess impact on key security operations (e.g. vuln. mgmt./ patching) Implement restrictions on security control changes	Review backup plans for single points of failure (people/ process/ tech) Review provisions for enabling remote PAM activity	Map 'as is' security architecture to identify operational gaps Document compensating controls where standard sec. arch. is circumvented Determine quick to deploy cloud security tools as potential interim controls	Track IT assets as they migrate to off-premise locations (physical / logical) Implement asset monitoring for business critical systems & data Restrict access to large repositories of sensitive data
3 **Strategic Remediation**	Map critical security services to critical business process Implement dynamic security control mapping to enable real time visibility	Migrate workforce to remote working to enable greater flexibility in crisis		Look at PAM cloud based solutions to provide backup for onsite PAM controls	Push cloud adoption to increase native cloud security capabilities Align security architecture to critical business processes	Leverage augmented reality to increase speed/ ease of asset review Use RFID/ location aware tracking to automate asset monitoring

Counter opportunistic threats looking to take advantage of the situation

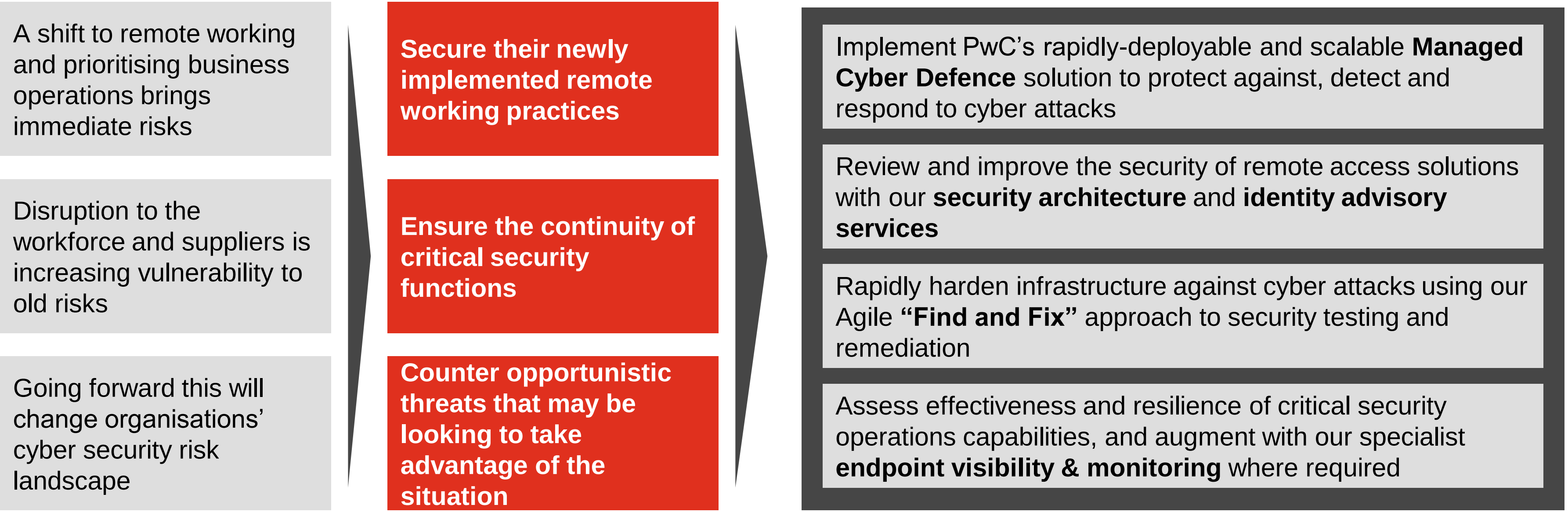
1 Focus Area	Enhance Threat Intelligence	Issue User Communications	Insider Threat Monitoring	Monitor Phishing Activity	Run Vulnerability ‘Find & Fix’	Implement ‘Quick Win’ Controls
2 Tactical Remediation	Extend TI monitoring to cover COVID-19 related threat actor activity	Issue communications related to likely threats (e.g. COVID-19 Phishing)	Implement insider threat monitoring plans during staff notice periods	Integrate TI data relating to phishing campaigns with monitoring controls	Rapid assessment to identify potential vulnerabilities	Extend anti-virus agents to include anti-malware scan interfaces
	Link potential TI activity to critical business function (e.g. cash collection)	Remind users of key security policies (end user guidance, data security)	Secure key data assets, critical system access from potential malicious users	Expand email filtering and blocking	Conduct red team exercise on ‘as is’ security control environment	Restrict the type of executables that end users can run
	Share threat intelligence within industry community groups		Implement targeted DLP policies to expand data exfiltration monitoring			
3 Strategic Remediation	Enhance threat intelligence signals & leverage supplier ecosystem	Look at multiple communication channels to engage end users	Implement user behaviour & heuristics monitoring	Automate & integrate TI phishing data with monitor & prevent controls	Implement a rolling vulnerability find and fix programme	Implement location aware controls change dynamically by scenario
				Use targeting training to focus groups of users on specific phishing risks	Expand use of automated security scanning within SecDevOps practices	

Our services that can immediately help organisations

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

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

PwC has four key **services** which can immediately help organisations:



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

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

Implement PwC's rapidly-deployable and scalable **Managed Cyber Defence** solution to protect against, detect and respond to cyber attacks

Review and improve the security of remote access solutions with our **security architecture** and **identity advisory services**

Rapidly harden infrastructure against cyber attacks using our Agile **"Find and Fix"** approach to security testing and remediation

Assess effectiveness and resilience of critical security operations capabilities, and augment with our specialist **endpoint visibility & monitoring** where required

Strategic response to COVID-19

The COVID-19 outbreak has been declared a pandemic by the World Health Organization, causing huge impact on people’s lives, families and communities.

Businesses face significant challenges and disruption. The ability to navigate through crises and unforeseen events is an essential aspect of operational resilience; particularly through a public health crisis.

To ensure continuing business operations through uncertain times, businesses need to build and rehearse a holistic capability to respond to cyber attacks, increased demand for remote working, and increasingly complex governance.

Culture & awareness

End user behaviour and culture awareness during a time of heightened cyber risk

Governance

Operating an effective level of governance in an uncertain environment to maintain an appropriate security posture

Data security

Protecting sensitive information whilst implementing and operating different working practices

Capacity management

Managing increased demand on the critical security services needed to enable remote working and secure data access

Detective/protective controls

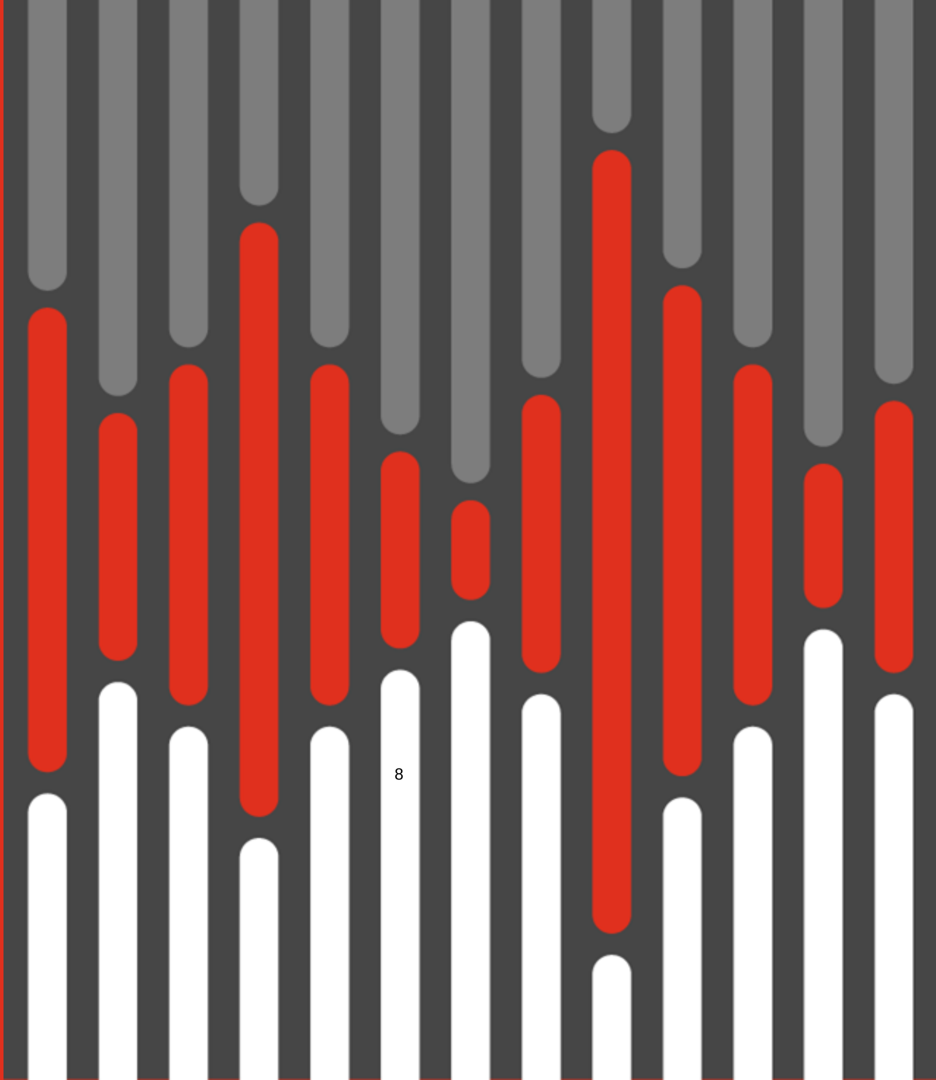
Maintaining effective monitoring, detection and protection controls during non-standard business operation

Incident management & business continuity

Continuing to operate incident management, crisis response and business continuity capabilities during a period of increased organisational stress

11 March 2020

Forward looking - what types of fundamental changes might we expect to see after this initial crisis period is over



Future....

Expansion of Ecosystem Business Models

Ecosystem business models that encompass a network of third parties are able to adapt and change to rapidly evolving risks more effectively than traditional supplier-customer models. Digital transformation has predominantly focused on business to consumer change, but greater benefits could be realised by extending the definition of digital transformation.

Accelerated Adoption of Cloud

Whilst most organisations have adopted Cloud for a variety functions, applications and services there is likely going to be a broader reassessment of how Cloud can help to alleviate some of the recent challenges related to remote working, running business critical operations and enabling access to key business systems.

Redefined Meaning of a Resilient Business

Disaster recovery and business continuity planning have for many years had some degree of focus on pandemic scenario planning, but as this is the first time that we have lived through such a widespread event there will doubtless be a need to revisit plans, apply lessons learnt and consider what makes a business resilient.

Augmented Reality/ Virtual Operations Functions

The use of new technology could change the way businesses and users interact with each other by extending location agnostic services and capabilities and by maximising virtual experiences. Such technology is already being adopted to address health and safety challenges in dangerous environments, but with the roll out of 5G there will be potential for much wider adoption and application.

Cross Business Industry Resilience

The definition of business and industry boundaries seems less applicable during periods of large scale crisis. Assessing how businesses work together during these periods could influence the way in which cross business and industry resilience is addressed in the future.