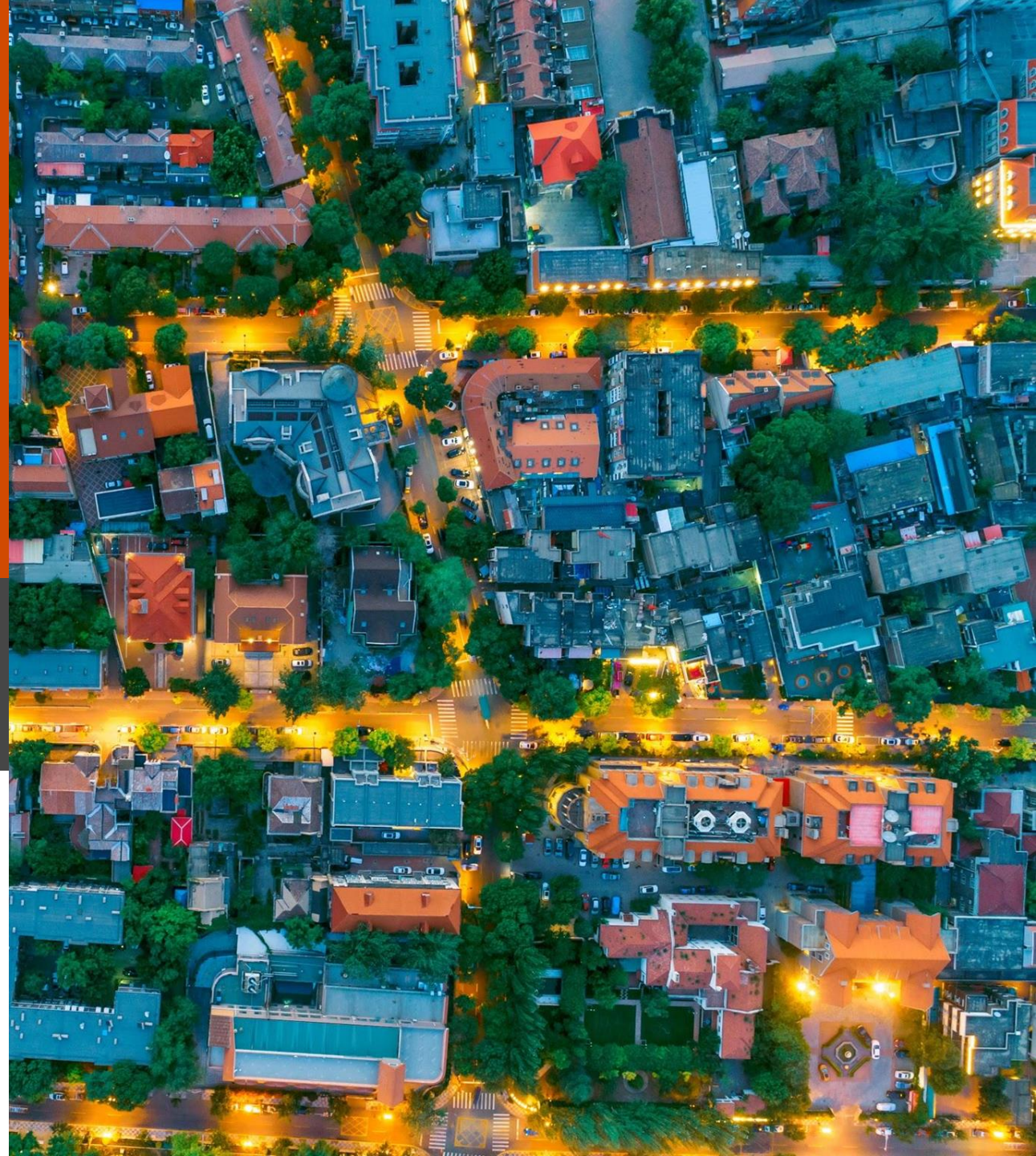
Cyber resilience in time of Covid-19 crisis

Understanding and managing the potential cyber security impacts of the COVID-19 outbreak

pwc



Responding to COVID-19: Cyber Security

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

Responding to COVID-19: Knowing when to act

Government's phased response plan - COVID-19

Containment

Detect early cases, follow up close contacts, and prevent the disease taking hold in this country for as long as is reasonably possible.

Delay

Slow the spread in this country, if it does take hold, lowering the peak impact and manage it particularly in the vulnerable population.

Research

Better understand the virus and the actions that will lessen its effect on the South African population; innovate responses including diagnostics, drugs and vaccines; use the evidence to inform the development of the most effective models of care.

Mitigate

Provide the best care possible for people who become ill, support hospitals to maintain essential services and ensure ongoing support for people ill in the community to minimise the overall impact of the disease on society, public services and on the economy.

Prepare

Mobilise your response

Organisations should enact cyber crisis management and business resilience plans as the organisation moves from standard business operations to a higher state of cyber readiness in the midst of a disruptive event. During this period, there will be a need to dynamically assess cyber risks as they evolve.

Respond

Dynamically respond to new developments

Organisations will be operating in a volatile environment, with crisis management and business continuity plans being invoked. In context of a heightened level of business risks, organisations should increasingly prioritise moving towards an agile operating model and may potentially require rapid deployment of new technology and engage third party specialist support. In particular, organisations may need to ensure that their current infrastructure is scalable on-demand to meet increasingly widespread to meet non-standard working practices, e.g. remote working, in order to sustain business operations for an indefinite period.

Recover

Transition to business as usual and review lessons learned

Businesses should phase out of crisis operation procedures and revert to business as usual operations. They may collate lessons learned to identify areas for improvement and update plans accordingly (e.g. identify deficiencies and review options to increasingly automate security operations).

Responding to COVID-19: Prepare Phase

COVID-19 response strategy

People

Ensuring that your people are ready for a shift towards alternative working practices

- ❑ Are all end users aware of technology and processes available to them for remote working?
- ❑ Has the organisation undertaken cyber risk assessments to understand how cyber risks will change when different working practices are introduced (e.g. securing data when working remotely)?
- ❑ Does the organisation have sufficient security expertise (internal and third party) to support the business as it moves to alternative working practices?
- ❑ Are there policies and processes in place to govern secure remote working and best practices for secure data handling, and have these been communicated to the wider business?
- ❑ Is the Security Operations Centre (SOC) ready to adapt to a higher level of cyber security resilience, for example by moving to 24x7 operations and changing to shift patterns?
- ❑ Are senior executives aware of security communication protocols in the event there is a cyber incident (e.g. managing PR, crisis team response)

Process

Working within your organisation to preserve data security and increase cyber readiness

- ❑ Are there established and understood processes for the secure handling of sensitive data when working remotely?
- ❑ Has guidance for remote working been established and communicated to the wider organisation?
- ❑ Is the guidance stored in an easily accessible central repository?
- ❑ Have knowledge transfer mechanisms been established to familiarise temporary/ emergency staff with the organisation's security procedures?
- ❑ Are there processes in place for dynamically updating security training and awareness materials in accordance with new developments?
- ❑ Does the SOC have formalised and documented escalation processes for responding to heightened alerts when operating under different circumstances (e.g. 24x7)?
- ❑ Will standard security processes continue to operate with staff working remotely (e.g. virus and patch updates)
- ❑ How will standard security functions continue to operate and serve the business (e.g. vulnerability assessments)?

Technology

Reviewing and upgrading existing technology to ensure sufficient capacity

- ❑ Do you have remote access and VPN applications in place for all endpoint devices?
- ❑ Are your remote access and VPN applications scalable on demand?
- ❑ Do your VPN applications have multi-factor authentication in place?
- ❑ How do you manage user identity when they access systems remotely?
- ❑ How do you provision user access when users access systems remotely?
- ❑ Can you implement additional security controls to provide enhanced control on the network (e.g. virtual network zoning, endpoint device compliance checking etc)
- ❑ Does your security monitoring capability alert you on suspicious / unusual VPN activity?
- ❑ Will network bandwidth support significant increased use of remote access services or is there heightened potential for loss of service (inadvertent DoS)?

Responding to COVID-19: Respond Phase

COVID-19 response strategy

People

Ensuring that staff remain supported in a non-standard working environment

- ❑ Has the current operating model been evaluated to identify key dependencies and single points of failure?
- ❑ Are training / guidance materials readily available to staff to ensure that they are kept up to date with best practices in relation to remote working and secure data handling?
- ❑ Have staff been briefed on security guidance for using their personal devices to access corporate applications?
- ❑ Is there an established key point of contact for security queries throughout the period of remote working?
- ❑ Are staff familiar with escalation procedures for reporting security incidents?
- ❑ Is information / guidance on escalation procedures readily available to staff on a central intranet location?
- ❑ Are secure communication channels known to users and are they familiar with how to use them?
- ❑ How is the security team organising itself to maintain services in the event team members become unwell (e.g. splitting into teams, limiting office visits etc)

Process

Adapting existing processes to align with new working practices

- ❑ Have escalation procedures been reviewed and updated to support remote working practices?
- ❑ How will remote working processes and practices be assessed to monitor effectiveness during the crisis period?
- ❑ Is there a formal process in place to continually update and disseminate training / guidance materials in response to new developments?
- ❑ Are there readily available process flow documents available to support teams to assist them with dealing with cyber incidents?
- ❑ How are critical security processes being adapted to accommodate different working practices?
- ❑ Can critical security processes (e.g. access certification, sensitive data quarantine etc) still function as required?
- ❑ Is there a clear and up to date communications plan in places with key third parties, in particular those who operate critical business services or locations (e.g. data centres)
- ❑ How are regular security services (e.g. vulnerability management) continuing during the crisis period?
- ❑ If critical vulnerabilities are discovered how will these be remediated or mitigated if the business implements a change freeze?

Technology

Scaling up technological capabilities to meet changing demand

- ❑ Can the security infrastructure scale up within a short time frame to meet rapidly evolving requirements?
- ❑ If additional security services are required how are they being integrated to avoid diluting existing security posture?
- ❑ Are there any access restrictions (physical or logical) in place that might prevent users from accessing key systems whilst remote (e.g. location based authentication/ access restrictions)?
- ❑ Are the data centres equipped for live/ hot network failover to accommodate business continuity?
- ❑ Are solutions in place to alert, investigate and respond to abnormal user behaviour on the organisations network given the change to standard user working patterns?
- ❑ Are technologies in place to review, update and renew user credentials within a short timescale (e.g. emergency access re-certification)?
- ❑ If AI/ automated detection systems have been implemented how are these been re-tuned to take into account changes to standard working practices?
- ❑ Have current security services been evaluated and prioritised, including considering temporarily discontinuing low-priority services in favour of retaining critical functions?

Responding to COVID-19: Recover Phase

COVID-19 response strategy

People

Transition staff back towards business as usual operations

- ❑ Have remote working activities been continuously monitored and where inappropriate end user behaviour has been identified have HR been engaged to assist?
- ❑ Are there any changes to standard operating procedure that need to be implemented in order to return to standard working practices?
- ❑ Are formal communications in place to assist with transitioning back towards business as usual whilst maintaining good security practices (e.g. secure data archive)?
- ❑ How are lessons learnt going to be captured and implemented?
- ❑ What security culture did you observe during the crisis event and how might this inform how you change security culture awareness in the future?
- ❑ Did your organisations security culture persist during this incident or did users revert to work arounds when facing pressured situations?

Process

Review lessons learned and update plans accordingly

- ❑ Have contingency plans been developed to address residual deficiencies in the operating model (e.g. key dependencies, single points of failure)?
- ❑ How is the process for capturing security lessons learnt going to be captured as updates to broader business continuity plans, specifically where security aided or impacted business operations?
- ❑ Have resource-intensive security processes been re-evaluated to identify areas of the process that can be automated?
- ❑ Has post-incident security testing been carried out based on vulnerabilities that have been identified throughout the period of working in a non-standard environment?
- ❑ Have new processes been drawn up in response to new scenario impacts to minimise future business disruption?
- ❑ Have security risk transfer mechanisms been assessed to determine how they might support business recovery (e.g. cyber insurance)?

Technology

Consider technological options for increasing operational agility

- ❑ Have options for automated security management (e.g. managed detection and response capabilities) been reviewed to sustain business operations through periods of staff shortage?
- ❑ Have cloud-based solutions been considered to improve on-demand scalability of services over the longer term?
- ❑ Have third party service line agreements been re-evaluated to include or amend existing contingencies?
- ❑ Have mobile device management solutions been considered to expand functionality on personal devices while keeping company data secure?
- ❑ How does your security architecture need to change to become more resilient or agile in the future (e.g. moving to zero based trust, re-design of location aware identity etc)?
- ❑ How can emerging technology further enhance the businesses ability to manage resilience and what are the security implications (e.g. augmented reality, drones)?

Contact us

Busisiwe Mathe
Partner
T: +27 (11) 797 4875
M: +27 (82) 210 3121
E: busisiwe.mathe@pwc.com

Hamil Bhoora
Partner
T: +27 (11) 797 4102
M: +27 (72) 388 4444
E: hamil.bhoora@pwc.com

Duane Carstens
Associate Director
T: +27 (11) 797 5389
M: +27 (72) 436 6252
E: duane.carstens@pwc.com

Chris Knox
Associate Director
T: +27 (11) 287 0586
M: +27 (72) 410 1980
E: chris.knox@pwc.com

Yvette du Toit
Associate Director
T: +27 (11) 797 4390
M: +27 (79) 509 8913
E: Yvette.du.toit@pwc.com

pwc.com/cyber