Prioritising cyber capabilities and managing cyber risk while enabling acceleration as we emerge from the business impacts of COVID-19

The coronavirus (COVID-19) continues to have a significant impact on individuals, communities and businesses globally. It is important that cyber professionals understand how they can be part of the solution to the business challenges that are presented by COVID-19.

Responding to COVID-19 brought about significant organisational change and new ways of working at scale. Most organisations have experienced, or are in the midst of the following three stages:

- **Mobilise:** Reacting to the need for change, often needing to relax security controls to allow for rapid change to take place.
- **Stabilise:** Adapting to the new changes, re-assessing risk and re-establishing processes and supporting technologies which enable new ways of working, while managing risk appropriately.
- **Strategise:** Commencing recovery and identifying opportunities for improving capabilities to support growth.

For organisations in the Stabilise stage, how can cyber risks be understood and assessed when there may still be constant change occuring? For organisations emerging out of the Stabilise stage and into the Strategise stage, what cyber capabilities are now needed to best support the organisation? What is a systematic approach to determining how to invest and prioritise on cyber control capabilities? Most importantly, how can the organisation's cyber risk capability be adapted to keep pace and enable further digitisation and rapid change of business processes?

Key Cyber Capability and Cyber Risk Considerations

Risk Management and Governance

The ability to (re)assess cyber risks rapidly and prioritise cost effective remediation

Authorised Access Management

Getting the right users access to the right systems whether working on-site or remotely

User Awareness and Training

Making the workforce aware and resilient to emerging cyber threats

Incident Detection & Response

Enhancing the ability to detect and manage cyber incidents and coordinating appropriate response

Third Parties (Including Cloud Services)

Understanding data flows and associated risks with third parties (including cloud services)

System and Data Protection

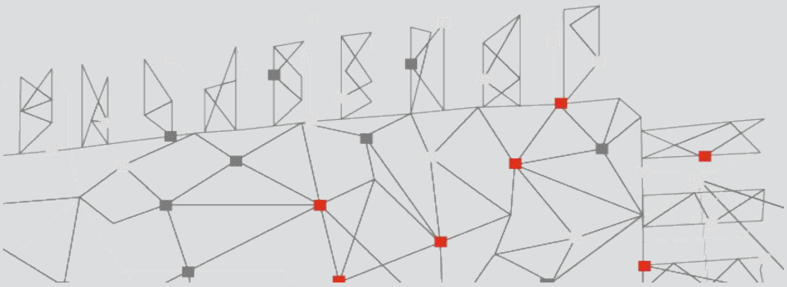
Protecting sensitive information while managing and implementing security controls to current and new systems

Have the Mobilise and Stabilise stages of COVID-19 altered how your cyber controls are operating?

Risk Management

- **Risk Assessment:** "Connectivity first" was the focus for many organisations during the early weeks of the crisis as businesses drastically increased their remote working capabilities and infrastructure to support their workforce needs.

  In the rush to maintain operations, organisations may have compressed or exempted their risk and change management processes. With the significant change in the organisational operating environment, prioritising a re-assessment of risk that reviews access and new threats facing remote workers is critical.
- **Third Party Risk**: Companies that place reliance on third parties such as Managed Service Providers (MSPs) for day-to-day IT and security operation activities are facing new risks and challenges, particularly if these operations are provided from offshore service delivery centres. How your third-parties are operating and how their own control environment may have changed needs to be critically reviewed.



Remote work capabilities

- **Data Exfiltration:** The mass deployment of remote-working capabilities has introduced the risk of data breaches as sensitive data may be accessed, processed or stored within employees' personnel environments that lack enterprise security controls. Being able to monitor and manage this data is key to minimise the potential of unauthorised/accidental data loss.
- **Device Management**: For organisations, the rapid deployment of devices for remote working or virtual desktop environments has left little time for security considerations. The same endpoint controls that exist for desktop environments need to be extended to mobile devices, including managing the use of personal devices for work activities (BYOD).
- **Training and Awareness**: Common sense may not be common practice, especially for members of the workforce who are not used to working remotely. Ongoing training and awareness is important to ensure that personnel are working securely and can stay vigilant as they face new and emerging threats.

Information Security capabilities

- **Shadow IT:** In the rush to preserve productivity, employees have resorted to the use of unapproved file sharing and applications ("shadow IT"). Visibility of which services have been activated and accessed is critical for assessing risk.
- **Security Monitoring and Detection**: At this time, an organisation's threat landscape is rapidly and constantly changing. Updating existing and introducing new use cases may be required to detect and minimise the impact of potential compromises.

Key COVID-19 related cyber security threats seen so far

Phishing campaigns & brand spoofing

Threat actors have been leveraging genuine concerns over COVID-19 to phish end users through emails impersonating the World Health Organisation (WHO), employers, health, financial, logistic, government and non-for-profit organisations. Fake email domains are also being used to steal legitimate credentials to gain a foothold in organisations and deliver malware.

Fake COVID-19 Websites

Researchers have noted that threat actors are using fake websites offering COVID-19 themed maps and free COVID-19 vaccine kits claiming to be manufactured by the World Health Organisation to lure users to download malicious files that infect the endpoint and exfiltrate credentials.

Ransomware, Keyloggers, RATs, and Banking Trojans

Increased activity of multiple cyber crime and nation state threat actors has been observed as they capitalise on the COVID-19 situation. Spreading the Emotet and Trickbot banking trojans, Netwalker ransomware (targeting healthcare industries) and Remote Administration Tool, CrimsonRAT are notable large scale campaigns that are being used for fraud and to gain unauthorised access to organisations to steal sensitive information or release ransomware.

Exploitation Of Router's DNS Settings

Researchers have noted that threat actors are hijacking router DNS settings, resulting in web browsers displaying alerts for a fake COVID-19 information app from the World Health Organisation that actually contains malware designed to steal information.

Spam and Disinformation on Social Media Platforms

Multiple ongoing spam campaigns have been observed as threat actors leverage hijacked Twitter accounts to advertise websites claiming to sell facemasks, for example. In addition, disinformation campaigns are increasing, spreading false information related to COVID-19 and the various responses by governments.

Vishing and Smishing: Voice and Text Message-based Scams

Threat actors continue to leverage phone calls to trick people into reserving a non-existent COVID-19 vaccine over the phone. In addition, multiple false text messages have been identified spreading malicious links and disinformation related to COVID-19.

Attacks on Mobile/Remote Working Infrastructure

Employees are exposing company devices to greater risk as they leave the safety and security of the workplace. This is particularly the case if these devices are not adequately protected with encryption, VPN, enterprise-grade endpoint AV solutions and strong password policies.

Capability considerations in the Stabilise and Strategise stages

A risk-centric approach is crucial to determining whether and how cyber capabilities need to be adjusted and/or uplifted. While the below sections provide a view of potential considerations, your organisation should take into consideration the overarching strategic shift and appetite of risk when evaluating your cyber capability roadmap. Where investment challenges arise, there are approaches that can be undertaken to critically re-assess your risk position, determine the effectiveness of current capabilities and provide more clarity as to how best to use your investment.

	Medium term (2 - 6 months) Stabilise	Longer term (6+ months) Strategise
Risk Management and Governance The ability to (re)assess cyber risks rapidly and prioritise cost effective remediation **Impact to risk management:** The immediate effect of COVID-19 has changed the way we work and has created challenges that require quick risk management responses from organisations. In this new environment, the likelihood of losses due to cyber security attacks is increasing, while the budget for managing this risk is expected to receive more scrutiny than ever before. The cost effective management of cyber risk becomes a crucial objective for every organisation. **Critical role of governance:** Operating an effective level of governance in an uncertain environment is essential to maintain an appropriate security posture to ensure the resilience of an organisation's most valuable or operationally vital systems or information against cyber threats.	● Adapt governance and risk management plans. ● Determine cost effective risk treatment options to manage cyber risk within appetite with limited budget and staff. ● Evaluate COVID-19 specific scenarios for your organisation. Identify potential risks and assess impacts. ● Re-assess risk with the lens of COVID-19 related threats (such as the increase in targeted spear phishing). ● Develop **likely and reasonable worst case scenarios** and their potential impact to support crisis and response planning.	● Enhance risk management process through automation (tooling and processes). ● Consider whether investment is allocated to the most effective controls or whether budgets could be used more effectively using data-driven risk analysis techniques. ● Streamline risk capabilities to support a potentially newer and more agile "digital focused" organisation so cyber risk management becomes a key enabler to the organisation's recovery and growth.
Authorised Access Management Getting the right users access to the right systems whether working on-site or remotely **Remote working considerations and gaining access to relevant systems:** There have been rapid transitions to remote working and often an urgent need to implement the tooling required to ensure that users are being productive while working from home. This has placed a heavy reliance on remote access systems and may leave organisations more vulnerable to cyber attacks. Additionally, employees may be required to work with technologies that they are not familiar with, potentially resulting in new security risks being introduced. A range of risk based considerations surrounding remote working conditions should be made. **Managing and monitoring user activity:** Organisations should consider defining guidelines on how privileged user access will be provisioned and monitored while operating remotely. This should include how privileged activities are monitored to ensure that they are appropriate and accountable, to prevent further threat actions.	● Confirm that technology infrastructure can support remote operations. ● Assess if web browsing is secured by web filtering when working remotely. ● Apply secure configurations should to email, identity management (e.g. Active Directory) and conferencing systems used by remote workers. ● Monitor the availability and functioning of remote systems and networks. ● Ensure that there is enough capacity to access the systems that users may require. ● Provide oversight on how user accounts are being provisioned, including mechanisms for the monitoring of user activities.	● Review processes surrounding system connectivity adaptation of remote access technologies. ● Adapt Privileged Access Management and ensure it offers a secure, remote access, work from home solution. ● Work to integrate rapid and Agile security testing into the deployment of new remote access systems. ● Review the effectiveness of privilege identity management solutions adopted for remote administrative access.
User Training and Awareness Making the workforce aware and resilient to emerging cyber threats **Channels and opportunities for cyber attacks are emerging as an increased number of threats are faced in the COVID-19 environment:** With staff working from home there has been a significant increase in the number of cyber threats and risks they face, particularly as threat actors seek to take advantage of potentially reduced control environment. A large increase has been observed in targeted phishing scams, fake websites and mobile applications as threat actors seek to leverage genuine concerns over COVID-19 to steal credentials and spread malware. **Encouraging workforce awareness and resilience to new cyber threats:** It is critical that organisations focus on maintaining the awareness of their staff to new processes, changes and the increased threat landscape. Enhanced user awareness and training is a priority for managing their response to such changes.	● Develop a clear communications strategy to ensure that employees are kept abreast of rapid changes and any new tools within their working environment. ● Conduct organisation wide awareness strategies and guidance materials to help employees understand and are conscious of different threats in a remote working environment (such as Phishing, SMS or other related scams) ● Conduct phishing exercises to identify weak points and help to remind employees of the increased cyber risks that may become more prevalent during the COVID-19 crisis.	● Review staff awareness of external threats and update guidance materials for staff in relation to the best practices for remote working, secure data handling and use of personal devices including the reiteration of cyber safety awareness. ● Establish processes for dynamically updating security training and awareness materials in accordance with new developments of the COVID-19 threat environment.

	Medium term (2 - 6 months) Stabilise	Longer term (6+ months) Strategise
Incident Detection & Response Enhancing the ability to detect and manage cyber incidents and coordinating appropriate response **Maintaining effective monitoring and detection controls during non-standard business operations:** Non standard business operations should encourage organisations to keep close surveillance on all digital infrastructure, client organisation's processes, and timely reports of all detected threats to ensure a greater level of safety and privacy. Monitoring and crisis response components should also consist of network/endpoint and mobile device security to ensure that all devices are properly connected and are behind the security network mandated by the organisation. **Managing crisis response during a period of increased organisational stress:** A cyber incident that occurs when an organisation is operating remotely will have a greater impact. Organisations should ensure they have a remote crisis management team with well-defined roles, responsibilities, accountabilities and the enabling technology to support the collaboration of the crisis team. It is important to manage such crises in the future through a remote task force and to ensure continuity of operations if the impact continues to spread over a longer period.	● Assessment of incident response plans and playbooks to ensure that they function with a workforce primarily working remotely. ● Deploy a rapid response process for identified cases and develop a personnel recovery plan. ● Adapt crisis response and business continuity planning. ● Utilise specific threat intelligence to detect threat actors targeting COVID-19 and related themes. ● Enable response teams to securely access compromised devices for analysis and eradication.	● Update all incident response and business continuity plans with lessons learned from the crisis, including pandemic response plans. ● Conduct tabletop drills and testing of updated incident, business continuity and crisis management plans. ● Update underlying incident detection and response procedures, especially where there is a significant dependence on third party providers to ensure that processes are effective.
Third Parties (Including Cloud Services) Understanding data flows and associated risks with third parties (including cloud services) **The sudden shift to remotely operating critical IT services has increased the reliance on third parties and their continuity arrangements, both for service and hardware provisions.** This shift could create associated risks with third party entities (including cloud services) due to the housing and flow of operational/sensitive data. Due to the associated risks with third party arrangements, the housing of critical data in low-risk data centers should be prioritised and if not possible, decisions to redeploy to on-prem and other cloud service providers can be made to ensure that data flows and storage is safe. **Possibility of third party service providers inability to work remotely:** Consideration should be made whether there is a possibility that third parties could be disrupted by an inability to work remotely, in this case further contingency measures should be implemented, i.e. migrating operations to a less disrupted offshore site. During this period, there may be a decision to reduce reliance on third parties and in-source these processes, with a potential decision to digitise them. For critical processes that rely on an overseas third party, it may be worth re-assessing whether utilising a more local supplier may provide improved reliability and lower risk.	● Communicate with third party providers to assess impacts and potential service disruption, especially for managed services. ● Maintain effective and protected remote operations and oversight of third-party suppliers and providers will be key in order to running business as usual during this period. ● Understand what cloud services are being initiated and monitor user cloud service activities to ensure only the main corporate approved services are being used. Where there might be legitimate reasons for non corporate services, appropriate controls should be identified and applied.	● Conduct periodic testing and review of key cyber controls to ensure risks are being managed appropriately, including those managed by 3rd and 4th parties. ● Perform targeted awareness campaigns and best practice for suppliers. ● Update standard contractual cyber security requirements, having re-evaluated risks. ● Conduct more rigorous assessments and ongoing monitoring. ● Explore digitisation and automation opportunities to drive improved resiliency in critical processes reducing reliance on higher risk suppliers.
System and data protection Protecting sensitive information whilst managing and implementing security controls to current & new systems **Organisations should be increasingly conscious of how end point devices and organisational data should be protected :** Devices need to be protected against compromise with options such as: encryption solutions (device and network), VPN, enterprise-grade endpoint AV solutions and strong password policies. Organisations should also evaluate mobile device management (MDM) solutions and expand the functionality to personal devices to ensure enterprise data security and protection on personal devices. **To ensure the protection of critical data it is recommended that organisations identify which activities should be monitored that are crucial to management and follow a risk based approach for data protection:** This may include patching security vulnerabilities, security monitoring, identity management and backing up key systems. It is also critical to ensure that sufficient resources are identified (with levels of redundancy) to deliver these critical services and identify how leadership can monitor that these activities are taking place.	● Ensure security operations are able to perform monitoring activities of how users are accessing and moving data as part of working remotely. ● Ensure user endpoints have up to date virus protection (E.g. machines may have been rapidly deployed to users). ● Review data security policies to enable remote working (including primary and 3rd party providers). ● Ensure staff utilise only secure access mechanisms for remote access – SSL VPN, secure remote desktop protocol (RDP) gateway, thin client access, etc.	● Review and allocate investment to controls that are most effective in system and data protection and that provide greatest risk buy-down. ● Review the effectiveness of key security controls including full disk encryption, anti-malware protection, data loss prevention, automated backup solutions and endpoint detection and response tooling applied.on the laptops/servers deployed for remote use. ● Implement capabilities to identify and track access to data so better visibility can be provided over where data is and how it is being used.

We can work alongside you to tackle the challenges you face in managing COVID-19

Cyber Risk Management and Optimisation

We bring expertise that can enhance your cyber risk management capability, including the analysis and recommendation of how best to leverage your current/future investment to implement the most appropriate and effective cyber controls. Areas we can assist with include:

Cyber Risk Identification and Assessment

- The identification, assessment and expression of cyber risks at an operational level.
- Development of Key Performance, Key Risk and Key Control indicators to support improved visibility and management of risk.

Cyber Control Analytics

- Validation of the likelihood and impact of cyber risks using analysis techniques such as advanced threat modelling, engagement with the business to quantify business impact and validation of the appropriateness and effectiveness of controls.
- Assessment of current-state cyber controls using relevant frameworks (e.g. NIST, C2M2 etc).
- Detailed analysis of how current-state controls contribute to the management of cyber risk.

Cyber Investment Strategy Validation

- Detailed analysis of proposed cyber control uplifts/additions and measuring the return of investment compared to the potential reduction of risk.
- Providing recommendations based on modelling of different scenarios to achieve the optimal risk outcome with available investment.

Cyber Business Case

- Supporting the establishment of business cases to uplift cyber control capability in alignment with target risk levels.
- Using risk and control analytics approaches to assist with identifying the value of the control and the amount of risk reduction achievable through the business case.

Third Party Cyber Risk Management

- Establishment of a Third Party Risk Management framework, including the stratification of third parties into appropriate risk tiers.
- Establishing control requirements for third parties based on risk tiers and conducting independent reviews to validate their control posture.

Cyber Control Capability Uplift

- Designing and implementing the policies, standard, processes and tooling for identified cyber capability controls.
- Enhance the reporting of cyber risk management through operational and executive reporting as well as real-time risk dashboards.
- Provide project assurance over cyber capability uplift programs to ensure timeliness and achievement of objectives.

Contacts

Nicola Nicol | Melbourne
Partner
M: +61 436 444 949
E: nicola.nicol@pwc.com

Ryan Ettridge | Brisbane
Partner
M: +61 417 702 234
E: ryan.ettridge@pwc.com

Philippa Cogswell | Sydney
Director
M: +61 410 588 877
E: philippa.cogswell@pwc.com

Robert di Pietro | Canberra
Partner
M: +61 418 533 346
E: robert.di.pietro@pwc.com

Jason Knott | Perth
Partner
M: +61 417 455 074
E: jason.knott@pwc.com

Kim Cheater | Adelaide
Partner
M: +61 414 227 035
E: kim.cheater@pwc.com

To find out how PwC Australia is responding to COVID-19, please visit:
https://www.pwc.com.au/about-us/notices/coronavirus.html

For our latest insights and resources, please visit:
https://www.pwc.com.au/important-problems/coronavirus-covid-19.html

PwC refers to the Australia 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.
This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.
Liability limited by a scheme approved under Professional Standards Legislation.