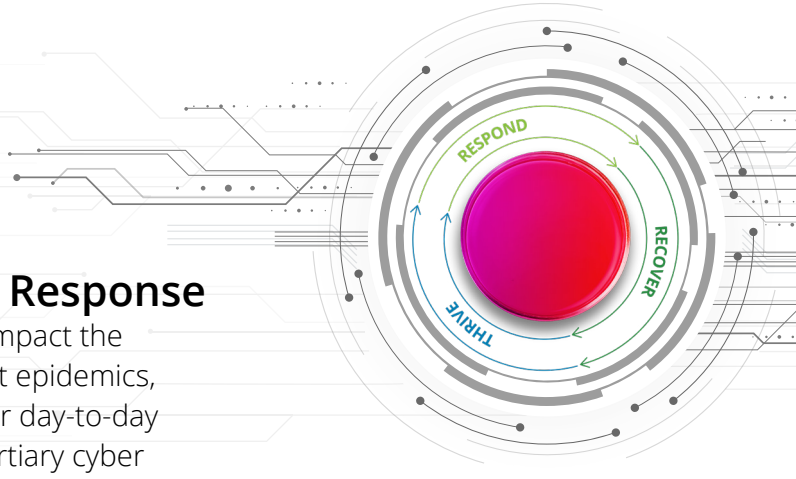
Deloitte.



COVID-19: Cyber Preparedness & Response

There is limited precedent into how COVID-19 will impact the technology-reliant business world today. Unlike past epidemics, COVID-19 has caused financial "shocks" and broader day-to-day disruption which will likely lead to secondary and tertiary cyber implications. The Deloitte Cyber team shares considerations that your organisation can use to ensure preparedness and response during these challenging times.

The Landscape

There is **limited precedent** into how COVID-19 will impact the technology-reliant business world today. Unlike past epidemics, COVID-19 has caused **discrete financial "shocks" and broader day-to-day disruption** which will likely lead to **secondary and tertiary cyber implications**

Cyber Considerations

Immediate impact / reactions to temporary disruption → **Long-term impact / reactions to economic climate**

	Remote work and staffing / availability disruption	Increase in click bait / social engineering	Relaxing risk tolerances for third parties	Latent threats and reduced / reallocated spend	Increase in opportunistic M&A activity	Layoffs / disgruntled Employees
Trend						
Cyber Impact	• Greater remote access demands test VPN bandwidth and controls • Some technology implementations are fast tracked • New need to secure and monitor home networks arises • Personnel availability is impacted by exceptional family care needs	• Uptick in socially-engineered cyber attacks target financial and PII data • Themed phishing and malware attacks raise cyber risk levels • Spread of misinformation poses crisis response challenges	• Supply chain disruption implicates security operations – contingency providers may not provide the same security coverage, increasing digital risks • Coverage of security service providers is implicated by quarantines	• Reduced budgets lead to under-resourcing of security functions, contributing to greater digital risk • Threats from early opportunistic attacks remain latent in the environment and pose sustained elevated risk	• Long term economic dynamics may lead to opportunistic M&As that move quickly and forgo sufficient cyber due diligence (e.g., adversary analysis, threat avoidance appetite assessment, compromise assessment, red teaming security assessment, etc.)	• Disturbances to normal business cycles force re-organisations or widespread employee cuts • Work and economic climates contribute to greater risks of insider threats
Consideration	• Are your remote access controls built to scale? • How will security keep up with expedited tech projects and new support needs?	• How are you raising awareness and bolstering threat detection & response to promote proactive identification of malicious activity?	• How are you fast-tracking third party security plans to prioritize access and availability of services?	• How will you make your security programs higher performing and more efficient in a tougher economic climate?	• How are you incorporating cyber into your M&A / corporate strategy?	• How are you positioned to pursue a risk-based insider threat monitoring program?

Steps to Secure your Environment

TODAY

Create a running diary (e.g., transcripts)
- Designate personnel as log-keepers

Get a handle on how teams are choosing to collaborate virtually
- Confirm systems are scaled
- Ensure threat / risk assessments are completed before technologies are adopted
- Identify global remote workforce, including data & delivery centers

Discern supply chain dependencies and disruptions
- Assess SLAs and analyse downstream impacts of third-party disruption
- **Update business continuity plans**
- Verify succession planning
- Determine essential functions and support activities to identify systems to be maintained and to be taken offline

TOMORROW

Engage the workforce on security implications of working from home
- Cover key remote work leading practices (e.g., sharing files securely, using VPN, maintaining secure passwords, ensuring security of wireless & home network configurations, adapting to shared living environments, and securing physical company-owned IT assets)

Secure remote access
- Review VPN governance security posture (e.g., patching status and scalability), deployment of multi-factor authentication, and scope of services to be securely accessed remotely
- Deploy remote workspace capabilities for employees and ensure they are securely configured

NEXT WEEK

Bolster threat detection and response capabilities
- Confirm integration of threat intelligence programs with security event monitoring
- Perform active vulnerability discovery and threat hunting
- Communicate proactively with your workforce and third parties to ensure focus on prevention
- Create a plan to ensure uninterrupted, 24x7 coverage and alert volume surge capacity

Revisit security monitoring controls
- Re-baseline traffic/behavior patterns
- Tune/develop and deploy new monitoring rulesets, thresholds, and escalation paths
- Increase scanning for shadow IT

NEXT MONTH

Assess scalability/longevity of security solutions, update security incident response playbooks, and create an after-action report
- Include changes in call trees, points of contact, IT procedures, and system prioritization
- Document gaps identified, insights gained, and areas of improvement

Bolster security in high-risk areas
- Update security architecture and ensure coverage for insider threat and cyber diligence

Develop a mature enterprise-wide crisis management capability to:
- Perform sensing, monitoring, reporting, fine tune operating picture
- Develop executive intent and strategy for response
- Plan stakeholder engagement, crisis communications, and operational response

Elevated threats of today will persist and pose sustained risk in your environment

Our Services

Cyber Fusion Services
- Security monitoring
- Threat intelligence
- Attack surface management
- Threat hunting
- Data loss prevention

Awareness & Training Programs
- Phishing awareness
- Training campaigns
- Enterprise communications

Incident Response (IR) & Business Continuity
- IR plans and retainers
- Digital forensics, malware, and threat analysis
- Breach impact analysis
- Business continuity and Technical resilience plans

Identity and Data Protection
- Identity governance
- Access management
- Risk-based authentication
- Data governance
- Data privacy (e.g., GDPR compliance)

Other Considerations

Overall Security Programs and Risk Tolerances:
- Scaling of security systems & processes
- Increased attack surface area
- Identity governance controls
- New hires & terminations
- Incapability of remote work
- Cloud security to support e-commerce
- BYOD & non company-issued device risk
- Complexities for power & utilities
- Privacy implications of employee health monitoring

For Hospitals and Healthcare & Emergency Response:
- Opportunistic and targeted disruption/ DoS and exfiltration of PII while organisation under extreme delivery strain

For Government and Public Services:
- Monitor for emerging cyber schemes to steal citizen identities and defraud government tax and benefits agencies
- Refresh alternatives for securing sensitive activities (e.g., mobile Sensitive Compartment Information Facilities [SCIFs], remote verification of identities to process clearances, hard tokens)
- Adopt new methods for students, faculty, and administrators to conduct transactions (e.g., secure testing, research lab security)

For more information and assistance on any incidents and issues experienced, please contact:

Eric Mc Gee erimcgee@deloitte.co.za | Cathy Gibson cgibson@deloitte.co.za | Tiaan van Schalkwyk tvanschalkwyk@deloitte.co.za