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

Remote work and staffing / availability disruption

- 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
- up with expedited tech projects and new support needs?

Increase in click bait social engineering

- Uptick in sociallyengineered cyber attacks target financial and PII data
- Themed phishing and malware attacks raise cyber risk levels
- Spread of misinformation poses crisis response challenges

Relaxing risk tolerances for third parties

- Supply chain disruption implicates security operationscontingency providers may not provide the same security coverage, increasing digital risks
- Coverage of security service providers is implicated by quarantines
- tracking third party security plans to prioritize access and

Latent threats and reduced /

Reduced budgets lead to under-resourcing of security functions, contributing to greater digital risk

reallocated spend

Threats from early opportunistic attacks remain latent in the environment and pose sustained elevated risk

security programs

more efficient in a tougher economic

Increase in opportunistic M&A activity

Long-term impact / reactions to economic climate

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.)

incorporating cyber into

Layoffs / disgruntled **Employees**

- Disturbances to normal business cycles force re-organizations or widespread employee cuts
- Work and economic climates contribute to greater risks of insider threats
- How are you positioned to pursue a risk-based monitoring program?



Steps to Secure your Environment

- Create a running diary (e.g., transcripts)
 - Designate personnel as logkeepers
- 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 analyze 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

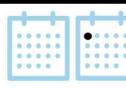
Tomorrow

- 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 companyowned IT assets)
- Secure remote access
 - Review VPN governance security posture (e.g., patching status and scalability), deployment of multifactor 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



- 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



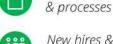
For Government and Public Services:

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:



New hires & terminations

BYOD & non company-

issued device risk

Scaling of security systems



Incapability of remote work

surface area

Increased attack

Complexities for

power & utilities

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such

making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before



Cloud security to support e-commerce

Identity governance

controls



Privacy implications of employee health monitoring

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Monitor for emerging cyber schemes to steal citizen identities

Refresh alternatives for securing sensitive activities (e.g., mobile

Adopt new methods for students, faculty, and administrators to conduct transactions (e.g., secure testing, research lab security)

Sensitive Compartment Information Facilities [SCIFs], remote

verification of identities to process clearances, hard tokens)

and defraud government tax and benefits agencies

Copyright © 2020 Deloitte Development LLC. All rights reserved.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

For further clarification on services & next steps to consider, please contact: Coronavirus Response | USCyberCoronavirusResponse@deloitte.com | Deborah Golden | debgolden@deloitte.com | Jason Frame | jframe@deloitte.com | Kelly Miller Smith | kellysmith@deloitte.com