Cyber Considerations

Immediate impact / reactions to temporary disruption

- Remote work
  - Greater remote access demand
  - 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

- Increase in click bait / social engineering
  - Upskilling in socially-engineered cyber-attacks targeting financial and PII data
  - Themed phishing and malware attacks raise cyber risk levels
  - Spread of misinformation poses crisis response challenges

- Relating risk tolerances for third parties
  - Supply chain disruption inflates security operations—contingency providers may not provide the same security coverage, increasing digital risk vulnerabilities
  - Coverage of security service providers is implicated by quarantines

- Latent threats and reduced reallocating spend
  - Reduced budgets lead to under-deployment of security features, contributing to greater digital risk
  - Threats from early opportunistic attacks remain latent in the environment, and pose sustained elevated risk

- Increase in opportunistic M&A activity
  - Long-term economic dynamics may lead to opportunistic M&As that move quickly and forge sufficient cyber due diligence (e.g., adversary analysis, threat avoidance, appetite assessment, compromise assessment, red teaming security assessment, etc.)

- 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

Consideration

- Are your remote access controls built to scale?
- How will security keep up with urgent shift to projects and in-person intelligence support needs?

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 disruption
  - Assess SUAs and analyze downstream impacts of third-party supply chain

- 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 leading and implications of working from home
  - Cover key remote work leading practices (e.g., sharing files securely, using VPN, maintaining secure passwords, ensuring security for multi-tenant network configurations, adapting to diverse working 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 and remotely enabled

- 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 mitigate unintended, 24/7 coverage, and alert volume surge capacity

- Reduce security monitoring costs
  - Reduce baseline traffic/behavior patterns
  - Tymber develop and deploy new monitoring tools, thresholds, and escalation paths

- Increase scanning for shadow IT

Next Month

- Assess scalability / functionality 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
  - 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

- IT plans and retainers
- Digital forensics, malware, and threat analysis
- Breach impact analysis
- Business continuity and Technical resilience plans

Identity and Access Protection

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

Other Considerations

Overall Security Programs and Risk Tolerances:
- Scaling of security systems & processes
- New hires & terminations
- ROI & non-company assigned device risk

- Increased attack surface area
- Inapplicability of remote work
- Complexities for power & utilities
- Privacy implications of employee health monitoring

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 Secure Compartment Information Facilities (SCIIF), 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)

About Deloitte

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 professional advice or services, nor should it be viewed as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

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 | dgolden@deloitte.com | Jason Frame | jframe@deloitte.com | Kelly, Miller Smith | ksmiller@deloitte.com

Copyright © 2020 Deloitte Development LLC. All rights reserved.