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

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 policies are stated
• Ensure threat / risk assessments are completed before technologies are adopted
• Identify global remote workforce, including data & delivery centers
• Discern supply chain dependencies and discontinuity issues
• 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 and office 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 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 volume surge capacity
  • Revise security monitoring controls
  • Re-base traffic behavior patterns
  • Tune&develop and deploy new monitoring tools, 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

Our Services

Cyber Fusion Services
• 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 rehearsals
• Digital forensics, malware, and threat analysis
• Breach impact analysis
• Business continuity and Technical resilience plans

Identity and Data Protection
• Identity governance controls
• 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
- Cloud security to support e-commerce
- Privacy implications of employee health monitoring

- New hires & terminations
- Inability of remote work
- Complexities for power & utilities
- Invalid or non-compliant device risk

- Increased attack surface area
- Identity governance controls
- Cloud security to support e-commerce
- 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 assets (e.g., mobile, sensitive Commercial Information Facilities [CIFs]), 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
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.