

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		
Trend	<b>Remote work and staffing / availability disruption</b>	<b>Increase in click bait / social engineering</b>	<b>Relaxing risk tolerances for third parties</b>	<b>Latent threats and reduced / reallocated spend</b>	<b>Increase in opportunistic M&amp;A activity</b>	<b>Layoffs / disgruntled Employees</b>
Cyber Impact	<ul style="list-style-type: none"> <li>Greater remote access demands test VPN bandwidth and controls</li> <li>Some technology implementations are fast tracked</li> <li>New need to secure and monitor home networks arises</li> <li>Personnel availability is impacted by exceptional family care needs</li> </ul>	<ul style="list-style-type: none"> <li>Uptick in socially-engineered cyber attacks target financial and PII data</li> <li>Themed phishing and malware attacks raise cyber risk levels</li> <li>Spread of misinformation poses crisis response challenges</li> </ul>	<ul style="list-style-type: none"> <li>Supply chain disruption implicates security operations--contingency providers may not provide the same security coverage, increasing digital risks</li> <li>Coverage of security service providers is implicated by quarantines</li> </ul>	<ul style="list-style-type: none"> <li>Reduced budgets lead to under-resourcing of security functions, contributing to greater digital risk</li> <li>Threats from early opportunistic attacks remain latent in the environment and pose sustained elevated risk</li> </ul>	<ul style="list-style-type: none"> <li>Long term economic dynamics may lead to opportunistic M&amp;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.)</li> </ul>	<ul style="list-style-type: none"> <li>Disturbances to normal business cycles force re-organizations or widespread employee cuts</li> <li>Work and economic climates contribute to greater risks of insider threats</li> </ul>
Consideration	<ul style="list-style-type: none"> <li>Are your remote access controls built to scale?</li> <li>How will security keep up with expedited tech projects and new support needs?</li> </ul>	<ul style="list-style-type: none"> <li>How are you raising awareness and bolstering threat detection &amp; response to promote proactive identification of malicious activity?</li> </ul>	<ul style="list-style-type: none"> <li>How are you fast-tracking third party security plans to prioritize access and availability of services?</li> </ul>	<ul style="list-style-type: none"> <li>How will you make your security programs higher performing and more efficient in a tougher economic climate?</li> </ul>	<ul style="list-style-type: none"> <li>How are you incorporating cyber into your M&amp;A / corporate strategy?</li> </ul>	<ul style="list-style-type: none"> <li>How are you positioned to pursue a risk-based insider threat monitoring program?</li> </ul>

Steps to Secure your Environment

Today	Tomorrow	Next Week	Next Month
<ul style="list-style-type: none"> <li>Create a running diary (e.g., transcripts)                             <ul style="list-style-type: none"> <li>Designate personnel as log-keepers</li> </ul> </li> <li>Get a handle on how teams are choosing to collaborate virtually                             <ul style="list-style-type: none"> <li>Confirm systems are scaled</li> <li>Ensure threat / risk assessments are completed before technologies are adopted</li> <li>Identify global remote workforce, including data &amp; delivery centers</li> </ul> </li> <li>Discern supply chain dependencies and disruptions                             <ul style="list-style-type: none"> <li>Assess SLAs and analyze downstream impacts of third-party disruption</li> </ul> </li> <li>Update business continuity plans                             <ul style="list-style-type: none"> <li>Verify succession planning</li> <li>Determine essential functions and support activities to identify systems to be maintained and to be taken offline</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>Engage the workforce on security implications of working from home                             <ul style="list-style-type: none"> <li>Cover key remote work leading practices (e.g., sharing files securely, using VPN, maintaining secure passwords, ensuring security of wireless &amp; home network configurations, adapting to shared living environments, and securing physical company-owned IT assets)</li> </ul> </li> <li>Secure remote access                             <ul style="list-style-type: none"> <li>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</li> <li>Deploy remote workspace capabilities for employees and ensure they are securely configured</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>Bolster threat detection and response capabilities                             <ul style="list-style-type: none"> <li>Confirm integration of threat intelligence programs with security event monitoring</li> <li>Perform active vulnerability discovery and threat hunting</li> <li>Communicate proactively with your workforce and third parties to ensure focus on prevention</li> <li>Create a plan to ensure uninterrupted, 24x7 coverage and alert volume surge capacity</li> </ul> </li> <li>Revisit security monitoring controls                             <ul style="list-style-type: none"> <li>Re-baseline traffic/behavior patterns</li> <li>Tune/develop and deploy new monitoring rulesets, thresholds, and escalation paths</li> <li>Increase scanning for shadow IT</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>Assess scalability/longevity of security solutions, update security incident response playbooks, and create an after-action report                             <ul style="list-style-type: none"> <li>Include changes in call trees, points of contact, IT procedures, and system prioritization</li> <li>Document gaps identified, insights gained, and areas of improvement</li> </ul> </li> <li>Bolster security in high-risk areas                             <ul style="list-style-type: none"> <li>Update security architecture and ensure coverage for insider threat and cyber diligence</li> </ul> </li> <li>Develop a mature enterprise-wide crisis management capability to:                             <ul style="list-style-type: none"> <li>Perform sensing, monitoring, reporting, fine tune operating picture</li> <li>Develop executive intent and strategy for response</li> <li>Plan stakeholder engagement, crisis communications, and operational response</li> </ul> </li> </ul>

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

Our Services

<p><b>Cyber Fusion Services</b></p> <ul style="list-style-type: none"> <li>Security monitoring</li> <li>Threat intelligence</li> <li>Attack surface management</li> <li>Threat hunting</li> <li>Data loss prevention</li> </ul>	<p><b>Awareness &amp; Training Programs</b></p> <ul style="list-style-type: none"> <li>Phishing awareness</li> <li>Training campaigns</li> <li>Enterprise communications</li> </ul>	<p><b>Incident Response (IR) &amp; Business Continuity</b></p> <ul style="list-style-type: none"> <li>IR plans and retainers</li> <li>Digital forensics, malware, and threat analysis</li> <li>Breach impact analysis</li> <li>Business continuity and Technical resilience plans</li> </ul>	<p><b>Identity and Data Protection</b></p> <ul style="list-style-type: none"> <li>Identity governance</li> <li>Access management</li> <li>Risk-based authentication</li> <li>Data governance</li> <li>Data privacy (e.g., GDPR compliance)</li> </ul>
---	---	--	---

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 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)

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 used 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.

**About Deloitte**  
As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see [www.deloitte.com/us/about](http://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.

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

Copyright © 2020 Deloitte Development LLC. All rights reserved.