Deloitte.

Staying safe – sustaining your organizational cyber hygiene amid COVID-19 disruption

Within a matter of days, business operations across industries and geographies have been radically altered. After initial business continuity efforts, organizations should now consider establishing new operating models to address an unplanned, rapid, and massive shift to a remote workforce. The ability to remain connected and productive is critical to executing the mission and may dictate the survival of the business. Meanwhile, our public health remains threatened and digital risks are rising.. In the coming months, organizations should consider leveraging a risk-based approach to realign business and security priorities to adapt to a new, increasingly complex, and more difficult IT landscape.

Security challenges heightened by COVID-19:

- Increased use of collaboration tools and other, often unapproved & unmanaged, SaaS applications (Shadow IT)
- Large numbers of new devices (personal and scaled corporate devices) connecting to the corporate network
- Rapidly implemented technologies that lack sufficient hardening and security controls
- Malicious and inadvertent insider threats caused by disgruntled or displaced employees and contractors
- Evolving compliance circumstances for regulated industries
- Early opportunistic attacks become sustained campaigns as network visibility is more difficult to maintain
- Limited and inconsistent security of home networks that store, process and transmit sensitive business data
- Already stretched cyber security resources manage an increased attack surface
- Greater difficulty in maintaining compliance with data privacy regulations in more distributed IT environments
- Complex requirements for identity and access management as roles and responsibilities change

Although many of these security challenges existed prior to the COVID-19 pandemic, they now pose an even greater threat to businesses as the size and scale of connectivity for remote operations expands. The current environment dictates that leaders place greater focus on these issues, while also prioritizing business agility. Risk-driven prioritization of initiatives during this time enables the mission, while providing long-term operational viability and organizational resilience.

Steps to consider:

Develop a risk-based prioritized security strategy and strengthen basic security coverage

□ **Define services critical to mission/business to inform prioritized security strategy**

- Determine service line criticality to prioritize access and availability. Involve stakeholders to understand how service line criticality has been impacted by COVID-19 (e.g., certain service lines have greater demand/importance of availability than under normal operations)
- Evaluate service and system risks, including access points and vulnerability. Quantify risk levels where possible
- Focus initial efforts on securing critical services and systems that pose the substantial security threat (e.g., sensitive data transactions or greater threat vector exposure)
- Explore whether high risk, lower value systems can be temporarily taken offline to avoid undue risk exposure
- Phase efforts and execute them methodically to bring security in lockstep with business operations

□ **Enhance threat monitoring capabilities and hunt threats within your network(s)**

- Re-baseline traffic patterns and tune endpoint agents for new processes
- Expand scope of threat intelligence focus to consumer services
- Confirm coverage for high-risk areas (e.g. data protection, insider threat)
- Integrate Data Leak Prevention (DLP) and document rights management into monitoring tools
- Perform periodic sentiment analysis of your workforce
- Actively monitor for disinformation that may negatively impact your mission
- Update your security incident response playbooks to reflect potential new threats/risks

□ **Address third party and supply chain risks**

- Identify supply chain dependencies and disruptions
  - Assess contractual coverage and analyze downstream impacts of third parties
- Determine surge support requirements associated with overstretched security personnel
- Integrate appropriate third party governance controls into identity and access management protocols and threat monitoring to support remote delivery requirements
- Implement technology and processes for secure communications and information exchange

□ **Stand up Project Management Office (PMO) to execute phased security approach**

- Recognize that elevated risk levels will persist and prepare to articulate sustained cyber risk exposure to leadership
- Integrate security project management efforts with broader COVID-19 response efforts to keep in lockstep with transformation and business continuity efforts

Client Perspectives

As the situation continues to evolve, businesses are facing distinct challenges associated with mission, industry, and corporate structure

"I need to evolve my Help Desk to accommodate greater remote service delivery"

Action: Develop plans to bypass traditional 'walkup' services—to include Software and Hardware Support; IT staff surge support plans; assistance with setting up secure home networks; and securely configuring home computers to be used for work

"How can I enable remote work of employees without company-issued machines?"

Action: Update software patches on BYOD devices; disable email attachment auto-downloads; use accepted cloud-based storage for backup; and deploy secure collaboration platforms and cloud-based technologies to share data

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

Deloitte.

Staying safe – sustaining your organizational cyber hygiene amid COVID-19 disruption

Implement and scale security controls for a mobile workforce

□ Secure systems that enable remote access

- Maintain security updates/patching for Virtual Private Networks (VPNs)
- Implement multi-factor authentication (MFA) for remote access
- Confirm sufficient number of VPN software client licenses are available
- Employ VPN split tunneling for improved performance
- Implement Cloud Access Security Broker (CASB), Secure Web Gateway (SWB), and other capabilities for SaaS and other hosted cloud-based platforms

□ Reinforce identity and access control mechanisms

- Adjust user roles and permission sets to accommodate new work requirements (e.g. rotational roles, remote access permissions for rulesets that traditionally may not allow for remote access)
- Require authentication for network and cloud-based systems and applications based on risk, including MFA and Single-Sign-On (SSO)
- Implement Privileged Access Management (PAM)
- Confirm use of least privilege principles across enterprise applications and systems
- Create a plan to navigate increased volume of individual rights requests and greater effort required to keep inventory of personal information processing up to date with business and technology changes

□ Bolster endpoint security

- Confirm configuration of host-based firewalls, antimalware and intrusion detection/prevention system (IDS/IPS) systems
- Confirm ability to patch and distribute software remotely
- Consider Mobile Device Management (MDM) technologies for BYOD needs

□ Define and communicate adjustments to privacy and data protection frameworks

- Identify deviations from normal data flows and impacts on laws/regulations
  - Consider whether explicit consent is required to adjust processes
- Evaluate implications of shifting privacy directives on business processes
  - Determine contractual coverage for third-party support areas
- Determine data protection strategies to accommodate operational shifts and implement Privacy by Design (PbD) where feasible
- Disseminate notices to customers where applicable
- Evaluate additional insurance options given elevated risk of a privacy breach
- Conduct a threat/risk assessment of new technologies to include integration with data privacy regulations

□ Implement technologies and processes to align with new IT operations model and accommodate capacity strains

- Adjust existing rulesets for tools (e.g., DLP, CASB, and UEBA) to align with new data and collaboration patterns and identify anomalous behavior
- Implement private access tools to allow for secure access to data and applications for credentialed users
- Implement secure virtual desktop environments to enable remote access and disable access to local storage and connected devices
- Leverage email and file level rights management for sensitive communications

□ Strengthen insider threat prevention & detection capabilities

- Implement Data Loss Prevention (DLP), User and Entity Behavior Analytics (UEBA) and Document Rights Management (DRM) technologies
- Encrypt and password-protect files, particularly where DRM is not possible, and provide password to intended recipient separately and via a separate communications channel (e.g., phone call, SMS text)
- Create tripwires associated with specific words within email content and policies prohibiting unmanaged USB devices

Communicate with and train employees to take an active role in security

□ Determine PMO communications strategy

- Plan PMO communications cadence, role-based content, mediums, etc.
- Include resources to facilitate engagement and prioritize physical and mental well-being

□ Create and communicate resources to support secure remote work environments, including:

- Updating wireless network name (SSID) to prevent identifying owner/user(s)
- Changing default or updating weak wireless network passwords
- Enabling wireless encryption (WPA2-AES)
- Deploying home network routers that provide firewall and network access translation (NAT) and enable web content filtering services
- Requiring use of corporate VPNs and disabling home network file sharing
- Locking unattended devices & preventing others from using company devices
- Being mindful of shoulder surfing depending on remote work setup
- Securing PHI/PII in a locked safe or drawer and secure printing practices

□ Update / tailor, as required, and implement employee security awareness, education & training

Review and update policies, trainings, and communications, as required:

- Identify areas that may require updated policies to accommodate changes to regular operating procedures
- Communicate policies (and updates), expectations and available resources to employees and contractors
- Determine deficiencies in the workforce's cybersecurity awareness, knowledge and skills and identify trainings that may be valuable to push out as refreshers
- Continually update cybersecurity awareness, education and training to focus on current and pervasive phishing campaigns and social engineering attack vectors (e.g. COVID-19-related schemes)
- Provide clear guidance and procedures for suspected malware incident, particularly ransomware, in order for employees to take immediate action and help contain incident damage and spread

Takeaways

Organizations should prepare for the long haul as they seek to serve customers and their workforce in the coming months. There is unlikely to be a "quick fix" to COVID-19-driven challenges; and when a return to normalcy occurs, it is likely to be gradual rather than a quick shift back to regular operations. Further, "regular" operations post-pandemic may be fundamentally different from those prior to this global outbreak, with impacts on organizational business models, resilience, and culture still unknown. Actions now will dictate risk exposure for months, if not longer, and gradual steps to mitigate IT-based risks will help safeguard organizational resiliency for the future.

1. Act rapidly to adopt a risk-based approach to managing elevated threat levels
2. Adjust your infrastructure to keep an active pulse on data protection and privacy
3. Empower your employees to work securely, while promoting physical and mental well-being

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.

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

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.

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