REMOTE WORK READINESS ASSESSMENT

LIBERTY ADVISOR GROUP

ARE YOU READY?

The novel coronavirus (COVID-19) outbreak has sickened over 2 million people worldwide. Governments have closed borders and are imposing quarantines, and most companies now work remotely. The full extent of human and economic impact remains to be seen.

This epidemic is a wake-up call for companies to carefully review the strategies, policies, and procedures they have in place to protect employees, customers, and operations in this and future epidemics, notes the *Harvard Business Review*.

Here are 5 questions to evaluate your organization's readiness.

1. **Do you have the right tools and technology to support remote work?**
   Make sure your virtual teams are working without interruption. Keep your employees productive, organized and connected by leveraging the right remote collaboration tools like Microsoft Teams, Zoom or Slack.

2. **Can your IT infrastructure and tools support the increased volume and traffic?**
   Not only do you need to ensure you are effectively using the right tools and technology, it is also important to optimize your network and manage bandwidth effectively to deliver the best user experience.

3. **Do you have the right cybersecurity controls in place?**
   As workforces are increasingly operating remotely, cybersecurity measures are essential to safeguard your workforce. IT departments are faced with a difficult balance of quickly pivoting systems and infrastructure to enable the remote workforce while also keeping the company's data and resources secure. The Federal Bureau of Investigation (FBI) recently issued warnings of an uptick in fraudulent crimes tied to the coronavirus. More than one-third of executives say that cyberthreats have increased as a majority of their employees work from home, according to CNBC. This is the time to make sure your organization has the right cybersecurity controls in place.

4. **Do you have the right procedures, policies and training to support a remote workforce?**
   Set your remote employees up for success. Working from home can feel very isolating and lead to confusion, fear and uncertainty. Outline clear expectations and remote work policies and take a flexible approach that can be modified. Set up clear protocols and performance measurements.

5. **Can your organization continue to perform essential functions without disruption?**
   As we learn more about the risks of the coronavirus, it is vital not to overlook the need to assess your organization's pandemic readiness, and to review your continuity plan. This includes policies on remote work, cybersecurity awareness, business continuity, backup, incident response and compliance with applicable regulations. Taking a comprehensive and integrated approach will help you to protect employees, insulate operations, and ensure supply chain stability to maintain essential services for your customers.

Leverage Liberty Advisor Group's experience helping clients navigate remote working and sustaining a remote workforce. Ensure your company is set up for productivity and success. **Here is our must-do remote readiness checklist.**

MUST-DO REMOTE READINESS CHECKLIST

1 REMOTE TOOLS AND TECHNOLOGY

- ☐ Ensure that your remote tools are easy to use and understand.
- ☐ Ensure that your remote tools are truly secured.
- ☐ Verify that your remote tools offer all of the functionality you need: video conferencing, file sharing, etc.
- ☐ Re-examine all firewall rules. Lock down all non-essential traffic.
- ☐ Verify all remote access protocols are secured.

2 BANDWIDTH

- ☐ Ensure that VPN networks can handle expanded remote workforce traffic.
- ☐ Work with network providers to quickly and securely deliver additional VPN connectivity and network capacity.

3 CYBERSECURITY

- ☐ Ensure that administrators have privileged accounts in place with strong security controls.
- ☐ Lock down access to sensitive data and applications.
- ☐ Identify and consider quarantining “high risk” technologies/devices.
- ☐ Ensure that all applications and operating systems are patched frequently.
- ☐ Confirm that anti-virus/anti-malware definitions are up to date and applied to all endpoints.
- ☐ Enact heightened security protocols on all financial transactions.
- ☐ Review email server rules/settings to ensure proper anti-phishing controls are in place.
- ☐ Examine monitoring, alerting and logging and consider lowering thresholds and increasing frequencies.

4 POLICIES AND PROCEDURES

- ☐ Do not allow personal computing equipment access to corporate networks without putting the proper controls in place.
- ☐ Ensure multi-factor authentication is enabled on all applications involving corporate data.
- ☐ Review and enhance password policies and controls.
- ☐ Provide enhanced and more frequent guidance and training on phishing.
- ☐ Review backup policy and procedures – ensure they are effective and viable in the event of a failure/incident.
- ☐ Consider deploying enhanced policies to further secure endpoints.

5 DISRUPTION

- ☐ Ensure the proper business continuity and incident response plans are in place and reviewed with key staff.
- ☐ Identify and delineate all essential functions.
- ☐ Create a succession plan for leadership and emergency delegation of authority.
- ☐ Ensure that all vital records and databases are secure.
- ☐ Identify alternate operating strategies.
- ☐ Ensure that you have a strong communications plan.