CYBER READINESS
INSTITUTE

Cyber Readiness for the Hybrid Remote-Office Workplace

Companies of all sizes now recognize that there is going to be a more permanent “new reality” to the workplace. Many companies are only sending a small percentage of their workforce back into the physical office, which means the hybrid work environment – some employees working from home and some working from the office – will become the reality.

This reality requires companies to develop and implement resilient cybersecurity policies that address the hybrid workplace. During the initial months of the pandemic, many companies had to focus on business continuity, and they relaxed security policies to help individuals work efficiently from remote locations. It is now time to replace those relaxed security policies with the development of hybrid policies that ensure equal security across all work environments.

CRI is focused on helping small and medium-sized enterprises (SMEs) establish secure policies and procedures in this hybrid environment.

For both managers and employees, it makes sense to think about cyber readiness for the hybrid workplace in terms of People, Process, and Technology. Although these categories may be over-used to some of you, they provide a useful way to think and communicate about cyber readiness – especially to people grasping to understand how to address cybersecurity issues in this dynamic environment.

People – what are the changes in behavior that are needed to be productive and cyber ready?

Process – what are the changes in policies and procedures that are needed to define clear expectations for employee behavior and set employees up for success?

Technology – what new technology is needed to improve cybersecurity when employees are working remotely or routinely shifting between home and office?

The Cyber Readiness Institute focuses on human behavior – the People and Process of the framework outlined above – but we will also provide guidance on technology in the hybrid work environment.

Below are important tips to help managers prioritize what they need to do to ensure a secure, hybrid environment.

Make sure each employee is trained and comfortable with your organization's policies on:

- **Passwords:** Strong authentication includes the use of 16-character passphrases and multi-factor authentication, whenever possible.
- **Phishing:** Provide frequent and up-to-date education on phishing activities that include examples of recent home vs. work phishing attempts – especially related to COVID-19.
- **USB use:** Provide disciplined guidelines for how to work on company documents from multiple locations. This approach could include the establishment of a cloud-based file-sharing system and training.
- **Software updates:** Outline expectations that updates should be downloaded immediately to any device used to access the company network.

All enterprises should attempt to issue a work laptop to all employees working from home to avoid the use of personal devices for work. If this is not financially possible, work with your employees to set-up a separate user account on their personal device.

Given the increased dependence on video communications platforms, ensure you are using platforms with security protocols in place – including the use of a distinct password for each meeting.

Establish proactive and regular communications with your team, including:

- Weekly staff calls
- Regularly scheduled 1:1 check-ins

Stay tuned for additional guides in our series on the hybrid workplace as we demystify cybersecurity in this new reality and work environment by providing tips for managers and employees.

About CRI

The Cyber Readiness Institute is a non-profit initiative that convenes business leaders from across sectors and geographic regions to share resources and knowledge that inform the development of free cybersecurity tools for small and medium-sized enterprises (SMEs). Our Remote Work Resources are available in Spanish and French. The self-guided, online Cyber Readiness Program is available in Chinese, English, French, Spanish, Portuguese, Arabic, and Japanese. To find out more, visit www.BeCyberReady.com.