

Navigating Coronavirus Cybersecurity Challenges

As the number of Novel Coronavirus (COVID-19) cases grows, most businesses are acting quickly to stem the spread of the virus and protect the health of their workers, while doing their best to minimize negative impacts on business operations and profitability.

Ramping up Your Remote Workforce

Many companies are asking employees to work from home. While this is a reasonable and prudent strategy in these uncertain times, it also exposes your business to cybersecurity vulnerabilities that do not exist with on-premise work. The good news is that Tevora's knowledgeable team of cybersecurity experts can help you make this transition quickly and securely.

Remote Work Cybersecurity Risks

Here are some of the key steps you'll need to take to address the cybersecurity risks associated with remote work:

- **Personal Devices**—If you plan to allow employees to use personal devices to access your network, you'll need to ensure they have the same level of security as devices provided by your business. This may involve implementation of technologies such as multi-factor authentication. You'll need to implement solutions to provide your business with visibility into which devices are accessing your network and how they are configured. You'll also need to ensure the required security patches have been applied.
- **Wi-Fi Networks**—If your employees will be accessing sensitive information, you'll likely need to implement Virtual Private Network (VPN) solutions to ensure their remote work communications are encrypted.
- **Access Management**—You'll need to have systems in place to ensure remote workers are granted the same privileges and access rights they have when accessing your network from the office.
- **Incident Response**—You likely have procedures in place for responding to a data breach or other type of security incident. However, you'll need to ensure your team has the tools and training required to effectively respond to an incident while working remotely. This may involve making tools such as conferencing, messaging, and security monitoring available to remote team members.
- **Training**—Remote workers will need training to ensure they understand the policies, procedures, and technologies required in a secure remote working environment. For example, it's critical that sensitive business information not be stored on their personal devices in unencrypted form.
- **Policies**—You'll need to ensure your cybersecurity policies address remote work environments. You may need to update your current policies to address the unique risks described above.

Tevora's cybersecurity experts have significant experience helping some of the world's largest companies navigate these challenges and are well-positioned to guide you as you scale up your remote work environment.

Security Audit

You may feel that you already have a robust and secure remote work environment, but would like a knowledgeable third party to audit your environment before you scale it up. Tevora's experienced audit team can work with you to identify potential cybersecurity vulnerabilities and recommend strategies for mitigation.

Choose a Partner That Offers Services Remotely

To honor the CDC's social distancing guidelines, it's important to work with partners that can provide services remotely. Fortunately, Tevora has the tools and skills needed to help you transition to remote work without the need to meet with your team in person. We're fully equipped to help you deploy the tools, technologies, and policies needed to enable your transition without visits to your site. We believe this is the responsible way to conduct business in these unique and challenging times.

In addition to supporting your remote work transition, Tevora offers a wide range of [services](#)—also available remotely—to fortify your company's defenses, reinforce your compliance with industry and government regulations, and guide you to more effective management of cyber risk throughout your environment.

Contact your Tevora representative to learn more about how we can be a trusted partner to help you navigate these challenging times.