DEANDORTON
Insights

Keeping business going and staying secure

The current situation and the necessary restrictions to keep congregating to a minimum have forced many organizations to quickly shift their workforce from being on site to working remotely – from home. While there are many things to think about while transitioning a workforce to remote working conditions, **cyber security should be a large focus of your strategy**.

During times of crisis, cybersecurity threats often increase with hopes of taking advantage of organizations in transition.

Here are some common cyber threats to keep an eye out for:

1. Increased **phishing and scam emails** related to Covid-19
2. Increased **use of remote access** solutions
3. More **company devices in the homes** of individual employees
4. Impact to the **privacy of information** when working from home

So what can organizations do to protect information security and privacy? While there is no silver bullet, here are some controls to consider:

1. Establish a **Telework** Program that includes an Acceptable Use Policy so employees know their responsibilities in protecting company systems and information.
2. Enforce **Multi-Factor Authentication (MFA)** for *all* remote access to company resources (including emails, VPN, cloud storage, etc.).
3. If your workforce is located in the United States, enforce **Geo Blocking** to limit access to systems within the United States.
4. Provide specialized **Security Awareness** training (e.g.: how to detect phishing emails, how to securely configure teleconferencing tools, how to identify and report suspicious computer activities).
5. Protect **mobile devices** in case they are lost or stolen with access controls like a passcode and encryption (on laptops, phones, tablets).

6. Consider deploying **Endpoint Detection and Response** solutions to further secure devices such as servers, workstations, and laptops from evolving threats like Ransomware.
7. **Review remote access logs** and have a process in place to quickly identify and follow up on suspicious sign-in activities.
8. Keep all servers and devices **patched** and up to date.
9. Review your **backup strategy** to make sure that business documents are saved where they can be backed up.

Don't fear, you don’t have to do this by yourself. Our team can assist you during this challenging transition by reviewing the current controls in place to support your telework strategy, by making recommendations based on the specific threats that your organization is facing, and by helping you implementing the right measures to protect your organization from cyber criminals.

Read More →

Learn More About our Cyber Services →

Questions?

Gui Cozzi | Cybersecurity Practice Lead
gcozzi@ddaftech.com
859.425.7649

Forward to a Friend!

The matters discussed above provide general information only. The information is neither tax nor legal advice. You should consult with a qualified professional advisor about your specific situation before undertaking any action.

Make sure you are receiving the information you want. Click here to update your preferences!

Dean Dorton, 250 West Main Street, Suite 1400, Lexington, KY 40507, United States
Unsubscribe