RSI

(858) 240 9263 • www.rsisecurity.com • info@rsisecurity.com

# Work From Home Cybersecurity Checklist for Companies

☑ **Best practices to keep your remote workforce safe and secure during COVID-19.**

☐

## Conduct Training and Education

Ongoing training is critical to making sure employees take the proper cybersecurity precautions while working from home. You'll want to assess your team's experience with working from home and the typical security measures they take.

You can then formulate a work-from-home focused cybersecurity awareness training program. This typically covers topics like virtual private network (VPN) use, password security and home wifi settings.

☐

## Create Company Wide VPN

A VPN is typically more secure than home or public wifi networks that work from home employees tend to use. Setting up a VPN effectively creates a secure tunnel for sensitive data to pass through, eliminating vulnerabilities associated with everyday wifi networks.

A VPN guarantees secure remote access for your entire organization and provides an additional layer of safety when using tools like cloud storage or enterprise messaging.

☐

## Implement Email Encryption

Email is often the main communication channel for work from home employees and the rest of the company. The problem is, many standard email services and settings aren't configured with end-to-end email encryption.

Make sure all company email communications are encrypted with both public and private keys. With end-to-end encryption, emails are encrypted prior to being sent and can only be decoded with the right keys.

☐

## Employ Multifactor Authentication

Working from home means that you and your team are physically disconnected from your IT, cybersecurity and/or compliance teams. This makes it easier for employees to ignore guidelines for things like access controls and password strength.

Multifactor authentication (MFA) is the best sure-fire way to prevent unauthorized logins. Things like email verification, fingerprint scanning, biometric facial recognition combine to form a secure MFA strategy.

# Work From Home Cybersecurity Checklist for Companies

☑ **Best practices to keep your remote workforce safe and secure during COVID-19.**

□

## Carefully Monitor BYOD Devices

New work from home BYOD guidelines have recently been released by the EU as a response to COVID-19. The optimal scenario recommended is to avoid BYOD altogether, supplying employees company-owned laptops, tablets and smartphones. This lets businesses standardize - and improve - device security in a remote work environment.

If you do require, BYOD all devices should go through security vetting processes like patch and configuration checks.

□

## Maintain Your Compliance Posture

The unfortunate reality is that you may need to relax some security measures to meet the productivity and convenience needs of your workforce. But that doesn't necessarily mean that you won't be in compliance with PCI DSS, HIPAA or any other relevant cybersecurity framework.

Review all changes with your compliance department or cybersecurity partner thoroughly to maintain compliance through the pandemic.

## Need to Secure Your Remote Workforce

Contact RSI Security today to discuss work from home cybersecurity, technology and compliance.

**CYBER INSURANCE** Keep your business on a stable financial foundation should a cyber security event occur — get cyber damage and recovery insurance today.