WINSTON & STRAWN LLP

BLOG

# 5 Remote Work Strategies for Companies to Reduce Data Privacy & Cyberrisks

MARCH 31, 2020

Companies are taking the dramatic step of migrating employees to work from home in order to keep their employees and customers safe from the COVID-19 virus pandemic. An employee's home environment may not be set up securely and presents an attractive target for cyberattacks. Companies should work with employees to remain diligent in using cybersecurity best practices while working remotely.

1. **Tighten up Access to Company Data**. Companies should ensure that all connections to their information systems are made through a secure connection, such as a virtual private network (VPN) or virtual desktop. Not every employee has secure Wi-Fi, so require employees to use a VPN to reduce cyberattacks. Employers should limit employee access to only information they need to do their job. Companies should consider implementing two-factor authentication for accessing company networks and systems. That way, if an employee falls prey to a phishing email and the email is compromised, two-factor authentication would prevent the phisher from accessing other company information.
2. **Partner with Employees on Patching**. Companies should ensure that critical weekly software, anti-virus and malware updates are installed. Ensure that employee computers provided for home use are up to date. Communicate with employees to ensure that any home systems used to perform work or connect to company systems are equipped with up-to-date antivirus and malware protection. Companies may want to send weekly reminders to employees to be sure patches are kept up to date.
3. **Be mindful about complying with new data privacy laws**. Remind employees about their obligations in handling personal and proprietary data. Request that employees avoid transferring any sensitive information via email. Provide employees and vendor partners with a secure portal or FTP site to transfer any sensitive or proprietary information.
4. **Remind employees to be vigilant against fraudulent phishing emails**. Be aware of the heightened risk of phishing emails. Bad actors know that workers are teleworking, which could provide soft targets. In the midst of the fear the crisis produces, employees may be more susceptible to clicking on phishing emails about Covid-19. Employers can remind employees to be suspicious of any email that includes a link to click on for more information or that asks for account credentials or financial information. Companies can require that an employee must call to verify any requests for information or payment requests.

5. **Be prepared to respond to a data security incident**. Companies should anticipate cyberattacks, including reviewing the Security Incident Response plan and confirming cyberinsurance coverage. It's critical to proactively monitor for security incidents, including monitoring the network for spikes in activity, unusual credential activity, or foreign IP addresses. Provide employees with a telephone number to call about any suspicious data security incidents.

This pandemic may have a profound impact on work practices in the future, with working remotely a more commonly accepted practice. The data security steps companies take now to establish proper remote-work cyber-hygiene habits will greatly reduce successful cyberattacks in the future.

Winston's Global Privacy and Data Security Task Force is available to handle privacy and data security issues that arise during this challenge.

View all of our COVID-19 perspectives here. Contact a member of our COVID-19 Legal Task Force here.

2 Min Read

## Authors

Steven Grimes

Alessandra Swanson

Sean G. Wieber

Eric Shinabarger

## Related Locations

Chicago | Houston

## Related Topics

COVID-19 | Workplace Privacy | Data Breach

## Related Capabilities

Privacy & Data Security | Privacy: Regulated Personal Information (RPI) | Technology, Media & Telecommunications

## Related Regions

North America

# Related Professionals

Steven Grimes

Alessandra Swanson

Sean G. Wieber

Eric Shinabarger

*This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.*