An iBridge Point-of-View

# How to Protect Your Data As More Employees Are Working from Home

Six tips that will help protect your data now that remote working is here to stay.

Remote working became the new normal for countless businesses because of the COVID-19 pandemic. Many organizations are considering—or have already decided—to give employees the option to continue to work from home (WFH.)

Many of these organizations would have never considered allowing their workforce to be remote but have now discovered that there are many benefits to remote working. Some have seen employees report higher productivity and job satisfaction. Others have realized that they can potentially attract better talent while lowering overhead costs.

However, the WFH movement has reenergized cyberattacks and phishing schemes targeting those who work from home. Accordingly, organizations need to strengthen their cybersecurity measures to protect the safety and integrity of the data transferred among different networks and systems as employees access files and information from outside the office.

The impact of a cybersecurity attack or data breach can be financially and reputationally devastating. If your company is in healthcare or higher education or does business in California or Europe, the fines associated with HIPAA, FERPA, CCPA, and GDPR infractions can be crushing.

## Sixways you can protect your data and support your WFH employees:

### Use VPN for Remote Access

Employees should be accessing your network via a VPN connection to ensure endpoint security. Even if you're already using a VPN, it's time to reevaluate its effectiveness as vulnerabilities can emerge if you don't implement security patches in a timely manner. Also, make sure you have the processes in place to regularly update your VPN settings moving forward.

### Update Remote Working Policy

While many organizations have a remote working policy, some are outdated and no longer sufficient for today's digital business environment. If you haven't revised your remote working policy in the past year, now is the time to make the necessary updates and take the current work-from-home scenarios into account.

### Inform Your About Malware Cyberattacks

Despite your company's best efforts, your employees are still your weakest security link. Don't blame them. Educate them and keep them informed of recent attacks and phishing schemes. Many organizations deploy phishing and social engineering threat simulators designed to imitate a threat and build a healthy awareness of how easily these attacks can occur. After all, it only takes one employee to click on a malicious link to infect the entire network with malware!

### Enforce a Bring Your Own Device (BYOD) Policy

You can expect more employees to use their own devices (e.g., smartphones, tablets, and laptops) to access company data when they work from home. Make sure they're aware of the company's BYOD policy. Provide the support to help them check their devices for vulnerabilities and ensure they select the right security settings for maximum endpoint security.

### Use a Device Management Solution

As employees take company devices out of the office, you need to keep track of the inventory and update them on the latest software and firmware. Your IT team should be able to secure and control each device remotely so that it can delete sensitive data and prevent unauthorized users from accessing it in the event the device is lost or stolen.

## Audit the Data You're Storing

From GDPR and CCPA to HIPAA and PCI-DSS, there's an increasing number of regulations to which, organizations need to adhere.  You can reduce risk exposure by mapping your data and then collecting and storing the minimum amount of customer data you need to conduct business.

If you have been storing more information than necessary, take this opportunity to remove any excess information from your database.

## Make Data Security Part of Your Overall Business Strategy

The ability to collect and analyze data, as well as maintain its security and integrity, is a key component of any successful organization. The capacity to support remote workers and their associated need for data security should be part of your key performance indicators and metrics -- especially at this transitional time.

Here at iBridge, we offer expert information security management, including data mapping and cleaning, and preparing our clients with an ISO27001 assessment program.  We help clients conduct risk assessments, design mitigation strategies, develop and deploy security measures, monitor and review the effectiveness of their tactics, as well as maintain and improve their systems to stay current with the latest cybersecurity best practices.

Get in touch to see how we can help you improve data protection to support remote working now and in the future.

iBridge

## iBridge is a Digital Transformation Company.

We help our clients collect, manage, and analyze their data to create meaningful operational control and improved profitability.  For more than a decade, iBridge has successfully distilled complex information into actionable results.

**www.ibridgellc.com**