Cybersecurity during COVID-19 transition to remote work policies

By [Cody J. Cooper]()

Cody Cooper

Allowing employees access to information outside of a company's traditional network ultimately means that the company has had to store company information on a medium that is accessible through the Internet. Companies should revisit security policies to make certain that they have in place the appropriate measures to prevent unwanted third-parties from accessing this information or employees' inadvertent misuse of sensitive information.

Companies can take several steps to put themselves in the best position to allow employees to work remotely and while also putting themselves in the best place to continue to secure the company's sensitive data.

The easiest and most important steps a company can and should take are:

> **(1)** limit access to only employees that need it and only the data they need to perform their job;

(2) set security settings to require password logins (whether through a company device or personal device);

(3) where possible, turn on multi-factor authentication to ensure a high level of security over the most sensitive data;

(4) decrease the time before device lock out the user and require re-entry of their password.

For companies with the financial and technology capability, they can also deploy data loss prevention (DLP) products such as mobile device management systems or cloud access security broker to add extra layers of data protection. Companies can also run security tests, i.e. fake phishing attempts, during this time to test which employees are practicing safe data security practices and remind those that are not of their responsibilities. It is always good practice to regularly circulate a newsletter with security updates and reminders, and that practice should continue – or or even increase – while employees are working remotely.

Unfortunately, there may be layoffs of employees during this crisis. While employers hope to avoid this at all costs, it is also important to remember to have a plan in place to protect and recoup company devices and data in the even that remotely working employees are terminated. During that time, it is important to terminate access to company data and to recover any outstanding devices. Hopefully these measures will not be necessary, but it is important to have a plan in the event they do occur.

Companies and individuals are in a state of triage trying to address the most pressing needs as they arise. It is especially important at this time for everyone to remain vigilant about their cybersecurity and data security practices, to be proactive, and put plans in place to address potential developments.

Cody Cooper traditional work settings and moving employees out of the office and enabling them to work from home. With this comes the obvious preparation to allow employees access to company information outside of the company's network. But, it is incredibly important to recognize that this comes with an increased risk of data security issues.

For more information on this alert and its impact on your business, please call 405.552.2405 or **email me.**

Keep up with our ongoing COVID-19 resources, guidance and updates at our **RESOURCE CENTER**.

Follow our coverage on ***FACEBOOK***