Courtesy of
Marshall & Sterling Insurance

CYBERRISKS&LIABILITIES_

Coronavirus and Managing Remote Work Cyber Risks

Given the implications of the coronavirus (COVID-19) outbreak, countless employees across a variety of industries are working remotely. While this allows businesses to remain operational, it can create a number of risks, particularly for those who fail to take the proper precautions.

Above all, information security is one the greatest challenges for companies allowing remote work during the COVID-19 outbreak. When an employee is at the office, their work is protected by safety standards that keep your company's network and data secure. However, an employee working from home may not have the same safety measures in place to protect your organization's devices and information.

In order to safeguard your business and employees from data breaches, cyber scams and viruses, consider the following strategies:

- **Train employees on how to detect and respond to phishing attacks.** Criminals prey on unfortunate circumstances, seeking to capitalize on victims during times of panic and hardship. Unfortunately, the COVID-19 pandemic is no exception. Cyber criminals have been known to pose as charities and legitimate websites to lure victims into sending money and revealing personal information. Individuals should scrutinize any emails, texts and social media posts related to COVID-19 and be cautious when clicking any links and attachments. Specifically, employees should be instructed to:
    - Avoid clicking links from unsolicited emails, and be wary of email attachments.
    - Use trusted sources when looking for factual information on COVID-19, such as CDC.gov.
    - Never give out personal or financial information via email, even if the sender seems legitimate.
    - Never respond to emails soliciting personal or financial information.
    - Verify a charity's authenticity before making any donations.
- Have a virtual private network (VPN) in place, and ensure employees are using it to access company systems and data when working remotely. VPNs encrypt internet traffic, which can be particularly useful when your employees are connected to a home or public network. Furthermore, it could be beneficial for your company to prohibit employees from accessing company information from public networks altogether.
- Mandate the use of security and anti-virus software. This software should be up to date and include the latest patches.
- Educate your employees on the kinds of sensitive data they are obligated to protect. This could include confidential business information, trade secrets, intellectual property and personal information. When working with sensitive data, employees should take to the same precautions

Marshall & Sterling INSURANCE

This Cyber Risks & Liabilities document is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel or an insurance professional for appropriate advice. © 2020 Zywave, Inc. All rights reserved.

they would if they were at the office. They should avoid using their personal email for company business and think critically about the documents they are printing at home. If they must print sensitive information, they should shred the document when it is no longer needed. Encrypting sensitive information can also help you protect any data that is stored or sent to remote devices.

- Prohibit employees from sharing their work devices with friends and family members. Doing so reduces risks associated with unauthorized or inadvertent access of company information.
- Have employees update their contact information. That way, if your systems are compromised, you can easily contact your staff and provide the appropriate updates and instructions.
- Create and communicate a system that employees can use to report lost or stolen equipment. This will help your IT department respond quickly and mitigate potential data loss threats.
- Require two-factor authentication for all company passwords. Two-factor authentication adds a layer of security that allows companies to protect against compromised credentials. Through this method, users must confirm their identity by providing extra information (e.g., a phone number or unique security code) when attempting to access corporate applications, networks and servers. This additional login hurdle means that would-be cyber criminals won't easily unlock an account, even if they have the password in hand.
- Consider security precautions for mobile devices. Proper phone security is just as important as a well-protected computer network. A smartphone could grant access to any number of applications, emails and stored passwords. Depending on how your organization uses such devices, unauthorized access to the information on a smartphone or tablet could be just as damaging as a data breach involving more traditional computer systems.

For additional protection, employers should consider backing up data and bolstering network protections as best as they can. For more cyber security guidance, contact Marshall & Sterling Insurance today.

.