NEXSEN | PRUET

The Rush to Remote Work Has Caused Some Organizations to Ponder - Just How Safe is Their Data?

Related Professionals

Bryan L. Baysinger*
864.282.1117
bbaysinger@nexsenpruet.com

Practices

Privacy & Data Security

Article
04.28.2021

The COVID-19 pandemic has changed how and where employees are able to work, and some employers are allowing their employees to continue to work from home despite restrictions lifting. While many revel in this new approach, it does cause concerns for privacy and data security. Data breaches have been on the rise in part due to the rushed response to COVID-19, as employers were unable to properly train and equip their employees prior to mandated shutdowns. Data breaches can cause severe reputational harm, and more and more states have passed, or are actively contemplating, legislation that would impose fines and other consequences should a breach occur.

Companies should evaluate their internal procedures and off-site policies in order to mitigate the chance of a breach, or severe fallout should one occur. Read on to learn what to look for as your company conducts these reviews.

1. Reiterate and enforce confidentiality measures. Employees should be directed to properly secure company property, and the policy should dictate the steps that should be taken should such property be misplaced or stolen. Employees should also use secure remote access procedures like a VPN, avoid downloading confidential information onto personal devices, practice password safety, complete anti-virus updates and computer backups, and maintain confidential information in a secure location at the remote location, among other considerations.
2. Develop and integrate Bring-Your-Own-Device (BYOD) policy. Employees may be tempted to use personal devices for work instead of more secure, company-authorized devices. Companies often use mobile device management (MDM) software to maintain control in such a situation, but companies can consider allowing the use of approved devices only. Companies should outline their rights with respect to the content of the devices, the procedures should a breach occur, and the repercussions should an employee's misuse of a device causes a

breach.

3. Implement a robust electronic communications systems policy. Such a policy should echo the BYOD policy in that remote employees should have no expectation of privacy when using employer-owned devices and systems. The policy should also warn that the company might monitor emails, internet use and activity, device use and activity, any internal chat functions, and location. Companies should consider blocking access to certain websites, including personal email and social media accounts, that often are the source of phishing, ransomware, and email fraud.
4. Review vendors and service providers. Vendors and contractors can pose a substantial risk to a company's security, as they often interact or process sensitive company data. Third parties should be properly vetted and periodic contract review and audits should occur. Additionally, now is a good time to review old contracts, and adjust the language to the changing climate of remote work. In many cases, agreements prior to COVID-19 may not have accounted for the changing dynamic of remote work and offsite meetings.
5. Develop a response plan. The company should also consider its plan should the unfortunate were to occur and a breach happens. The policy should clearly outline the various employee and departmental duties, including information regarding reporting methods both internally and externally. The company should understand its obligations under relevant state law and any contractual obligations it has should a breach occur, including notifying insurance carriers.

Companies should consider providing additional training for their employees about the company's data security policies. While a revamped data security policy will go a long way to reduce the chance for a data breach, employees need specific guidance as to how these policies and procedures will be implemented in light of their specific roles or departments. Companies should also take the time to explain the reasons for the policies; for example, explain that penalties for violating data privacy laws can be costly and can include damages (including treble damages) and attorney's fees, along with reputational harm. Finally, companies need to be aware of any laws that may apply to their collection and use of the information it maintains in pursuit of a strong security policy. By maintaining a proactive approach to privacy and data security, organizations can rely less on reactive measures.

Should your company need help to develop any of these policies, or should it need a review of existing policies and procedures, please reach out to a member of our Privacy and Cybersecurity team.