Featured Professionals

Nadja Baer

Sten-Erik Hoidal, CIPP

Related Services

Data Protection & Cybersecurity

Employment, Labor & Benefits

Technology & Data

Question of the Day: Data Security for a Remote Workforce

Legal Update
05.20.2020

By Sten-Erik Hoidal and Nadja Baer

Question

What should companies do to mitigate the security risks of a remote workforce?

Answer

With millions of Americans under active stay-at-home orders, companies that have never had a remote workforce are playing catch-up in terms of system and data security. Bad actors have taken notice — phishing and other cyberattacks have increased significantly, and the Department of Homeland Security has issued an alert recommending that organizations with a remote workforce "adopt a heightened state of cybersecurity."

As a result, companies need to take action to mitigate the potential risks presented by their remote workforce. Below are some recommended steps.

1. Warn employees about, and train them on, the risks presented by working remotely.

Privacy and security training is not simply a one-and-done event to check off during new employee orientation. A thoughtful training program requires regular participation and engages employees as new threats emerge. Employees that are made aware of such threats are in a better position to identify them and respond appropriately if perpetrated against their employer.

With a remote workforce, some of the most prevalent threats are phishing and similar social engineering schemes that are intended to get the employees to volunteer their email credentials or other information that would permit access to companies' email or computer systems. It is imperative to communicate with employees about the risks of social engineering schemes and train them on how to recognize and address those threats.

Companies should consider instructing employees to:

- Remain hypervigilant about potential phishing and cybersecurity threats;
- Refrain from providing email or computer credentials in response to requests that come by email or phone unless they are absolutely certain, and have verified the legitimacy, of the source;
- Use **extreme caution** in reviewing emails that ask the recipient to click a link or download a document, and refrain from clicking links or downloading documents contained in emails that were not expected or come from unknown senders;
- Contact the company's IT department, help desk or other designated resource immediately regarding any suspected phishing attempt or cybersecurity incident; and
- Use a unique password for their work email account that is completely different from the passwords that the employee uses for other purposes, including personal purposes.

2. Update information security policies and communicate updates to employees.

Information security policies help provide direction to employees regarding secure and appropriate use of company systems and technology assets. For example, many companies have acceptable use policies that specify what employees can and cannot do with their technology assets. Companies should review these policies and update them as necessary to account for their current remote work environment. Once updated, the policies should be communicated to the employees so they understand exactly what is expected of them as remote employees.

3. Implement multi-factor authentication (MFA) for remote access.

Adding multi-factor authentication can prevent unauthorized intrusion to company systems where employee access credentials are lost or stolen. MFA can be managed via hardware- or software-based tokens. Additionally, companies should consider having employees enable MFA controls when employees must use personal or commercially available accounts for work purposes.

4. Monitor internal and external security controls.

Identify points of weakness in internal and external information systems used by a remote workforce. Where monitoring capabilities for external systems are limited, evaluate whether the company has sufficient contractual remedies.

Internal

To decrease risks associated with intrusion into company systems, perform continuous network monitoring and encrypt critical communications between mobile devices and the company's servers. Companies should take preventive measures to secure devices through multi-factor authentication, secure remote access methods and other device management applications, physical locks for unattended laptops, strong password management practices and short timeframes for locking devices due to inactivity.

External

Review contracts for any cloud service providers and other outsourced security or IT managed services. In addition to the service provider's own established security processes, those that handle confidential and potentially sensitive information should be able to provide a third-party certification of their internal security controls. Make sure that the level of security identified in those reports is appropriate for the company's business, and establish contracting practices that allow the company to audit and enforce vendor compliance. Further, if a remote workforce has caused the company to start using publicly-available file transfer and sharing services, the company should evaluate what type of security controls (including MFA as described above) are available to limit access to files posted and shared via these resources.

5. Prepare for an incident.

Swift action is critical in complying with reporting obligations in the event of a confirmed security incident. A comprehensive Incident Response Plan (IRP) should lay out how the company will assess and react to potential and confirmed incidents, as well as identify the incident response team members and the external resources that may be called upon in responding to an incident. An established IRP should be tested periodically with various breach simulations to identify any gaps in the plan. In addition, companies should review whether they have appropriate coverage to mitigate the costs of, and losses from, potential cybersecurity events. Companies that do not have a cyberliability policy should consider investing in one.

If you have questions or need assistance, contact your Fredrikson & Byron Data Protection and Cybersecurity attorney.

View All: COVID-19 Employment Question of the Day