Proskauer

Protecting against Cybersecurity Threats when Working from Home

New Media and Technology Blog on **March 11, 2020**

With the spread of the novel coronavirus (COVID-19), many organizations are requiring or permitting employees to work remotely. This post is intended to remind employers and employees that in the haste to implement widespread work-from-home strategies, data security concerns cannot be forgotten.

Employers and employees alike should remain vigilant of increased cybersecurity threats, some of which specifically target remote access strategies. Unfortunately, as noted in a prior blog post, cybercriminals will not be curtailing their efforts to access valuable data during the outbreak, and in fact, will likely take advantage of some of the confusion and communication issues that might arise under the circumstances to perpetrate their schemes.

Employees working from home may be accessing or transmitting company trade secrets as well as personal information of individuals. Inappropriate exposure of either type of data can lead to significant adverse consequences for a company. Exposure of trade secrets or confidential business information can potentially cause significant business damage or loss. Exposure of personal information can potentially trigger state or federal data breach notification laws, and result in significant liabilities for a company as well as expanded identity theft issues for individuals. The threat is not only an online concern – physical security is at issue as well. Unauthorized access to printed copies of sensitive documents could lead to additional exposures.

Increased Risk with Personal Devices

Employees working from home may take shortcuts, such as downloading or saving sensitive company materials to their personal devices, desktops, thumb drives, hard drives and file hosting services in the cloud (e.g., Dropbox). Employers should remind their workforce that saving company materials to personal devices that have not been appropriately configured with security systems (e.g., company-sanctioned level of anti-virus software, password protection technologies, or secure network connections) increases the risk of exposure to cybercriminals. Moreover, personal devices may be more susceptible to "physical breaches," as employees may leave laptops or devices unguarded in places without the physical security of an office setting, such as in their car or at a coffee shop. If an employee is working in a public place, such as a coffee shop, third-parties with a view of the employee's computer screen or printed documents also poses a security risk to trade secrets or personal information.

To guard against these threats, employers should consider:

- Requiring all employee devices to be equipped with the employer-provided security software and the latest manufacturer software updates prior to permitting access to any remote systems;
- Requiring multifactor authentication upon each login to a company portal;
- Only allowing remote access through a virtual private network (VPN) with strong end-to-end encryption;
- Prohibiting working from public places, such as coffee shops or on public transportation, where third parties can view screens and printed documents;
- Prohibiting use of public WiFi, and requiring the use of secure, password-protected home WiFi or hotspots.
- Imposing additional credentialing with respect to the ability to download certain sensitive data.

Naturally, given the urgency behind the "work from home" transition, it may not be practical to implement all of these steps immediately.

Coronavirus-related Phishing Attempts

In an effort to keep employees informed about company policies regarding the coronavirus, many employers are creating new email accounts which send out daily email updates. These emails often contain several links to forms or information about company policies. Given the sensitivity of such emails, employees may be quick to open these emails or to click the links, even from previously unknown company email addresses. Employers should recognize that phishing emails disguised as coronavirus updates or as updated company policies may deceive employees. For example, the World Health Organization (WHO) specifically warned that, in connection with COVID-19, cyber criminals are sending phishing emails with malicious links and are impersonating WHO officials to steal money and sensitive information.

Many companies already include warning banners on emails that originate outside of the company, but ensuring that such banners continue to attach to email addresses outside the company will help employees parse out which coronavirus updates are legitimate. An additional solution is to create a coronavirus portal on the company website that employees can access for live company policy updates when they are not confident that an email communication from the company is legitimate.

Off-Network Communications

With more employees working from home, groups and teams will become increasingly reliant on phone, email, and instant messaging communication systems instead of in-person meetings. Companies should ensure that their email and messaging systems remain encrypted and secured. Additionally, some employees may be tempted to communicate outside of normal company communication systems, such as text messaging on personal devices or private chatting on social media. Communicating on platforms outside of the enterprise-wide security systems poses a far greater security risk than communications on company platforms. Employers should remind employees of these risks and should encourage employees to use good judgment about when, where, and how they discuss work-related matters.

Incident Response

While employers are working hard to protect the health and safety of their employees, incident response requirements remain in effect. Employees should be reminded that if they become aware of a possible data security breach while out of the office, they should inform the organization's designated recipient for such notifications. Moreover, each company's data breach response team should be reminded that due to the possibility of increased risk during this period of time, their attention and resources may be called upon.

* * *

Although employers may be wary of sending out additional communications on top of daily coronavirus updates, it is critical to remind employees of these security risks. Even though employees may feel more comfortable working from home, they should maintain good cyber hygiene practices and not get too comfortable at such a critical time.

Every company is dealing with significant human resource, health and business issues associated with the coronavirus. With a little extra care on security at this strenuous time, hopefully companies can avoid having to deal with additional issues associated with data breaches or loss of valuable business information.

Proskauer's cross-disciplinary, cross-jurisdictional Coronavirus Response Team is focused on supporting and addressing client concerns. Visit our Coronavirus Resource Center for guidance on risk management measures, practical steps businesses can take and resources to help manage ongoing operations.

View Original

Related Professionals

- **Jeffrey D. Neuburger**