BUSINESS FOCUS:

Preventing remote workers from creating cybersecurity risks

By Cameron G. Shilling of McLane Middleton, Professional Association

Cameron Shilling

Many businesses transitioned to remote workforces to combat the coronavirus. For businesses that already support remote work, that transition occurred fluidly. For businesses that did not, the cybersecurity risks are more frightening. Those companies need to have implemented appropriate safeguards. So what should businesses do to prevent remote workers from creating cybersecurity risks? The following are ten of the most important.

1. Protocols

Businesses that have protocols for remote working should reinforce them with employees. Businesses that do not should create temporary protocols.

2. Laptops

Businesses should permit employees' access to networks using only company computers, with encrypted hard drives, up-to-date anti-virus/anti-malware, strong passphrases/passwords, and locks after 15 minutes of inactivity. Employees should not have administrator privileges. Employees should be instructed to shut down when not in use, and that family members may not use company computers.

3. Virtual Private Network (VPN)

Access to the network should be only through a secure company VPN, which has multi-factor authentication, prevents downloading to a local drive, prevents access to local printers and internet-of-things devices, and is configured with robust logging. Employees should not be allowed to use the VPN on a personal computer.

4. Mobile devices

Businesses should permit employees to access company email only using a mobile device that has a password or biometric. More effective controls exist with a mobile device management application.

5. Email

Remote access to company email and cloud storage should be allowed only using a company computer or mobile device discussed above, with a strong password and multifactor authentication. Outlook Web Access should be disabled.

6. Wi-Fi

Home and public Wi-Fi are vulnerable. Employees should be prohibited from using insecure public networks. Businesses should ensure that executives' home networks have a company monitored firewall, and other employees use a VPN described in #3.

7. External drives

Businesses should prohibit employees from using external or USB drives, unless encrypted and company owned. Disabling USB ports or installing an application that encrypts drives are effective protections.

8. Attacks and crime

Hackers are capitalizing on this crisis. Businesses should have safeguards against phishing and social engineering, like headers alerting employees to emails from outside the organization, a button permitting employees to forward suspicious email to IT, and a 'sandbox' that executes links and attachments in a safe environment. Businesses also should require employees to confirm the authenticity of every monetary transaction via a secondary authorization (like voice confirmation).

9. Privacy

Privacy laws are in effect during this crisis, including laws protecting health and personal information (like HIPAA, GDPR and CCPA). Businesses cannot disclose health or personal information about a person who is or may be affected by the coronavirus without complying with statutory requirements.

10. Prohibited activities

Businesses should remind employees that certain activities are prohibited, including handling company information using a personal email account, personal cloud (like Dropbox or iCloud), or personal computer.

While this crisis can tempt businesses to facilitate remote work without effective cybersecurity, the crisis will become far worse for a business that also experiences a breach. Implementing the above safeguards does not have to be prohibitively costly or time-consuming and will establish a foundation for appropriate cybersecurity after the crises. Businesses should take time to ensure that their remote workforces are cybersecure.

Cameron founded and chairs McLane Middleton, Information Privacy and Security Group. The group assists businesses and private clients to improve their information privacy and security compliance, and address any security incident or breach that arises. You can reach Cam at (603) 628-1351 or cameron.shilling@mclane.com.

MCLANE MIDDLETON

11 South Main Street, Suite 500
Concord, NH 03301
www.mclane.com