EST 1989 nyrej

Cyber security considerations for businesses with employees working remotely - by Joseph Saracino

April 07, 2020 - Long Island

Even prior to the current COVID-19 pandemic, the number of businesses using remote workers was steadily growing. Working remotely does offer some advantages, but a remote workforce also introduces new cyber threats to an organization’s information technology (IT) systems and proprietary data. Businesses now operating with remote workers should be vigilant and proactive in implementing effective cyber security measures.

Zero Trust

In today’s climate of data security, growing government compliance reforms and mandates, it is imperative that “Zero Trust” policies be implemented as part of the corporate governance protecting internal and external data activity. Now that circumstances have forced thousands of employees to work from home, zero trust policies are more important than ever. Data breaches are taking a toll on businesses and consumers at an alarming rate. This trend has forced us all to look at how we handle data in a new way. While for some, working from home is not new, for many, it will take time to acclimate. Therefore, we can’t take it for granted that everyone will have the same intensity regarding data protection consistent with best practices. We are a society that freely gives up our data through social media placing us in a much more compromised position than we have ever imagined. Employees must be reminded that working from home is an extension of their corporate environment.

Risk Mitigation

Working remotely has its pros and cons. On the plus side, productivity, communications and interaction can be maintained using technology. On the negative side, some workers have difficulty managing their time between work and home responsibilities. Specifically relating to cyber threats, their home technology may not be equipped with the latest system updates, anti-virus and encryption software. They may not routinely change their router user IDs and passwords. Remote workers must be instructed to implement these and other best practices to protect company data, and also advise others including family members who may also have access to the same device. It is often said that the weakest link in a security chain is the end user.

For the most part, many devices may be used to perform various tasks. That is okay as long as the devices have current updates and security software, and can support the corporate application(s) needed for an employee’s assigned tasks. It is important that remote workers be advised to review their company’s policies for guidelines on different devices and related cyber security requirements. Be vigilant regarding these potential risks:

It is inherently more challenging to take a proactive cyber security posture when working in a more relaxed home environment.

97% of malware today targets the end user. Hackers set up emails that look so real and users, whose guard is down, may be more prone to click on them at home, than at work.

Cyber security awareness training on best practices should be provided to all staff. Implementing mock phishing campaigns as part of this training should be conducted to keep everyone’s skill set at the highest level. For businesses relying on cloud computing, the risks can be even greater. When data is distributed over a larger number of devices (i.e., multiple data storage units in different locations), the security of that data must be amplified.

Cyber Security Guidelines

Businesses of all sizes should have policies in place and expect all employees to follow them. The National Institute of Standards and Technology (NIST) has guidelines for best practices. They should be followed, but also customized to accommodate each organization’s operations.

Here are some other practical guidelines:

Have the latest anti-virus software updated on your operating system.

Even if you are automatically downloading the latest updates, it is prudent to manually perform the updates periodically.

If using a Virtual Private Network (VPN), install key encryption software on your system to protect you from keyloggers that may be on your system. Note: Keyloggers are stealing data at the keystroke before it gets to the VPN. Don’t be fooled even if you have a VPN, that your data is encrypted at the key stroke. It is not.

When it comes to a cyber attack, it is not a matter of if, but when. We are all now part of the cyber battlefield. There are three stages of cyber security to consider:

Pre-Breach: Be proactive and take cyber security measures.

Breach: Know what to do and have written policy to follow during an event.

Post-Breach: Have a response team ready including a cyber team and legal team.

Keep in mind that an ounce of prevention is worth a pound of cure.

Joseph Saracino is the president and CEO of Cino Ltd. Companies, Coram, N.Y.