Guidepost

CREATING A SECURE "WORK FROM HOME" CYBERSECURITY ENVIRONMENT FOR EMPLOYEES & EMPLOYERS

The COVID-19 pandemic and resultant shelter-in-place enforcements have led to widespread adoption of remote work environments. Recently, Twitter CEO Jack Dorsey announced that some employees can work from home "forever." As we adjust to this new reality, there is an immediate need to consider how the work-from-home employee maintains a safe and secure cybersecurity environment.

In the weeks since many states issued stay-at-home orders, we have seen a tremendous increase in the number of phishing attacks. The phishers impersonate a person by adopting a role that appears familiar to their targets (e.g., a trusted colleague of their organization, such as someone from human resources, IT or senior management) and send emails to trick them into sharing personally identifiable information (PII); or worse, try to enter corporate networks via unsecured home network entry gateways. We have seen hackers utilizing both simple and sophisticated methods to attack both PII and corporate business networks.

The work-from-home environment has placed an increased focus on maintaining productivity and collaboration. Many businesses were equipped to immediately transition to the working-from-home environment; however, many others were unprepared to address the unforeseen increase in cybersecurity vulnerabilities associated with a home office environment. As we all move forward with a new normal, the corporate network and individual exposure to cyber security issues and increase in hacker methods place a new emphasis on corporate IT responsibilities and risk management.

Below are some tips that will protect your employees and help your organization maintain a safe cyber environment and reduce potential risk to organizational intellectual and confidential property:

Stop, Think, Connect – Train your employees to utilize the **STOP, THINK** and **CONNECT** approach if an email looks

suspicious. They should not open **(STOP)** any attachments or respond to an email with any personal information. Confirm **(THINK)** that the email has a valid sender, URL, and timestamp. Then, **CONNECT** and approach any attachment and links with caution. If they are uncertain, they should contact your IT security department or manager for further investigation.

Protect Home Networks – Encourage employees to change the default password on their routers and Service Set Identifiers (SSIDs) and encrypt traffic using WPA2-AES or WPA3-SAE. They should also add a firewall appliance to their home network setup for another layer of security.

Encryption – Ensure your employees have access to a VPN secure data connection between their computers and your organization's servers/databases.

Authentication – Implement multi-factor authentications for employees to associate with their log-in credentials, such as a code to their smartphone.

Segment WIFIs – Help employees create a hidden wireless network name SSID for their work laptops separate from their home networks. Family and friends should not be connecting to their work SSID.

Public Spaces – Discourage employees from connecting to public WiFis; instead, encourage them to use personal hotspots whenever possible. Their laptops should be locked when they need to step away for a minute.

Secure – Create policies for employees to keep their work data on their work secured environments (i.e., computers, clouds, etc.) and to avoid using personal devices for any work-related activities. These policies should not allow employees to connect external hard or thumb drives that are shared with family/friends to their work laptops.

Update – Remind employees to ensure their operating systems, antivirus, IOT devices firmware/software, and other security appliances/software are updated to the latest versions.

For many businesses, working from home may become a permanent setup, at least for the foreseeable future. To ensure the continuous network and data security of your employees' working environments, ensure they have easy access to your IT department regarding the latest security updates and recommendations, and have the ability to attend security awareness trainings on a yearly basis.

Returning to the Office

As shelter-in-place requirements lift across the states, companies are turning their attention to creating a safe and comfortable work environment. Critical return-to-work considerations include:

- Return-to-office procedures and cybersecurity scanning policies
- Touchless technology solutions
- Integrated visitor management systems
- Occupancy control per space

- Social distancing analytics
- Remote intelligence
- Protection measures for public-facing interacting points
- Cloud solutions
- Cybersecurity penetration test and vulnerability assessment
- Security and safety policies
- Screening policies
- Business continuity and risk analysis

Remote workers present new security threats. Understanding these vulnerabilities and keeping pace with the risks can easily be overlooked as companies begin focusing on reopening their businesses. If you are not sure where to start, consider the help of a qualified consultant for direction and strategic guidance with technology solutions, operational policy and procedure, and staff training.

AHMAD ZOUA PMP

Director, Cybersecurity + Infrastructure

Ahmad's proven experience as an engineer and project manager allows him to handle a broad range of projects from inception to completion. While overseeing projects from designing and planning to commissioning and testing, Ahmad fosters an environment of teamwork and ensures that strategy is clearly defined and clients' expectations are met. His expertise with data center preparation, design and construction are invaluable for clients as they take the necessary steps to ensure continued operations in the wake of heightened concerns. This includes security and telecommunication systems design, cybersecurity, quality control reviews, and data network migration and integration.