BSSI
Business System Solutions, Inc.

Call the work what you will: Remote | Virtual | Telecommuting | Telework

The transition to mandatory telework due to the coronavirus is defining our new norm.

Many leaders had to dive in with little preparation to keep their organizations moving forward and afloat. As we begin to stabilize our remote workforce, we must revisit best practices in protecting our organizations. Personal technology and computing practices within an employee's home typically are not as sound as inside of the company walls. This coupled with cybercriminals adjusting their lures with coronavirus bait to "phish" in people centric (vs company) waters, suggests we need to review how we manage telework teams.

Here is a list of items you should be considering.

Employer checklist

These are items we recommend implementing at a company-wide level and managing by system group policies when possible.

1. Practice good cybersecurity hygiene with your team.
   a. Employee cybersecurity training. (95% of successful attacks can be attributed to human error. ~cybint)
   b. Safety tips
   c. Phish testing

   Currently, these practices are THE best thing a company can pursue, especially those who have recently transitioned to a remote work platform due to COVID-19.

2. Set auto screen locks on company devices to be enabled after five minutes.

3. Make passwords strong and change them frequently.
   a. Require three of the four below for password complexity:
      i. Uppercase Character – A,B,C
      ii. Lowercase Character – a,b,c
      iii. Number – 1,2,3
      iv. Special character - !,@,#
   b. Lengthen passwords – at least 12 characters
   c. Change them every 30 to 90 days
   d. Enable lockout after five failed login attempts
   e. Discourage password re-use
      i. Do not allow the same password or a previously used password to be used when a user is prompted for a password change.
      ii. Discourage the same password being used for any other account such as social media, banking, etc.
   f. Use passphrases and avoid associating passwords with the user, such as spouse/child/pet's name, wedding anniversary or birthdays.

4. Protect Your Email
   - a. Enable a spam filter
   - b. Use email encryption
   - c. Archive email (e-compliant)

5. Manage Physical Devices
   - a. A basic rule of thumb is always for employees to keep laptops and devices in sight – no leaving them in hotel rooms, on public tables while running to the restroom or checked luggage
   - b. Encrypt the hard drive on company devices, especially those devices leaving the physical office.
   - c. Disable access to the BIOS
   - d. Disable USB ports or utilize media encryption

6. Create and implement Data Backup and Disaster Recovery programs
   - a. On company networks
     - i. It is ideal for all company data to be saved in one central location for backup.
     - ii. Backups should also be stored offsite (systematically) to protect the data from localized events such as fires and malware.
     - iii. There are several backup and offsite solutions available to fit the specific needs of an organization based on their mobility, applications, and budget.
   - b. On desktops (if business data is being saved locally and not on a company network)
     - i. Locally saved data should be backed up to an encrypted external medium.
     - ii. Encrypted thumb and hard drives prevent access to the backed-up data.
     - iii. Cloud based backups are available and will protect from localized events such as fires and malware.
   - c. Most cloud-based applications, such as office 365, have innate backups for simple file recovery based on defined retention periods. The disaster recovery systems in place are designed with the provider's needs in mind and not their end-clients. There are many supplemental backup programs for data being utilized and saved in the cloud.
   - d. There are several backup, offsite, and cloud-based solutions available to fit specific needs of an organization based on their mobility, applications, and budget. If you have any questions, feel free to contact us at 740.475.1700.

7. Set-up Mobile Device Management (MDM) Software for Personal and Company Owned Devices
   - a. MDM software provides more security for personal and company-owned devices as it gives the company control in requiring complex passcodes, remote wiping of the devices, and controlling the applications that can be used.
   - b. MDM software is dependent on the mobile devices being managed (Apple, Android, Windows, etc.). Some software is device/operating system specific while others will support multiple platforms.

8. Provide secure remote connectivity tools to access the company network (e.g. VPN)

9. Control Access Levels
    a. Establish access needs by Category/Department based on job functionality. Employees should only have access to the areas they need to perform their job.
    b. Each user login or user-ID should tie to only one user. Shared or group user-IDs should not be permitted unless approved by management as part of standard operating procedures.
    c. The centralized users directory (Active Directory) should be updated on a consistent basis. For example, employees who have left the company should be removed.

10. All devices should have up-to-date software.

11. All devices should have up-to-date antivirus.

12. Mandate that only Admins are allowed to install software on the computers.
    a. Admins should also have a secondary account that is different from their normal user account to ensure it does not become compromised by day-to-day activities.

13. Users should not have pirate applications, music, or videos on their computers.

14. Set up Multi-factor Authentication (MFA)
    a. MFA is a security process in which users provide two different pieces of identification consisting of something you know (your password) plus something you have (a fingerprint or a generated code) to verify themselves before gaining access.
    b. The "something you have" component, typically comes from a third-party service. This service will send a unique, one-time code to a separate device owned by the user such as their cell phone.
    c. Some applications and services have built-in MFA, if so, ensure it is enabled.
    d. If not, there are several MFA solutions available to fit specific needs of an organization based on their mobility, applications, and budget. If you have questions, please contact us at 740.475.1700.

15. Provide consistent feedback and support for teleworkers.
    a. Provide initial and then regular feedback to staff on how to react in case of problems. That means providing information on who to call, hours of service, and emergency procedures.
    b. Give suitable priority to the support of remote access solutions. Employers should provide at least login and secure session capabilities (e.g. VPN and/or other secure connectivity tools).
    c. Provide virtual solutions. For example, the use of electronic signatures and virtual approval workflows to ensure continuous functionality.

   d. Ensure adequate support in case of problems.
   e. Define a clear procedure to follow in case of a security incident. (Incident response plan)

16. Cyberliability Insurance
   a. Cyberattacks can be very costly for companies. Cyberliability Insurance covers financial losses that result from security breaches. Cybersecurity Insurance is available through BSSI for its clients.

17. Polices
   a. Remote Work Policies
      1. If the company owns the device, the company should be ensuring the device is properly protected with up-to-date antivirus, device encryption, and firewalls.
      2. Cybersecurity policies should designate which devices (organization-owned v. employee owned) can be used for which kinds of business activity and outlines how and when the company provided tools should be used.
      3. Organizations should prohibit remote workers from using public WiFi and shared computers for work-related activities.

   b. Bring-your-own-device (BYOD) Policies
      i. BYOD policies are set by companies to allow employees to use their personal smartphones, laptops, and tablets for work.
      ii. BYOD can lower expenses for companies, however it also opens up security risks. A well-crafted BYOD policy will mitigate most of the security threats.

   c. Industry Legislation
      i. When crafting your technology policies make sure you are also compliant with your business's industry legislation – e.g. HIPAA, SOX, GLBA. BSSI provides access to its clients a turnkey HIPAA compliancy program which includes sample HIPPA compliant policies.

   d. Wire Transfers
      i. No one should ever transfer money based on a text or email communication.

How can remote workers minimize security vulnerabilities?

An employer's biggest concern is having remote workers introduce new vulnerabilities to the company network. Melding home networks and personal equipment with the work environment is a complicated situation. Between weak company password policies, poorly secured home WiFi routers, and device sharing with family members there are numerous areas for hackers to penetrate a company's network. Many businesses have a VPN setup to minimize risks, however there are still loopholes a hacker will find. The more security layers we can introduce into remote working environments, the safer everyone becomes.

The below points should be taken into consideration when reviewing a company's security posture.

1. Ensure employee's Wi-Fi connection is secure.
   a. If a Wi-Fi is not secure, people (neighbors) in the vicinity can snoop the traffic. If an employee goes to a web browser outside of the VPN connection to log into an email system, a hacker can see the passwords being typed in if the Wi-Fi is not secure.
   b. NOTE: Password or not, secure or not, public WiFi (hotel, coffee shop, hopping onto a neighbors Wifi) is not a secure method of accessing the Internet.
   c. Use only WAP2 Protocol when setting up a home network.
   d. Always use a strong password for the home network – making sure it is not still the manufacturer's default password.

2. All devices should have up-to-date software.

3. All devices should have up-to-date antivirus.

4. Employees should not be allowed to download company files locally onto a personal device.
   a. More than likely the updated file will not be returned to the company network which introduces a number of privacy, compliancy, security, and backup concerns.
   b. There are tools that can be installed on an employee's personal device to prevent and report such activity. For example, a notification can be created if someone is downloading company information ranging from a document to a patient database to a prospect database. The ability to install such a tool depends upon the BYOD policy.

5. Device Protection.
   a. Lock the screen and don't allow family members to use that device.
   b. A polarized privacy shield may be added to mobile devices to prevent the viewing of data unless directly in front of the screen.
   c. Devices should not be left unattended.
   d. Hard drives should be encrypted.
   e. Passwords/pass codes should be required on all personal devices being used for business including cellphones, tablets, etc.

6. All business-related activities should be routed through the VPN versus, for example, logging into the business bank by opening a browser on a personal device and logging into the bank directly. (Employers, depending upon the company bandwidth, may have previously decided to not force all that traffic through the company network. However, this allows another access point for hackers to enter the company network and should be revisited.)

7. Require employees shred confidential information printed locally.

As always, should you need assistance or have any questions, BSSI is here to help. You can contact us at 740.475.1700.

Resources:

Sample Policies by the SANS Institute

National Institute of Standards and Technology

Cybint