FOCAL POINT
DATA RISK

REMOTE WORKFORCE SECURITY CHECKLIST

In the rush to move employees remote in response to Covid-19, many IT leaders have scrambled to launch widespread remote access programs in a matter of days, potentially exposing their organizations to new risks. This is Focal Point's essential checklist for securing your remote workforce.

MULTI-FACTOR AUTHENTICATION (MFA)

As the number of users relying on remote access solutions has increased and attacks against them in response to the global pandemic have spiked, it is increasingly important to use multi-factor authentication (MFA).

- [ ] Enable and enforce MFA for remote access and hosted services (e.g., Office 365). MFA has become even more critical as phishing and other attacks have increased.
- [ ] Where practical, require IT to register MFA devices and restrict self-registration of MFA devices (do not allow users to register their own MFA devices). Alternatively, periodically audit user MFA settings to verify that users are registered with only known devices.

VIRTUAL PRIVATE NETWORKING (VPN)

Properly securing your remote connections into your network is a critical control. Effective virtual private networking assists in protecting you from compromise.

- [ ] If you have good filters in place and adequate bandwidth, use full tunnel VPN to route and better control all traffic to/from the remote workers' systems. Remind users that VPN should only be used for business purposes. If split tunneling is necessary, make additional investments to secure the user endpoint.
- [ ] When supplying computers to remote workers, use an "always-on" VPN solution (i.e., "force tunneling") to prevent users from accessing the Internet without VPN. Accessing the Internet without proper corporate controls that limit risk can expose remote users' systems to potential compromise.

PHISHING PREVENTION

As corporate, government, and personal electronic communication has increased in response to the pandemic, so has phishing. Tightening controls around email can be effective in preventing phishing.

- [ ] Tighten phishing controls to trigger on keywords such as "COVID," "Coronavirus," or "stimulus." Prevent emails that contain these words and a link from reaching the intended recipient, or replace dangerous email contents with a security warning curated by the organization.
- [ ] Where you can, filter web traffic to unknown or uncategorized websites and/or Internet hosts. For personal equipment, encourage remote users to use endpoint security suites that also do this.
- [ ] Tighten restrictions on traffic to and from risky, out-of-country hosts.

SYSTEM AND DEVICE SECURITY

Securing home networks and the equipment remote workers use to access your network can help prevent compromise. Whenever possible, use solutions you can control.

- [ ] Where possible, for remote users, assign endpoint equipment that you configure and control.
- [ ] Make sure the equipment you deploy limits your risk. Utilize a robust endpoint production solution that monitors and controls several aspects of the device OS. Limit (if possible) local administrative rights. Enable full disk encryption in the event that the device is lost or stolen.
- [ ] If your remote workers need to use personal equipment, take suitable steps to protect them and the enterprise. Provide and/or require endpoint protection software on personal devices. Use controlled Virtual Desktop Infrastructure (VDI) to support remote workers using their own personal equipment to access the network. Encourage them to use full disk encryption.
- [ ] Remind remote workers to store all systems and devices in a locked location.
- [ ] Enable (if possible) regular patches and updates to remote workers' computers.

USER SECURITY

The rush to work-from-home has increased the number of remote workers who may not be familiar with effective security practices. Continue to educate users on the risks of remote work and enforce corporate security standards.

- [ ] Instruct employees to only use trusted networks, including trusted WiFi networks, and avoid using open WiFi networks such as in local coffee shops or other shared spaces.
- [ ] Instruct employees to protect home networks with strong WPA2-PSK WiFi keys and secure home routers.
- [ ] Enable passwords for remote meeting bridges and video conferences.
- [ ] Regularly check for and install security related updates for all software, prioritizing popular third-party meeting and remote access applications that have been the subject of recent security advisories.
- [ ] Continue to educate on the risks associated with opening attachments (of any kind) from unknown senders.
- [ ] Continue to educate users on the importance of strong passwords that are lengthy, not based on dictionary words, and not shared between personal and corporate systems.
- [ ] Educate users on the need to validate email and voice-based requests (such as requests to transfer money or pay an invoice) to confirm the sender's identity by following established policies and procedures.

LOOKING TO LEARN MORE?

Check out our on-demand webinar on scaling your MFA and VPN programs and enabling your remote workforce.

Watch Now

FOCAL POINT
DATA RISK

Contact Us

focal-point.com

+1-813-402-1208 // askforadvice@focal-point.com