Eight Checkpoints to Safeguard Your Network

Thank you for downloading this free resource from Capital Data Service. This list will help you identify important checkpoints in your network's security system to ensure your business is protected from cyberthreats and attacks. While each organization has specific security needs and requirements, the checkpoints below will give you a strong foundation to determine whether or not your network is at risk.

Is Your Network Secure?

Confirm a serviceable firewall is installed. Make sure you are not just using the router from your ISP as a firewall. A standalone firewall is the best protection for your network and is the first item in the line of defense on a network.

Regularly check for firewall firmware updates. Your firewall is only as good as it's latest firmware update from the manufacturer. If you do not know how to check the firmware level of your firewall, it is very likely that your network is at risk.

Keep firewall services running & current with manufacturer support. These services can include ICSA-Certified Gateway Anti-Virus, Intrusion Detection & Prevention, Content Filtering, Anti-Spyware, Application Intelligence and control services. Make sure you subscribe to the manufacturer's 24/7 support. This provides access to critical firmware updates and urgent notifications of the latest threats! If your firewall is more than a year old and has not been renewed for services and support, your network is most likely at risk.

Make sure your WiFi network is limited and protected with a complex passcode.

Limit physical access to network devices, providing access only to authorized individuals.

Do not allow rogue devices access. Rogue devices such as unknown WiFi routers and network switches can cause major issues.

Install and regularly update Anti-virus. Anti-virus should be up-to-date on all devices that access the network including servers, desktops, laptops, tablets and mobile phones. It is strongly recommended to use an enforced Anti-virus that integrates with your firewall. This allows authorized devices to connect only after they have the Anti-virus definitions updated to the most recent version.

Confirm you have an Anti-SPAM solution in place. This can eliminate phishing attacks from ever reaching your email.

Have an accredited third party analyze & test your network. Having a CISSP certified, experienced third party perform a network security analysis and penetration test can identify holes that may be left open from poor configuration practices or that were only meant to be open temporarily but never closed.

If you are unsure whether any of these items are being handled or are unable to confirm you have these basic items in place, you should **contact us immediately for a comprehensive network audit!**

We can quickly discover and document where your network is vulnerable. From there, we can develop a plan of action to make sure your network is always protected against current and future malicious threats.

CAPITAL DATA
SERVICE
770-277-9406
info@capitaldatainc.com
www.CapitalDataInc.com