Cyber Security Check List - 2021

By www.sliceutilities.com

Let us help you get your company protected today!

- What is Cyber Security
- 2020 -2021 Goals of Cyber Attackers
- Cyber Security Basics
- Basics of Firewall and Network Security
- OS/Patch Management
- Basics of MDM - Mobile Device Management
- Basics of End Point Security
- Basics of Identify / Login Access
- Data and Server Backup
- Email Backup and Protection
- Areas businesses forget to protect (IOT)
- 2019 Top Threats in Cyber Security
- Big Attacks and loss of Data in 2019
- Are Building Automation Systems Really Vulnerable to Cyber Threats?
- Automation Systems - IOT must be secure
- Summary of Advance Security that you could take advantage of in 2019/2020.
- Understanding CARTA and the philosophy behind it.

If you need assistance with any of these topics.

You can schedule a free, no obligation, appointment to discuss your needs and how we can help.

Visit Us: SliceUtilities.com

Glenn Davis
Business Technology Consultant
Energy Efficiency Consultant
714.713.1528 cell
949.579.9341 office
Email: glenn@omegamagnus.com
www.sliceutilities.com

Firewall Security:

1. Is your firewall more than 3 years old, it may be a prudent to replace it with a newer model:_____
2. Do you have a spare firewall programmed and ready to go to swap out if your firewall fails? _____

- Replacement Firewall - This could simply be one shelf ready to go, or a more advanced auto failover system in place.
- The key is to remember is to take snapshots of your current firewall configuration after any major changes and store it in accessible storage (USB) to upload to failover / spare firewall to quickly get backup and running.

3. Do you have antivirus and deep packet inspection turned ON? _____
4. Firewall VPN— Does your firewall have a secure VPN solution? _____
5. Firewall VPN— Do you document who has access to VPN and Is there security in place to immediately revoke access when an employee is no longer with the company?_____
6. Is your firewall actually blocking unsecure ports and services of high risk from accessing your network? _____

Notes: Your firewall is your primary defense from unwanted access and theft of data, not only do you need a good firewall it must be configured correctly.

Network Security Options:

1. Do you have a separate VLAN or Physical LAN for Computers, Guest WIFI, IOT and Phones (keep each group separate and pay attention to public internet access to these devices)? _____
2. **Advanced Network Security options:** Are you using Level 3 switches and level 3 routers to work together to optimized network traffic? If SMB— I recommend Level 2 switches and maybe Level 3 Firewall.
3. **Advanced Network Security options:** is used to separate all internet enabled devices to a separate subnets and physical switches, (0r VLANs) by group. Next allow only the needed ports to transverse to each network segment. If SMB—I recommend IOT on its own network and switch, VOIP on it own network and switch, then the workstations and Servers together. Do not allow your IOT to be accessed from the internet or public WIFI unless it is behind a IOT Gateway, or a secure tunnel.
4. **Advanced Network Security options:** automatically block any new device that attaches to your data/computer network by default. This is an advanced option by some Level 3 switches and Firewall working together.

Notes: At minimum, keep a spare switch on shelf or in failover mode to more effectively get the network back online after switch failure.

OS updates for Workstations and Servers:

OS updates and 3rd party apps: In 2019 - the development of malware designed to look like a important upgrade, update or patch is on the rise!

1. Computer Operating Systems and 3rd party app updates - how often do you update your software? _____
2. A Remote monitoring and management system for computers is now a mandatory service for even SMB size companies, do your have one in place? _____
3. Replace when possible, WIN 2007 workstations and Server 2008 / Server 2008 R2 - support ends on JAN 14 2020.
   _____

Notes: RMM: Detect hardware issues, devices offline, history on computer, and OS patches, updates and related information.

(MDM) Mobile Device Management:

1. Do you have a system and procedure for managing the purchase, life cycle, replacement, and security of your mobile devices such as phones, tablets, chrome books, and WIFI hotspots? _____

- More people are using company email, FTP, VPN, and other company data on portable devices. Do you have a way to quickly remove data and cut off access from a device if needed?_____

Note: If a device is stolen and you can not remotely wipe it, then your company is liable for a data breach for all data that employee had access to on that device!

Endpoint Security:

(A new term for antivirus, malware, and related protection services)

1. **Does your computers have (Antivirus, Malware, Crypto Security) ?_____**
2. **How often does your antivirus update - weekly, monthly, daily, hourly?_____**
3. **Do you have a Managed End Point Security that can be access from a Web Portal to provide critical data on End Point Security for all your computers on a single pane of glass?_____**
4. **Does your managed antivirus solution block web content, and device control such as USB drives?**
   _____
5. **Does your antivirus solution auto scan USB drives, Flash Drives and other portable data devices when they plug into a computer? _____**

Note: A computer needs updates and antivirus even if it is seldom used. Any business computer without antivirus and updates is a potential tool to access your network and cause issues for everyone in the company!

Identity Management / Login Access:

(A new term for how to allow access a computer, website, or device to gain information.)

1. Does your company have a password policy?_____
2. Does your company use a 3rd party password manager? _____
3. Does your company have a 2 factor or Multifactor solution to confirm your identity before accessing critical data, such as computer login, email, VPN, Password Manager? _____

Note: Having a very difficult password or constant changes to a primary password usually results in causing employees to store the password in the open, for others to find. Make your policy balanced for everyone.

Social Engineering is still a critical way for government sponsored hackers and competitors from gaining access. You need to avoid passwords and security information being left in the open for janitors, visitors, and temp employees to find.

Disaster Plan (DR Plan) and Backup Solutions:

1. Does your company have a realistic Disaster Recovery Plan ?_____
2. Does your company have a realistic File level and Server Backup system?_____
3. How long does it take to recover a lost File from a network drive, do you have file versioning enabled?_____
4. How long does it take to restore a Server from backup? _____
5. Is your onsite backup server physically located in a different location then your Servers?_____
6. Do you have backups offsite in a secure location? _____
7. Do you have an install copy of your backup software solution to install, if you lose your backup server? _____

Note: Many new versions of even the same backup software will not support older backup sets, thus be unable to restore them. Consider what would happen if you lost your office and only had your offsite backups to rebuild your data and systems?

Email Backup and Protection:

1. Is your company email protected?

_____

2. Even office 365 and Google GSuite could use additional antivirus scans on email, and phishing attacks. Does your email have 3rd party email protection?_____

3. Do you have training classes and test to see if the employees can tell the difference between a real email from the CEO, CFO or a phishing attack?

_____

4. Do you have adequate email backup by a 3rd party for secure auditable reviews for HR and Legal requests?

_____

Note: Office 365 and Google G Suite - they both claim up time of around 99%, but with such a large client base, that 1 percent down or 1 percent data loss can still be you!

IOT Security Concerns:

Any small device that connects to the internet or network (IOT):

1. VoIP Telephones should be on a separate VLAN or preferably different physical network then the computers and data shares.

2. Most VoIP Phones are easily hacked, be sure they are up to date, and are not accessible directly from the internet without going through an IOT gateway or secure web portal.

3. Most DVR / NVR are easily hacked, be sure they are up to date, and are not accessible directly from the internet without going through an IOT gateway or secure web portal.

4. IOT devices on WIFI - at the very least put them on a secure WIFI network with no access to other key networks such as computer network, data shares, SQL servers and so forth.

5. WIFI Network for IOT Devices - use an extremely long and difficult WIFI password, set the login authority to most secure as possible, do not share or allow employees to use the same WIFI Network!

6. WIFI Network - hidden SSIDs or WIFI Names do not deter hackers anymore, so do not feel safe because no one can see the name.

7. WIFI Network - WAP (Wireless Application Protocol) standard 2003 is no longer secure, any novice can hack the network within a few hours! Upgrade to WAP2, or if possible the new standard WAP3 if your IOT devices can support it.

8. WIFI Network - WAP2 2004 has been around for a few years but in 2017 a few critical holes became known, be sure your WIFI Routers and WIF APs have the latest firmware on them if you are using WAP2, which most companies are using today.

9. WIFI Network - WAP3 2018 - before purchase, be sure your current IOT devices can support WAP3, and consider the need to upgrade them as well, when you roll out the new IOT WIFI Network.

10. IOT reboot - there are efficient (more expensive) ways to remotely reset the power on IOT Devices in order to easily reboot them.

11. IOT Monitoring - IOT devices are the hackers new area of focus since late 2016. Though the IOT device may only have minimal info on it, like a light bulb, or thermostat. IOT can be infected with a Botnet (like Mirai) and then used as an attack point against your critical network.

12. Keep your IOT off the public internet, unless it is behind a IOT Gateway, type of tunnel like VPN, or IOT Services.

CARTA

Continuous Adaptive Risk and Trust Assessment is a new approach with cyber and physical security. This philosophy acknowledges there is no perfect protection or security solution. Thus, security needs to be adaptative - everywhere - all the time improving to keep up with modern hackers and government sponsored attacks.

This is why you must have access to people that can see the big picture and are constantly developing procedures, systems, and tests to try to stay ahead of the latest threats of cyber attackers.

This is the future for Cyber Security, never assume you are really secure everywhere and all the time. Limit your exposure to hackers by managing your data, basic employee training, and use security systems that change and grow as your company does.

Financial Responsibility: understand your financial risks and then use that as the measure of what Cyber Security to invest in. Do not be tricked by fancy Cyber Security Firms with fancy terminology, trying to sell you something you do not understand or think you need.

The only worse thing then a hacker breaching your security is a tech company selling a device or service that you will not use, or does not protect the areas that are critical to your company.

Just because many companies are using that service, or security equipment, does not mean it is a right fit for your budget or company.

Financial Budget:

The expected budget for IT Technology in a business is for SMB is 6.9% (average-size company) and 4.1% (midsize company). Out of that IT budget up to 10% should be on Cyber Security systems.

Remember to continue to adapt to your security needs, educate your team and plan for the worst.