TECHNOLOGY CHECKLIST

Businesses are quickly deploying all kinds of technology. Different kinds of technologies come with different risks and strategies to protect them. This checklist is designed to help you identify the technology in your business you need to protect. In addition, there are some basic security tips, considerations and links to resources that can help you learn more to detect, respond to and recover from cyber incidents.

- ☐ WIFI
- ☐ ROUTERS
- ☐ FIREWALLS
- ☐ MOBILE DEVICES
- ☐ EMAIL
- ☐ FILE SHARING
- ☐ COPIERS/PRINTERS/FAX MACHINES
- ☐ CLOUD SOLUTIONS
- ☐ VPN
- ☐ SWITCHES
- ☐ USB
- ☐ WEBSITE
- ☐ SOCIAL NETWORKING
- ☐ POINT OF SALE
- ☐ 3RD PARTY VENDORS

WIFI:

- Use strong administrative and network access passwords
- Use strong encryption (WPA2 and AES encryption)
- Use separate WiFi for guests
- Physically secure WiFi equipment
- Get savvy about WiFi hotspots – Limit accessing sensitive information on public WiFi – Use VPN when using public WiFi

VIRTUAL PRIVATE NETWORK (VPN):

- Use strong passwords, authentication and encryption
- Limit access to those with valid business need
- Provide strong antivirus protection to users

NETWORK DEVICES:

Routers and Switches

- Use a network monitoring app to scan for unwanted users
- Restrict remote administrative management
- Log out after configuring
- Keep firmware updated
- Use strong passwords

Firewalls

- Default rules should block everything that is not specifically necessary for the business

USBs:

- Scan USBs and other external devices for viruses and malware when connected
- Only pre-approved USBs allowed in company devices
- Educate users about USB risks

NATIONAL CYBERSECURITY ALLIANCE

STOP | THINK | CONNECT™

WEBSITE:

- Keep software up to date
- Require users to create strong passwords to access
- Prevent direct access to upload files to site
- Use scan tools to test your site's security – many are free
- Register sites with similar spelling to yours
- Run most current versions of content management systems or require web administrator/hosts to do the same

MOBILE DEVICES:

- Keep a clean machine: Update security software on all devices
- Delete unneeded apps
- Secure devices with passcodes or other strong authentication such as a finger swipe and keep physically safe
- Encrypt sensitive data on all devices
- Make sure "find device" and "remote wipe" are activated

EMAIL:

- When in doubt, throw it out: Educate employees about remaing alert to suspicious email
- Provide all email recipients with an option to opt off your distribution list
- Require long, strong and unique passwords on work accounts
- Get two steps ahead: Turn on two-factor authentication

FILE SHARING:

- Restrict the locations to which work files containing sensitive information can be saved or copied
- If possible, use application-level encryption to protect the information in your files
- Use file-naming conventions that are less likely to disclose the types of information a file contains
- Monitor networks for sensitive information, either directly or by using a third-party service provider
- Free services do not provide the legal protection appropriate for business

SOCIAL NETWORKING:

- Create page manager policies and roles
- Limit administrative access
- Require two-factor authentication
- Secure mobile devices

CLOUD AND OTHER 3RD PARTY VENDORS:

- Discuss the approach to security and codify in any agreements and contracts

POINT OF SALE (POS):

- Make unique, strong and long passwords and change regularly
- Separate user and administrative accounts
- Keep a clean machine: Update hardware and software as needed
- Avoid web browsing on POS terminals
- Use antivirus protection

COPIERS/PRINTERS/FAX MACHINES:

- Understand that digital copiers/printers/fax machines are computers
- Ensure devices have encryption and overwriting
- Take advantage of all the security features offered
- Secure/wipe the hard drive before disposing of an old device
- Disable the web management interface or change the default password

OTHER:

Secure Disposal

- Be aware that many devices, not just PCs and phones, have memory. Know how to clean old data before disposing

Internet of Things (IoT)

Consumer Protection and Defense Recommendations

- Isolate IoT devices on their own protected networks and change default passwords
- Know what information is being collected and how and where it's being stored and protected
- Consider whether IoT devices are ideal for their intended purpose
- Purchase IoT devices from manufacturers with a track record of providing secure devices
- When available, update IoT devices with security patches

(Source: www.ic3.gov)

Consumer Reports –
Privacy Tips for the Internet of Things
http://www.ic3.gov/media/2015/150910.aspx

FTC – Careful Connections:
Building Security in the Internet of Things
http://1.usa.gov/1Vgftep

NATIONAL CYBERSECURITY ALLIANCE

STOP | THINK | CONNECT™