# BUSINESS CYBERSECURITY CHECKLIST

Your business needs to prioritize cybersecurity, no matter your size, no matter your industry. Every business with digital assets faces cybersecurity threats. This checklist helps identify risks, protect assets, and plans for the worst.

- [x] **Inventory your I.T. assets.**
- [x] **Perform a risk assessment.**
- [x] **Maintain a strong password policy.**
- [x] **Limit user access.**
- [x] **Protect your end points.**
- [x] **Update your I.T.**
- [x] **Secure your Wi-Fi.**
- [x] **Monitor for threats.**
- [x] **Educate your employees.**
- [x] **Back up your data.**
- [x] **Plan for data recovery.**

323-638-1870 hello@stginfotech.com www.stginfotech.com

IT CONSULTING GROUP

## Inventory your I.T. assets.

You can't protect what you don't know you have. An important first step is to inventory all your business technology. This includes hardware such as company desktops, mobile devices, and routers; plus, you'll need a current list of all software and applications you use. This will evolve, so plan on updating your inventory asset list on a regular basis.

Encrypt any mobile devices and make sure you have the ability to wipe those devices clean. That way, if a laptop or smartphone is stolen or goes missing, you have control of the data.

Note: If users bring their own devices, you need to inventory those devices, too. You'll want to establish a policy for the types of devices people can connect. Further, limit the apps users can download, as they could harbor malware or other risks.

## Perform a risk assessment.

Once you have an IT inventory, it's easier to perform a risk assessment. Besides the hardware and software you have to secure, you'll also want to determine your data assets. For example, if you're in healthcare, you have patient health information to protect. If you're in retail, you have to protect payment information.

Other valuable assets could include trade secrets, employee details, and market trend data. You might also be at risk because of the role you play in the supply chain. A costly breach at a major big-box retailer started with illicit access of its HVAC company's IT systems.

As part of the assessment, consider the most critical threats you face. Natural disasters and extreme weather could be more common in your location. Maybe your industry is often targeted by hackers or you're using legacy technology that you haven't yet replaced.

## Maintain a strong password policy

Better protect customer, employee, and proprietary data by calling for strict password guidelines. Your business might encourage users to use password generators to ensure password complexity. Also, encourage the use of an encrypted-password manager to securely store all those unmemorable passwords. Also use encrypted-password managers for different passwords for each employee's online account.

On your end, require password changes on a scheduled timeline or when data breaches occur. Also, use multi-factor authentication to add a layer of protection to your user access.

## Limit user access

Manage your users' access privileges. Give team members the ability to access only the tools they need to complete tasks. This follows the Principle of Least Privilege for restricting access rights. It's like the "need to know" principle you hear about in spy movies. Limiting user access can minimize the damage caused by a breach.

## Protect your end points

There was a time when you set up firewalls around your business systems and tried to keep the bad guys out that way. But now that more people are working remotely or in hybrid environments, you need to protect all IT end points. You have your people outside the firewall trying to get in, too, so you'll need to establish stronger security parameters. Firewalls check all your incoming and outgoing traffic. Geofencing, which tracks access based on the internet protocol address, can help too. Antivirus software and malware-removal tools also play an important role.

## Update your I.T.

Maintaining current Web browsers, software, and operating systems supports your security profile. Manufacturers update their technology to block attacks when threats or vulnerabilities are detected. If you ignore an update notification, you could be leaving your business at risk.

If you're relying on old technology, think twice. Cyber bad actors target legacy infrastructure, because they know that people get complacent and don't upgrade, even when security support is no longer available.

## Secure your Wi-Fi

If you haven't changed the default password on your Wi-Fi device, do so now. Also, plan to rotate the passwords for your Wi-Fi to keep the network safer. In your work environment, use separate guest and business networks, and limit access and how long someone can be online using the guest network.

Another good idea? Turn off your Wi-Fi during business off hours. Leaving it on makes it more likely a hacker can get in when no one is there to notice.

You should also restrict off-site Wi-Fi use by your employees. When they connect from outside of your business, require them to be on private, encrypted Wi-Fi.

## Monitor for threats

You'll also want to set up scanning to look for trends and spot a possible attack or vulnerability sooner. Monitoring your data logs and user access behavior can help you spot traffic you don't want. Also, keep current on the latest threats. Product manufacturers work to stay abreast of what cyber bad actors are up to. You can also benefit from staying informed about new threats discovered. This will help you know what signs to look for and be proactive.

## Educate your employees

Employees are often the weakest link in your cybersecurity – mistakes will happen, and people grow more careless over time. Make ongoing awareness a priority, and don't rely only on an onboarding cybersecurity session. You might even test your employees' ability to identify phishing scams and ransomware.

You should also be changing your security policies regularly to reflect changing security trends. Communicate those new policies to your employees and offer training sessions as needed.

## Back up your data

Having a backup plan can help secure your business data if the worst happens. Data backup best practices include:

- implementing a data backup process;
- keeping more than one data backup;
- encrypting data backups;
- limiting access to your data backups;
- test your backups.

Regularly scheduled data backups can help you through a hack or other emergency. But don't rely entirely on automated backup. Something could go wrong, and you might not know until you need that backup. Have a process for human evaluation of the data backup process.

## Plan for data recovery

Plan ahead for the worst. Data recovery is smoother and faster if you proactively evaluate and test your process. Write down the steps you will take if a breach occurs or a natural disaster strikes, and know who is responsible for what.

Decisions to return to business as usual are easier if you put a process in place first. It's more difficult to do when you’re in the midst of crisis stress.You should also be changing your security policies regularly to reflect changing security trends. Communicate those new policies to your employees and offer training sessions as needed.

## Help protecting your business

Ultimately, every business needs to expect and prepare for a cybersecurity crisis. This checklist helps you gauge risk and put plans in place to protect assets and recover sooner. Our IT experts are here to help your business improve its security status. Contact us today at 323-638-1870.