












# 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 will help you identify risks, protect assets and plans for the worst.

-  **Inventory your IT assets.**
-  **Perform a risk assessment.**
-  **Maintain a strong password policy.**
-  **Limit user access.**
-  **Protect your end points.**
-  **Update your IT.**
-  **Secure your Wireless Network.**
-  **Monitor for threats.**
-  **Educate your staff.**
-  **Back up your data.**
-  **Plan for data recovery.**





## 1. Inventory your IT assets.

You cannot protect all your assets when you don't know what you currently have. The important first step is to inventory all your business technology. This includes hardware such as company laptops, desktops, mobile devices (phones & tablets), and network equipment (routers, switches, firewalls, wireless access points etc); plus, you will 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 all mobile devices and make sure you can remotely wipe those devices clean. This way, if a laptop, phone or tablet is goes missing or is stolen, you have control of the data.

Note: If users bring their own devices, you need to inventory those devices too and establish a policy for the types of devices people can connect. Further limiting the apps users can download, will increase security as they can harbor malware and you don't know what other security holes they may contain.



## 2. Perform a risk assessment.

Having an IT inventory makes it much easier to perform a risk assessment. Besides the hardware and software you have to secure, you will also need to determine your data assets. For example, if you are in healthcare, you have to protect patient health information and if you're in retail, you have payment information to protect.

Other valuable assets could include company IP, staff and client details. You might also be at risk because of the role you play in the supply chain. A recent breach at a major big-box retailer started with illicit access of its HVAC company's computer 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 are using legacy technology that you are yet to replace.

### 3. Maintain a strong password policy

Better protect customer, employee, and proprietary data by using strict password policies. Your business should encourage the use of password managers and to use password generators to ensure password complexity.

On your end, require password changes on a scheduled timeline or when data breaches occur. Also, the use multi-factor authentication (MFA) is a must. MFA adds a layer of protection to your user access.

### 4. 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 is like the "need to know" principle you hear about in spy movies. Limiting user access can minimize the damage caused by a breach.

### 5. 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 will need to protect all IT end points. You have your people outside the firewall trying to get in, too, so you will 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 other security software tools also play an important role.

## 6. Update your IT.

Regularly updating your web browsers, software and operating systems increases your security profile. Software manufacturers update their software to help block attacks when threats or vulnerabilities are detected. If you ignore an update notification, you could be leaving your business open to attack.

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

## 7. Secure your Wireless Network

If you have not changed the default password on your wireless network recently, do so now. 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 wireless use by your employees. When they connect from outside of your business, require them to be on private, encrypted Wi-Fi.



## **8. Monitor for threats**

You will 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 do not want.

Try and 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.



## **9. Educate your staff**

People are always the weakest link in your cybersecurity – mistakes will happen, people grow more careless over time and accidentally click on links or open attachments they think are legitimate. Make ongoing security awareness a priority, and do not rely only on an onboarding cybersecurity session. You can even simulate a phishing attack to help test your staff's 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.



## 10. 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 an emergency. But do not 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.



## 11. 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.

## Help protecting your business

Ultimately, every business needs to expect and prepare for a cybersecurity crisis. This checklist helps you to gauge risk and put plans in place to protect your assets and recover sooner. Our IT experts are here to help your business improve its security status. Contact DP Computing today on (08) 8326 4364.