Microland Computer Center

Threat Assessment

Here at Microland, our goal is to keep the data of your business and employees safe and secure. Organizations of all sizes face a constant barrage of data security threats. Together, we can make sure your business has the best possible protection to prevent security breaches.

So what is a threat?

A threat is an attack or neglect that could do your business harm. This threat may come from an employee, a customer, an unknown person, or even from system or equipment failure which can happen for a variety of reasons.

Can threats be prevented?

Absolutely. Unfortunately, no system is 100% impenetrable, but there are preventive measures and safeguards that can be implemented to keep your data as secure and protected as possible.

Determine your vulnerabilities.

In computer security, a vulnerability is a weakness which allows an attacker to reduce a system's information assurance. This Threat Assessment will walk you through how to identify vulnerabilities in your environment.

How do I keep my data safe?

Backups are one of the most important things you can do for your business. Loss of data can happen due to threats, natural disasters, and other factors. Having a current and accessible backup is key to making sure you can get back to business when catastrophe strikes.

On the next page, you will be asked a series of questions to evaluate your business security. Answer these questions honestly and accurately and partner with your IT department for ways to shore up your weak spots, reinforce your current protection, and ensure that your data stays safe, secure, and accessible.

Microland Computer Center

Threat Assessment Questionnaire

Below are some simple questions to assess how well your business is protected...

Is your equipment secure...

1. Is your server and network equipment stored in a locked room?
2. Is your server and network equipment stored off the ground?
3. Is your server and network equipment stored in a locked rack?
4. Who has access to this equipment?
5. Is your server and network equipment password protected?

Are your workstations secure…

6. Are all of your workstations password protected?
7. Do your employees work off of personal computers?
8. Do you have trusted antivirus and antimalware software on all devices that connect to your business network?
9. Do your employees use external devices like flash drives or external hard drives to download data off company computers?
10. Do your employees use external devices like flash drives or external hard drives to upload data to company computers?

Is your network secure…

11. Do you have a Firewall?
12. Where is your Firewall kept? Is the room secure? Is the room well ventilated?
13. Who monitors your Firewall? When is the last time the firmware was updated?
14. What kind of physical security does your firewall possess?

Is your data secure…

15. Who has access to your most sensitive data?
16. What qualifies a person to have access to this sensitive data?
17. How is access to sensitive data monitored?
18. What is the action plan or steps to be taken in the event this data or the people given access to this data is compromised?

Is your data recoverable…

19. Do you have a backup?
20. How often is your data backed up?

If you backup your data locally…

21. Who is responsible for monitoring the backup?
22. What kind of device do you use to store the backup?
23. Is your backup storage device encrypted?
24. What is the process to replace a failed storage device?

If you backup your data remotely…

25. Who is responsible for monitoring the backup?
26. Does your remote monitoring system provide you with regular backup status reports?
27. What is the plan of action when data needs to be restored?
28. Is the information encrypted?
29. How is their data protected?

30. If your data is lost, what level of impact will it have on the business?

Low impact – the data is not critical for the functions of our business; will not result in revenue lost

Moderate impact – the data only mildly impacts the functions of our business; will not result in revenue lost

Severe impact – the data is vitally important to the functions of our business; would result in revenue lost

Catastrophic impact – the data is the backbone of our business operations; would result in temporary or permanent loss of revenue