Cybersecurity Threat Assessment and Action Checklist

Wyoming SBDC Network

Please email Wyoming SBDC Cybersecurity Program Manager Paul Johnson or call 307-314-5208 for assistance with completing this checklist or contact your SBDC Advisor for assistance. Visit the Wyoming SBDC Network website for comprehensive small business assistance.

Yes	No	N/A	Password Security
			1. I changed all default passwords on my devices and software.
			2. I use strong, unique passwords for each of my accounts made up of at least 12 characters and include uppercase, lowercase, numbers, and symbols.
			3. I enabled two-factor authentication (2FA) wherever possible.
			4. I use a password manager—not a browser—to securely store my passwords.

Yes	No	N/A	Software and Systems
			5. I keep all my operating systems and software up to date with the latest security patches.
			6. I have antivirus software installed and updated on all my devices.
			7. I activated a firewall on my network and devices.
			8. I regularly back up my important data and store it securely off-site or in the cloud.
			9. I double-check the output from AI for any errors and/or biases.
			10. I am cautious with the usage of third-party applications, software, and AI technology/ plug-ins.
			11. If I do use any third-party AI-driven applications, I am aware of the data that is collected and permissions given.

Yes	No	N/A	Email and Web Browsing
			12. I can confidently identify phishing emails.
			13. I activated spam filters on my email systems.
			14. I check links and attachments before clicking on them. If the address or file type does not match what I expect, I do not click on it.
			15. I use secure, encrypted connections (HTTPS) when browsing sensitive websites.
			16. I use a business grade WiFi network.
			17. I implemented web filtering to block access to potentially malicious websites.
			18. I have a VPN installed for safe internet browsing.
			19. I have a proxy server in place.

Yes	No	N/A	Mobile Devices and Remote Work
			20. I password-protected or enabled biometric authentication on all my business mobile devices.
			21. I can remotely wipe data from my devices if they are lost or stolen.
			22. I use a secure method to access my business data when working remotely, such as a VPN.
			23. I avoid using public Wi-Fi for business purposes without a VPN.
			24. I set clear boundaries between personal and business use on my devices.
			25. I regularly back up business data and have a recovery plan in place in the case of a security breach.
			26. I ensure that all my business devices are up to date with the latest software updates to protect against vulnerabilities.

Yes	No	N/A	Data Protection
			27. I encrypt my sensitive customer and business data.
			28. I established a clear data retention and destruction policy for my business.
			29. I securely store physical documents with sensitive information and shred them when no longer needed.
			30. I limit access to my sensitive data, even when sharing devices with family or friends.
			31. I ensure compliance with relevant data protection regulations (e.g., FTC, WDGC, WCPA, HIPPA) that apply to my business.
			32. I only use a USB when necessary for information storage/sharing.
			33. If I use a USB device, my antivirus software automatically scans it when connected.
			34. My method of file transferring is secure (e.g., cloud storage, network share drive, managed file transfer).

Yes	No	N/A	Incident Response and Internal Training
			35. I documented a plan for responding to a cybersecurity incident.
			36. I regularly educate myself and my staff on current cybersecurity best practices.
			37. I test myself and staff with online phishing simulators to maintain awareness.
			38. I identified IT or cybersecurity professionals I can consult if needed.
			39. I have personnel and administrative cybersecurity policies and procedures and review and update them at least annually.
			40. I have considered or purchased cybersecurity insurance for my business.