Business System Solutions

Caretakers of Your Productivity
since 1995

THE BSS ADVISOR

Monthly Newsletter

February 2025

IT Security Audit: An Owner's Checklist

Knowing what's in place can guide your path to better safety and protection of your business.

Business System Solutions is your IT Service Partner who provides peace of mind through guidance, education, and responsive support. We are the Caretakers of Your Productivity.

With Offices in:
North Central Indiana
(765) 742-3440

Middle Tennessee
(615) 819-0600

West Michigan
(616) 776-0400

info@bssconsulting.com

"For God so loved the world that he gave his one and only Son, that whoever believes in him shall not perish but have eternal life.'"
John 3:16

by Anisa Williams, BSS Staff

Security should not be a burden, but business owners don't have time to think about, research, and implement IT security protocols. CEOs have to trust that their IT folks are keeping up on security and doing all they can to protect the company. As the cybersecurity landscape becomes increasingly challenging to navigate, reliance on IT expertise is more important than ever before.

One challenge is that IT vulnerabilities must be constantly reviewed and addressed. Ignoring or choosing a lesser protection in one area can mean at best, a disruption to a user and at worst, a ransomware/data exfiltration event that is irrecoverable or a massive financial setback.

The best security is a multi-layered approach: Even doing the minimal protection in all areas is better than doing nothing at all.

Use this checklist to audit your current IT systems or as a guide when selecting a new IT company. For each security protocol, review the column that most closely matches what you have. If Vulnerable (1 pt.), Minimal (3 pt.), or Best (5 pt.), write your score in the last column. Then total up the score to find out next steps and recommendations to create a defensive IT roadmap. *Acronym definitions are listed below the table.*

(Continued on Next Page)

(Continued from page 1)

SECURITY PROTOCOL	VULNERABLE (1)	MINIMAL PROTECTION (3)	BEST PROTECTION (5)	SCORE
Patches & Updates	Manual application, initiated externally	Upgrading when notified or receiving all updates automatically	Reviewed by IT for compatibility and pushed on a schedule; regular restarts scheduled	
Monitoring	No monitoring	24/7 automatic issue tickets	Advanced Proactive MDR/EDR; 24/7 NOC & remediation; Advanced Microsoft 365 & Azure AD management	
Passwords	No password requirements; passwords reused or shared and stored in excel spreadsheet	Minimum Policy requirements (12 characters or more); individual use of password manager	Minimum Password length and/or complexity; Enterprise Password Manager with automatic alerting; Dark Web monitoring	
MFA	No or inconsistent use	Authenticator App used for one or some apps by individuals	Enterprise MFA like Duo; company policy enforcement; required for all network and workstation access	
Firewalls, Switches, Wireless Access Points	10+ years old or no longer supported; Firmware and security settings not updated	Manual device management & updates; <10 years old; enough throughput for current needs	Enterprise Managed devices with automated patching & updates; <5 years old; additional throughput for growth; Automatic notifications for issues & downtime	
Network Security	Device defaults; no web or content filtering; no password on WiFi	Basic category web & content filtering for network devices only; no seperate network for guest use	Granular web & content filtering for all devices on the network; reporting, automated updates, audits, & health checks; Segmented VLAN for guests and smart devices	
Data Encryption: at rest & in transit	No or spotty encryption	Encryption at rest (like in SharePoint) but data sent through unsecured email or public networks	End to end encryption for data at rest and in transit; access only by VPNs from remote workers with MFA	
Data Backups	No backups	Backup storage on the network, accessible to staff, and editable; Cloud backups stored in same system as company data	Onsite: Immutable hourly plus daily offsite backups on segmented from network; Cloud: 3rd party backup of all email and files; Critical workstation encrypted backups	
eWaste Wipe & Disposal	Dumped into local trash (illegal) or let employees take home; data not removed from drives	Drop off at local eWaste recycling facility; data drives might be wiped; cell phones not considered	Removal and proper destruction of company data before disposal; Cell phone wipe of company data; Chain of Custody with Certificate of Destruction	
Anti-virus, Anti-Malware	"It can't happen to me"; not installed	Subscription based home versions individually installed with expiration	Managed Enterprise grade with regular updates; automatic renewals; automatic reporting	
Advanced Cybersecurity	No systems or reactive-only	IT technician review and remediation during business hours	Enterprise MDR (on premise or cloud) with canary deployment; 24/7 SOC and SIEM; Hard drive encryption management	
Access Controls	No limits to what any user can access across the network	Least-privilege: Role-based access to specific areas of the network, devices, applications	Zero-Trust: Every user, device, application login attempt is verified and authenticated inside or outside the network	
Physical Security	Unlocked facilities; no visitor processes; server and network devices accessible to everyone	Manual monitoring; internet connected camera; visitor management; segregated server & network equipment	Enterprise system for door entry with card readers; ID badges; locked facilities; camera & infrared alerting; visitor escort only; locked server/network infrastructure	

(Continued from page 2)

SECURITY PROTOCOL	VULNERABLE (1)	MINIMAL PROTECTION (3)	BEST PROTECTION (5)	SCORE
Mobile Device Security	Leaving it open to each user; no password/PIN or MFA	Secured credential login to company apps & files like email; home anti-virus and security software	Enterprise device management; security & access control; remote wipe; Policy enforced anti-virus & web security software	
Equipment Replacement	Replace when it breaks at great cost and downtime; Old computers kept for redeployment	Network devices & servers added to annual budget; computers may be replaced as needed;	4-year Computer Replacement Program (Tech Rider); 3 to 5 year Roadmap for network equipment & server upgrades	
Staff Education and Testing	Common Sense	Passive learning platforms	Mandatory monthly testing for users & reporting; additional resources for security learning	
Strategic Planning & Budgeting	Reactive "break fix"; no planning	Advice from IT or individual research; Annual review	Dedicated Account Manager with your business plan and growth in mind; monthly or quarterly review	
Policies & Procedures	No policies in place	Custom policies or minimal blanket coverage like Acceptable Use	Highest level of compliance policies implemented, regular reporting & audits, such as NIST, DOJ, FTC, PCI, or HIPPA with employee training;	
			TOTAL SECURITY SCORE	

Score Your Results

For each row, select the protection score (1 = Vulnerable, 3 = Minimal Protection, 5 = Best Protection) that matches your company environment. Total up your score and review the recommendations.

1-35: Take Action! Your company is open to risk and threats. Work with your IT team to implement the processes and technologies that can keep you protected and safe, starting with the easiest.

36-74: Needs Improvement. You have some protections in place but there are still many vulnerabilities that could be fixed. Work with your IT Account Manager to identify your needs and make a plan to protect your data and secure your network.

75-90: Great work! You are cyber-savvy and protecting your company from threats. Review what items could be more secure and use this document to regularly review and audit your security needs.

If you need to get your security in shape in any area listed above, give BSS a call and we'd be happy to work with you on a roadmap to your best cybersecurity protections. □

Acronym Definitions

MFA: Multi-Factor Authentication. A secondary identity verification other than a password.

MDR: Managed Detection & Response. An advanced cybersecurity service that helps organizations proactively defend against threats using technology and human expertise. Often deploys "canaries" inside the network that give warning when there is unusual activity.

EDR: Endpoint Detection & Response. Often used interchangeably with MDR, this cybersecurity service works specifically on computers and servers as they are often first line of attack. This includes continuous monitoring and forensics post-attack.

SOC: Security Operations Center. A command center for IT experts to monitor, analyze, and respond to security threats 24/7.

NOC: Network Operations Center. A central location for technicians to monitor, manage, and update the network infrastructure. This may be an IT department or IT Managed Service Provider.

VLAN: Virtual Local Area Network. A segmented network for guest use that is often unsecured and with no password.

Business System Solutions

Return Address:
601 3-Mile Road NW, Suite C
Grand Rapids, MI 49544

The BSS ADVISOR

info@bssconsulting.com

North-Central Indiana Office
1211 Cumberland Avenue
West Lafayette, IN 47906
(765) 742-3440

Middle Tennessee Office
1026 West College Street
Murfreesboro, TN 37129
(615) 819-0600

West Michigan Office
601 3-Mile Road NW, Suite C
Grand Rapids, MI 49544
(616) 776-0400

6 Years in a Row!
2019-2024 Winner
Channel Futures.
Leading Channel Partners Forward
MSP 501

Photo by nini Dorothe/Pixabay

2025

MARK YOUR CALENDARS FOR GREAT EVENTS WITH BSS THIS YEAR!

APRIL
Indiana eWaste Recycling Drive
in partnership with Technology Recyclers
bssconsulting.com/ewaste

AUGUST and SEPTEMBER
BSS 30th Anniversary Celebration Open Houses
in Indiana, Michigan, and Tennessee

OCTOBER
Indiana eWaste Recycling Drive
in partnership with Technology Recyclers
bssconsulting.com/ewaste

Keep an eye on bssconsulting.com/news-events
for the latest updates!