

# DO-IT-YOURSELF COMPREHENSIVE CYBERSECURITY ASSESSMENT CHECKLIST



*Where are the gaps in your information security? Can hackers get into your files? Is your staff able to spot and avoid malware and ransomware attacks? This self-assessment will help you gauge your current state of cybersecurity readiness so that you can plan for the future accordingly. Need help? SwiftTech Solutions will work with you to evaluate your security, create an IT strategy, and execute for optimal results.*

Physical Security	YES	NO	UNSURE	NOTES:
<i>Do you have security procedures such as sign-in books and badges?</i>				
<i>Are your visitors being escorted and given badges?</i>				
<i>Have you checked your security camera systems to make sure they are monitoring and recording?</i>				
<i>Are you preventing access to the physical network in your reception area?</i>				
<i>Do you have your server room locked to prevent unauthorized access to critical network infrastructure?</i>				
<i>Do you secure your server access room, restrict access to key personnel, and log all visitors?</i>				
<i>Do you keep records of who entered the server room?</i>				
<i>Do you check your climate control settings in the server room?</i>				

Policies and Procedures	YES	NO	UNSURE	NOTES:
<i>Do you have Cyber Liability Insurance?</i>				
<i>Have you held an employee cybersecurity awareness training class?</i>				
<i>Have you developed an updated Acceptable Use Policy?</i>				
<i>Have you developed an updated Wireless Access Policy?</i>				
<i>Have you developed an updated Removable Media Policy?</i>				
<i>Have you developed an updated Remote Access Policy?</i>				
<i>Have you developed an updated BYOD Policy?</i>				
<i>Do you have a Disaster Recovery/Business Continuity Plan?</i>				
<i>Have you ensured that only authorized users have access to certain files?</i>				
<i>Do you have a clean active directory to prevent ex-employees from accessing your network via old accounts?</i>				

Policies and Procedures	YES	NO	UNSURE	NOTES:
<i>Do you require a two-factor authentication for sensitive applications?</i>				
<i>Have you applied security policies to your network?</i>				
<i>Do you have strong password requirements throughout the network?</i>				
<i>Are you properly disposing of old equipment?</i>				
<i>Do you have a dedicated password manager that will store your passwords in an encrypted form?</i>				

Servers	YES	NO	UNSURE	
<i>Do you have a business-class, name-brand server with redundant features?</i>				
<i>Have you checked the current and extended warranty coverage on your servers?</i>				
<i>Have you consolidated server hardware and resources?</i>				
<i>Have you made sure your desktop operating system is current and updated?</i>				
<i>Do you have properly licensed server operating systems?</i>				
<i>Are your current server applications installed and updated?</i>				
<i>Do you have server application support contracts?</i>				
<i>Do you provide sources for support and upgraded assistance?</i>				

Workstations	YES	NO	UNSURE	
<i>Do you know if all your laptops are encrypted?</i>				
<i>Have you replaced consumer-grade laptops with business-class equipment?</i>				
<i>Have you standardized your desktop hardware?</i>				
<i>Have you checked the current and extended warranty coverage on your hardware?</i>				
<i>Are your desktop applications and operating systems current and updated?</i>				
<i>Do you have proper licensing of desktop applications and operating systems?</i>				
<i>Do you have desktop application support contracts?</i>				

Power Protection	YES	NO	UNSURE	NOTES:
<i>Is your UPS operating correctly to protect your equipment?</i>				
<i>Is your UPS auto-shutdown operating system configured cleanly in the event of a power loss?</i>				
<i>Is your UPS protecting against power dips, surges and complete power loss incidents?</i>				

Network Infrastructure	YES	NO	UNSURE	NOTES:
<i>Are you providing business-class Gigabit switches that are industry current, fast-core network performance and that allow servers, desktops, and laptops to communicate at optimal speed?</i>				
<i>Are you in compliance with patching panels, cables, &amp; in-wall wiring Cat5e or better?</i>				
<i>Do you have high-speed business-class Internet connection?</i>				
<i>Do you have advanced monitoring of your network device hardware?</i>				

Remote Connectivity	YES	NO	UNSURE	NOTES:
<i>Are you utilizing multi-factor authentication for remote users?</i>				
<i>Are you utilizing SSL-VPN connection security?</i>				

Firewall	YES	NO	UNSURE	NOTES:
<i>Are you making sure your security service subscriptions are current?</i>				
<i>Is your business-class firewall programmed to distinguish legitimate packets from potentially harmful ones?</i>				
<i>Are your open ports on the firewall locked down?</i>				
<i>Have you implemented content filtering?</i>				
<i>Is your firewall under warranty and supported by the manufacturer?</i>				
<i>Have you engaged a third-party to regularly perform external vulnerability and penetration testing?</i>				

Wireless	YES	NO	UNSURE	NOTES:
<i>Do you have business-class wireless access points?</i>				
<i>Do you have WPA2 or better wireless encryption?</i>				
<i>Do you have seperate corporate and guest Wi-Fi?</i>				
<i>Are you guarding your guest wireless network?</i>				

Phone System	YES	NO	UNSURE	NOTES:
<i>Have you moved to a cloud-hosted VoIP phone system?</i>				

Email	YES	NO	UNSURE	NOTES:
<i>Do you have Office 365 email hosting?</i>				
<i>Do you have Office 365 multi-factor authentication?</i>				
<i>Do you have Office 365 advanced threat protection?</i>				
<i>Do you have Office 365 email backup?</i>				
<i>Are you protecting your email messages with email encryption?</i>				
<i>Do you have anti-spam and anti-virus protection for your email?</i>				

Monitoring, Maintenance, & Management	YES	NO	UNSURE	NOTES:
<i>Are you installing Windows updates regularly?</i>				
<i>Do you review event logs for anything unusual?</i>				
<i>Are you managing your anti-virus and anti-spyware software?</i>				
<i>Do you regularly update commonly-used applications?</i>				
<i>Do you routinely run dark web scans?</i>				
<i>Are you running anti-ransomware server scripts?</i>				

Backup	YES	NO	UNSURE	NOTES:
<i>Do you conduct daily server imaging?</i>				
<i>Do you conduct daily file and folder-level backups?</i>				
<i>Are you providing secondary backup sent to dual-US coast secure offsite locations?</i>				
<i>Are you getting regular confirmations of success and ability to restore data?</i>				

Backup	YES	NO	UNSURE	NOTES:
<p><i>Do you have the ability to can spin-up servers locally or in-cloud during a disaster?</i></p> <p><i>Can you ensure your backup destination is blocked off from the rest of the network?</i></p>				



*Good work! "Yes" answers indicate a good state of readiness for the associated control. Any "No" or "Unsure" items should be evaluated for their impact on your business' risk profile.*

*Contact a SwiftTech Solutions security specialist for a free IT consultation to help you review your results.*



**FOR A FREE CONSULTATION, CONTACT US AT**

**877-794-3811**