SHARP®

15 Ways to Protect Your Business from a Cyberattack!

☐

Security Assessment

It's important to establish a baseline and close existing vulnerabilities. When was your last assessment?

Date: _____

☐

Spam Email

Most attacks originate in your email. Be sure to choose a service designed to reduce spam and your exposure to attacks.

☐

Passwords

Apply security policies on your network. Deny or limit USB file storage, enhance password policies, and set user screen timeouts.

☐

Security Awareness

Train your users—often! Teach them about data security, email attacks, and your policies and procedures.

☐

Computer Updates

Keep Microsoft, Adobe, and Java products updated for better security. Automate updates to protect your computers from the latest known attacks.

☐

Advanced Endpoint Detection & Response

Protect your computer's data from malware, viruses, and cyberattacks with advanced endpoint security. Today's latest technology protects against file-less and script based threats.

☐

Multi-Factor Authentication

Utilize Multi-Factor Authentication whenever you can. It adds an additional layer of protection to ensure that even if your password does get stolen, your data stays protected.

1/2 Nearly half of all cyberattacks are committed against small businesses

Every 11 seconds a businesses will fall victim to ransomware by 2021

Cyberattacks will cost businesses more than $6 trillion each year by 2021

Source: Cybersecurity Ventures

☐

Dark Web Research

Knowing in real-time what passwords and accounts have been posted on the Dark Web will allow you to be proactive in preventing a data breach.

☐

SIEM/Log Management

(Security Incident & Event Management)

Review all event and security logs from all covered devices to protect against advanced threats and to meet compliance requirements.

☐

Web Gateway Security

Internet security is a race against time. Cloud based security detects web and email threats as they emerge, and blocks them within seconds—before they reach the user.

☐

Mobile Device Security

Cyber criminals attempt to steal data or access your network by way of your employees' devices. They're counting on you to neglect this piece of the puzzle.

☐

Firewall

Turn on Intrusion Detection and Intrusion Prevention features. Send the log files to a managed SIEM.

☐

Encryption

Whenever possible, the goal is to encrypt files at rest, in motion (think email) and especially on mobile devices.

☐

Backup

Backup local. Backup to the cloud. Have an offline backup for each month of the year. Test your backups often.

Take a step to become more resilient against cybersecurity threats by signing up for our technology review or visit www.sharp-sbs.com/cybersecurity

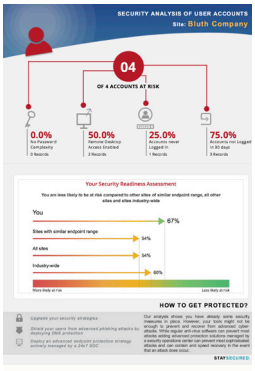
Is Your Company at Risk?

Uncover Vulnerabilities through a Network Risk Report

Nine out of 10 computer networks that we analyze have undetected problems that may lead to unauthorized access and costly interruption of business.

What's Included in the Network Risk Report

Our Risk Report is a 6 – 8 page executive summary that provides an overview of the devices on your network along with a network Risk Score and analysis of each potential issue. We will review this document with you and discuss our findings in detail. Our Sharp IT specialists can answer your questions and provide specific recommendations on how to: get more from your existing technology, identify weaknesses in your current network, increase mobility and much more.



Our process has many benefits, including:

- No software is installed, so no one—including your current IT provider—will be aware unless you want them to know
- Quickly scans your network in approximately 30 minutes (for an average, mid-sized network)

Areas we analyze	What we uncover
Hardware	- Servers, workstations, printers, and non-AD devices (like switches/routers/printers) - Old computers that are still joined to the domain and have not been removed
Software	- Systems with missing patches/service packs/security updates - Local accounts (per-system) with weak/insecure passwords - Systems with missing anti-virus, anti-spyware, or firewall misconfiguration
Configuration	- Inconsistent security policy across network servers/computers - Outbound system access that should be blocked - Lack of content filtering (social media, entertainment, pornography, illegal downloads)
Accessibility	- Misconfiguration of user access to network shares - Which users have Mailbox Delegate access (send on behalf of, access other mailboxes) - Membership to email distribution groups
Security Risks	- Old user accounts that still have access and have not been properly disabled - Internal systems with open ports that pose a potential security risk - External issues that put your network at risk of business disruption or data loss

Next Steps

There's absolutely no obligation to retain us, however if we do find a serious problem hiding on your network, you'll want to take prompt action to correct it. Our IT specialists will be ready to provide a quote, at your request, to help remedy the situation.

SHARP®