2023 Cybersecurity Essentials Checklist

Managed IT | Co-Managed IT | Cybersecurity

ANDERSON TECHNOLOGIES

A Handbook by Anderson Technologies, a St. Louis IT Company

info@andersontech.com | andersontech.com | 314.394.3001 | © 2023 Anderson Technologies

ANDERSON TECHNOLOGIES

2023 Cybersecurity Essentials Checklist

Do small businesses need to worry about cybersecurity?

These days, the answer is increasingly yes. In a world where normal individuals are frequently the target of malicious scams and attacks, small- and medium-sized businesses can present an even more appealing target.

The cost of ransomware or other cyberattacks to businesses is expected to exceed

$30B

in 2023 (Tech.co). According to IBM's 2023 Cost of Data Breach report, the average cost of a data breach is $4.5M, 15% higher than three years ago. For many businesses, a cyberattack at that scale can be fatal. Can you afford to ignore your cybersecurity protections?

Reducing your company's risk means knowing where you currently stand in terms of cybersecurity and knowing who to call if you discover a breach. When you assess your company's risk factors, evaluate the factors on the following pages.

ANDERSON TECHNOLOGIES

2023 Cybersecurity Essentials Checklist

Hardware

Understanding a company's hardware security needs can be a bit confusing for people who don't consider themselves "tech-y." Regardless of your technical knowledge, you should be able to identify your business's primary hardware devices.

Having the equipment is only one part of setting up your hardware. Enterprise-grade equipment must be installed and configured by an IT professional so your business can run safely without disturbing the day-to-day operations.

- [ ] **Can you identify your:**
  - [ ] **Hardware Firewall?**
  - [ ] **Router/Modem?**
  - [ ] **LAN Switch?**
- [ ] **Do you know if your hardware is properly configured to protect you now and as your business grows?**
- [ ] **Do you know what to do or who to call if there is a problem? Do your employees know?**

ANDERSON TECHNOLOGIES

2023 Cybersecurity Essentials Checklist

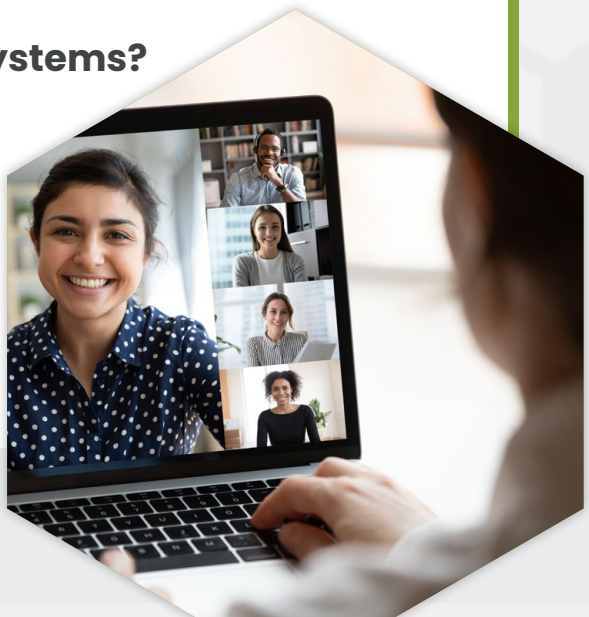
Software

Software solutions tend to be the most well-known "face" of cybersecurity. You're probably familiar with antivirus programs and email spam filters, but even these aren't "set it and forget it" solutions. Best practices for securing your small business include ensuring all workstations have the necessary software configured correctly.

Nothing invites bad actors into your systems like unpatched software, such as Windows 7, which stopped receiving updates after January 14, 2020. Security updates are not just slight improvements; they often fix known bugs and zero-day threats that bad actors can use to infiltrate or bypass the implemented security safeguards.

If you don't keep your software up to date, criminals can exploit unpatched vulnerabilities to breach your security. Once inside, they can install malware to watch you, prepare a larger attack, infect your network with ransomware, or extract valuable and private information from your systems. When an update appears, make sure that it gets installed right away, and upgrade unsupported software as soon as possible.

- [ ] **Do all your workstations have:**
  - [ ] **Updated Software and Operating Systems?**
  - [ ] **Antivirus/Malware?**
  - [ ] **Software Firewall?**
  - [ ] **Website Blacklisting?**
  - [ ] **Email Filters?**



ANDERSON TECHNOLOGIES

2023 Cybersecurity Essentials Checklist

Breach Readiness

Ransomware, data theft, and security breaches are only a few of the cybersecurity issues that businesses have to deal with. It's no longer a matter of **if** you will be attacked, but **when**. If you're not ready to address a breach as soon as it happens, your business could pay in money, data, and reputation.

- [ ] **Are all of your backups:**
  - [ ] **Properly configured?**
  - [ ] **Tested regularly?**
- [ ] **Are all user access controls:**
  - [ ] **Set to minimum necessary use?**
  - [ ] **Reviewed annually?**
  - [ ] **Revoked as soon as employees leave or are terminated?**
- [ ] **Are all your mobile devices and laptops encrypted?**
- [ ] **Do you use multi-factor authentication whenever available?**

ANDERSON TECHNOLOGIES

2023 Cybersecurity Essentials Checklist

Everyday Security Measures

Password policy and management is especially important for small businesses, because it's a security measure that everyone deals with on a regular basis. If your employees are rotating through a handful of passwords that they use everywhere, that puts your business at risk. Give them the support they need to have secure passwords.

- [ ] **Do all user access controls:**
  - [ ] **Require a minimum of 12 characters?**
  - [ ] **Not allow password re-use?**
  - [ ] **Encourage random alpha-numeric passwords?**
  - [ ] **Require default passwords to be changed on a regular basis?**
- [ ] **Are employees required to use password managers?**
- [ ] **Do you use multi-factor authentication whenever available?**

ANDERSON TECHNOLOGIES

2023 Cybersecurity Essentials Checklist

This leads us to a final—often overlooked but extremely critical—security measure:

Employee Cybersecurity Training

In the last year, 74% of breaches involved a human element (Verizon). Teaching your employees how to spot phishing emails, the importance of password security, and the real threat of social engineering can go a long way toward protecting your business. But employee training isn't a one-time meeting.

Train and test employees continuously.

Wondering whether your business could benefit from managed IT services?

If you answered no to any of these questions—or didn't know the answer, or weren't sure why the question mattered—having access to a team of experienced IT professionals could be exactly what you need.

Anderson Technologies has been helping St. Louis businesses handle their IT needs for over 20 years. We know that running a small business means your needs are constantly changing. If you'd like to learn more about what we can do for your business, give us a call for an IT Infrastructure Audit.

Managed IT | Co-Managed IT | Cybersecurity