Keeping Your Business Secure in an Unsecure World

A STRATEGIC GUIDE SPECIFICALLY FOR WEST MICHIGAN BUSINESSES

Macatawa TECHNOLOGIES | IT Solutions & Support For Business

If you're not with a managed services provider who is proactively protecting you, your security is in your own hands.

And that's where things could go wrong.

Security threats no longer just target large businesses, they're going after small enterprises. You need to know how to protect your company.

We put together this guide to offer our first-hand expertise working with businesses in Holland, Grand Rapids and throughout the rest of West Michigan to help you make the best security moves – both tactical and strategic – and keep your business safe.

Security isn't something you can set and forget. It's a process. And it starts here.

Table of Contents

8 Signs Your Company Has Security Issues

8 **You rely only on antivirus and firewalls.** These two elements are critical to securing your organization's technology, but they are not enough, especially if they are not consistently monitored and updated.

7 **You have no IT budget and spend only as needed.** To be secure, IT needs to be proactive and planned for through a budget. There are many components you don't know you need until a crisis.

6 **You have no IT provider.** Without a dedicated team of IT experts keeping you secure, your IT is likely exposed to risks you don't know about.

5 **IT provider lacks best practices.** Ask your provider to explain their technology standards and security measures to you and why they are important.

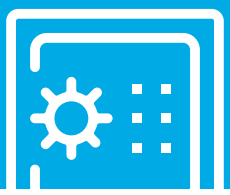
4 **You have no plan for disaster.** When disaster strikes, what happens? Your provider should restore your network quickly and seamlessly, with no data loss and minimal downtime. Test your plan and make sure it works.

3 **Your users aren't trained.** Your users are typically the frontline of defense against ransomware and phishing. If they don't have ongoing education, they're a poor defender.

2 **Employees use their personal devices on your network.** Unsecure devices can expose your networks to a number of threats, especially without any safeguards in place.

1 **You have no network security plan.** Consider this the top security gap. If you have no awareness or strategy to manage your security, you might already be infected.

The True Cost of Not Securing Data



Some businesses don't use security tools because they believe it's more cost effective to take the chances and pay to fix the servers or restore the data if something takes their systems down.

But the cost of repair or data recovery is not the true cost of being unsecure. In fact, whether you get hit by ransomware, disaster or just have equipment go belly up, the costs are much higher than you think.

HERE'S A POTENTIAL SCENARIO

You get hit by ransomware and it impacts half your network. Without backups, you are dead in the water until the ransomware is cleaned off each end point and server impacted, and data is restored. This can take several days.

Direct cost of recovery. These are the hourly costs you pay to your IT provider (if you're not on a monthly service contract), and can be up to thousands of dollars. **$2,500** is reasonable.

Lost productivity. When networks are compromised or corrupted, people can't work. If your daily payroll is $4,000 and 50% of your staff can't work for 2 days, you're out another **$4,000**.

Missed opportunities. An outage like this will have a negative impact on your daily revenue. If your daily revenue is $5,000, then 2 days of an outage can easily take **$10,000**.

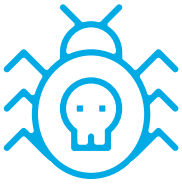
In this scenario, ransomware cost your company $16,500.

There are indirect impacts on the bottom line as well, such as the loss of reputation and missed opportunities. While unquantifiable, they have a major impact.

PRO TIP

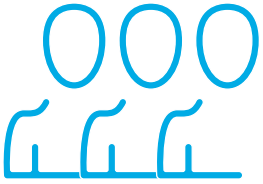
If you get ransomware, don't pay the ransom. There are no guarantees your data will be returned and many ransomware strains will lay dormant on your systems, striking again and again.

The Top Threats to Your Business



Ransomware.
This refers to a broad (and growing) class of malware that encrypts files and requires the user to pay a ransom anywhere from $500 to a few thousand. It brings businesses to a halt.

Why you should worry:
It's in the news and on every business owner's mind for good reason: ransomware is not just targeting the big players, it targets everyone and is not something your antivirus is going to catch or prevent.



Man in the middle attack.
This type of attack is where a hacker essentially gets in the middle of your business infiltrating processes without detection. For instance, they can send emails requesting money to clients and delete those sent emails.

Why you should worry:
If someone gains access to your network at this level, they can act as an employee and there is nothing really stopping them. It can damage your reputation and break trust with your clients.

Social engineering.
Similar to a man in the middle attack, social engineering allows a hacker to pose as a high-ranking person in your company. This is often done to set up a wire transfer or gain access to financial information.

Why you should worry:
These attacks specifically target small businesses because criminals know that they have fewer authentication practices in place.

REAL LIFE STORY

A scammer sent an email to a company's controller pretending to be the business owner with a request to wire money to their bank account. The controller was at the bank making the wire transfer when the business owner called the controller about something unrelated – and the transfer was just barely averted!

LESSON: Security is about more than just technology, it's also about good policies and procedures. This client now requires all wire transfers be in writing and confirmed by a phone call.

5 Cost-Effective Tactics to Reduce Risk

IT security is not a single event or application. It's an ongoing, multilayered approach, both tactically and strategically. You can't set up a firewall and forget it.

START HERE →

Get a security assessment so you know exactly where your weaknesses are. You can address the most critical vulnerabilities first.

1. **Automate patch updates.** All of your software on every device needs to dial home and check for updates at least weekly. Configure these updates to be installed automatically.

2. **Keep your antivirus up to date.** If your antivirus is not receiving up-to-date definitions, it's no longer serving you. Definition updates need to happen as often as you can set them.

3. **Check your firewall.** If your firewall is more than 3 years old, it may be doing very little to protect you. Your firewall needs to keep up with the changing threat landscape.

4. **Use the right backups.** Your backup model needs to be foolproof – and tested on a regular basis. No matter what happens, the ability to retrieve data depends on the quality of your backups.

5. **Use two-factor authentication.** For sensitive data and financials, single-factor authentication might not be enough.

PRO TIP

Use a managed services provider who is looking out for your best interests. That means they make the most cost-effective, tactical recommendations and implement them as part of your IT.

Security Strategy Checklist for SMBs

Security starts with the right strategy. Review these essential strategic IT best practices.

☑ Check off the ones you're currently doing.

PLANS AND POLICIES

- [ ] **Acceptable use policy.** Define how users are permitted to use the company network, computer devices and other technology. For example, prohibit certain websites.
- [ ] **Disaster recovery plan.** When disaster strikes, how will your company recover and how will your data be protected and restored? Have a plan – and put it into action.
- [ ] **Bring your own device policy.** Employees use personal devices for company data and email – put safeguards in place to protect your company.
- [ ] **Password policy.** Insist that passwords meet a bare minimum of complexity and have employees use password management tools to secure passwords.
- [ ] **Turn incidents into policies.** Things happen. Turn security incidents into policies and education opportunities for the whole company.
- [ ] **Train users.** When users know what to consider suspicious and how to handle incoming threats, it can go a long way toward protecting your company.

STRATEGICALLY MANAGE IT

- [ ] **Do an annual review.** Once a year, review your security policies and procedures to ensure they align with best practices.
- [ ] **Be proactive year-round.** Standards are constantly changing and evolving. Constantly evaluate your infrastructure to make sure you're up to speed.
- [ ] **Refresh equipment.** Older equipment is prone to failure, data loss, data corruption or exposure to threats. Replace servers every 5 years and laptops/PCs every 3-5 years.
- [ ] **Use a Managed Services Provider that is strategic and tactical.** Not all MSPs are the same. Macatawa Technologies offers everything from policy development to technical implementation.

6 Questions for Your IT Provider

Many companies find out the hard way that they are not secure.

Ask your IT provider these 6 questions to make sure that you're covered:

1 **What kind of security software is installed on our networks and devices?**
What to expect: At a minimum, you should have antivirus, firewalls, patch management and spam filters.

Their answer:

2 **How often are our backups verified?**
What to expect: They review logs daily, do monthly chain verification and are testing annually at a minimum.

Their answer:

3 **What would happen if we got hit with ransomware? How much extra would that cost?**
What to expect: They can restore your data and systems quickly and remove the ransomware from your networks. It should be included in your service plan.

Their answer:

4 **Can you share what you're doing for remote monitoring and maintenance of systems?**
What to expect: They're proactively monitoring systems for signs of trouble and updating software patches at least weekly.

Their answer:

5 **How often is security software updated?**
What to expect: Antivirus definitions being updated as close to real time as possible. Firewall configurations checked regularly.

Their answer:

6 **How often is your technology being reviewed by a vCIO or account manager?**
What to expect: At least once per quarter.

Their answer:

PRO TIP

Ultimately, you want a managed IT provider who is PROACTIVELY looking out for your best interests and offers affordable solutions to meet your needs.

Conclusion

Just like you can't eat a bag of carrots and expect to have lifelong health and vitality, you can't install an antivirus once and expect your networks to be secure.

Small businesses are not immune to threats and security pitfalls. In fact, you might be more vulnerable if you're managing things yourself. By using the tools contained in this guide, you have the power to reshape the way you look at security and technology and protect your business.

FINAL TAKEAWAY

Security is an ongoing, ever-changing process that you need to integrate into your business planning and expenses because it's not going away. Consider it the cost of doing business in the 21st century.

ABOUT MACATAWA TECHNOLOGIES

Macatawa Technologies has served West Michigan since 2002 providing a full suite of IT Support including technical helpdesk support, computer support, and consulting to small- and medium-sized businesses. Our goal is to provide enterprise-level IT practices and solutions to the small business sector with small business prices. Our experience has allowed us to build and develop the infrastructure needed to keep our prices affordable and our clients up and running.

Our dedicated staff loves seeing our clients succeed. We partner with many types of businesses in the area and strive to eliminate IT issues before they cause expensive downtime, so you can continue to drive your business forward. Your success is our success, and as you grow, we grow.

MAKE SURE YOUR COMPANY IS SECURE.

Contact us for an assessment online or (616) 394-4940

Macatawa TECHNOLOGIES