INTELLIGENT
TECHNICAL SOLUTIONS

FROM RISK TO RESILIENCE:

Warning Signs Your Business Needs Better Cybersecurity

Table of Contents

Introduction

Maintaining a strong cybersecurity posture for your organization isn't easy. With all the day-to-day tasks, deadlines, and demands, it's easy to understand why security would often get pushed to the back burner. It's because you have to do this balancing act, where you have to try and keep your network secure while staying on top of your operations.

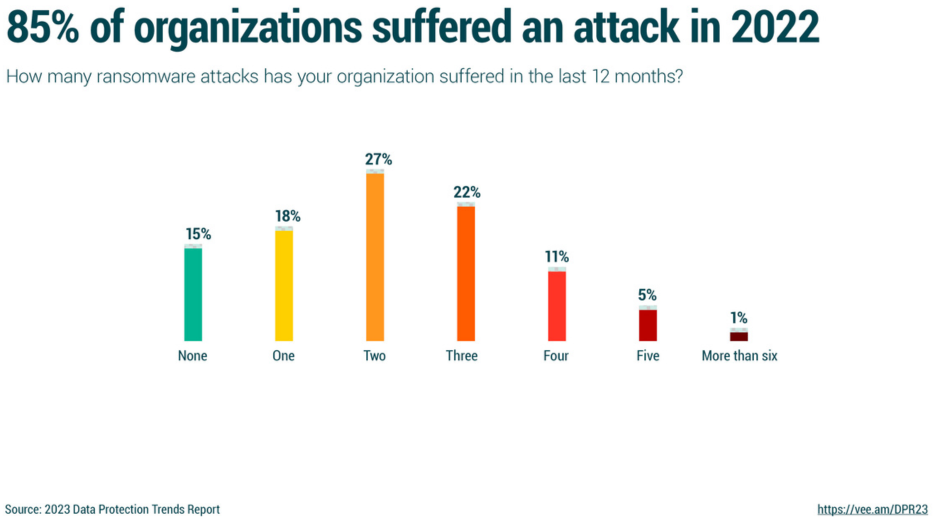
What tips the scales against cybersecurity, however, is that it can be a very complex topic. It's often hard to understand what you need to do to build your defenses. In fact, you might not even be aware that your network is vulnerable despite your best efforts. Unfortunately, that's exactly what cybercriminals are looking for. They seek businesses that don't know any better because it makes their job easier.

Intelligent Technical Solutions (ITS) is a managed security service provider (MSSP) that has helped hundreds of businesses improve their cybersecurity efforts for almost 20 years. In this comprehensive guide, we'll help you understand why cybersecurity is important, as well as the risks of not practicing it. We'll also dive into the signs that your business has weak cybersecurity and how you should address it.

Why It's Important to Put a Bigger Focus on Cybersecurity

The bare minimum security just doesn't cut it anymore. Cyber threats have grown more sophisticated in the last few years, and it's not showing any signs of slowing down.

According to the 2023 Data Protection Trends Report by Veeam, 85% of organizations surveyed suffered at least one cyber attack in the last twelve months. This is a 76% increase from the previous year.



Source: 2023 Data Protection Trends Report https://vee.am/DPR23

More Attacks Than 2022 (source: Veeam)

What does this mean for your business?

It means the question is no longer if a cyberattack will happen to you - but when. You can no longer just wait for a threat to pop up before you act on them; you need to hunt for them proactively. Otherwise, it will be too late, and your business will suffer the consequences.

We understand the desire to just let your team focus on tasks like growing the business. You don't have a lot of resources to spare. But you have to understand that you're putting your entire business at risk without adequate security measures. Shifting your focus to a security-first mindset is crucial for the long-term sustainability of your organization. It's vital if you want to survive in today's digital world.

What are the Risks of Having Weak Cybersecurity?

Poor cybersecurity practices can expose your business to various risks and potential consequences, such as:

Data Breaches

Inadequate cybersecurity practices can make businesses vulnerable to data breaches, where sensitive information is accessed, stolen, or exposed. This can result in financial loss, reputational damage, legal implications, and regulatory penalties.

Malware Infections

Failing to maintain proper cybersecurity measures can lead to malware infections, such as viruses, ransomware, or spyware. These malicious programs can disrupt operations, compromise data integrity, and extort businesses for financial gain.

Unauthorized Access

Weak or reused passwords, lack of multi-factor authentication, and improper access controls create opportunities for unauthorized individuals to gain access to critical systems and sensitive data. This can lead to data manipulation, theft, or unauthorized actions.

Financial Loss

Cybersecurity incidents can result in financial loss through various means, including ransom payments to regain access to encrypted data, recovery costs to restore systems and data, legal fees, regulatory fines, and loss of business due to reputational damage.

Damage to Reputation

Poor cyber hygiene can damage a business's reputation, erode customer trust, and lead to loss of clients or contracts. News of a data breach or cyber incident can spread quickly, impacting brand image and customer perception.

Business Disruption

Cybersecurity incidents can cause significant disruptions to business operations. Downtime, system failures, or loss of critical data can result in productivity loss, missed deadlines, dissatisfied customers, and potential financial ramifications.

Legal and Regulatory Consequences

Non-compliance with data protection regulations, such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA), can result in legal consequences and substantial fines. Failure to implement adequate security measures and protect customer data can lead to regulatory investigations and legal actions.

Intellectual Property Theft

Insufficient security practices can make businesses vulnerable to intellectual property theft, where proprietary information, trade secrets, or innovations are stolen. This can have long-term negative effects on competitiveness and market position.

Business Email Compromise (BEC)

Poor cyber hygiene practices can expose businesses to BEC attacks, where cybercriminals impersonate company executives or partners to deceive employees into making unauthorized financial transactions. This can result in significant financial losses.

Supply Chain Risks

Weak cybersecurity practices in one organization can also introduce risks to its supply chain partners, potentially leading to a chain reaction of cyber incidents affecting multiple businesses.

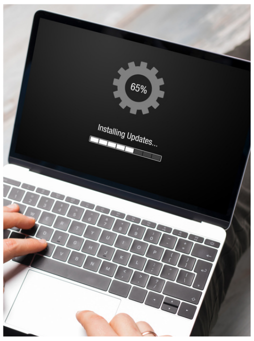
By understanding and addressing these risks through robust cybersecurity practices, businesses can significantly reduce their vulnerability to cyber threats and protect their valuable assets, operations, and reputation.

5 Warning Signs That Your Business Has Weak Cybersecurity

It's not always easy to know what your weaknesses are, but that doesn't mean they're not there. In fact, you might not even realize that your business is riddled with vulnerabilities until it's too late. Thankfully, there are ways to tell whether you need to up your cybersecurity efforts. Here are the five signs that your business has weak security:

1. Your Software is Outdated

When software is outdated, it often means that important security patches and updates haven't been applied. It's like having a lock on your door that can easily be picked because you haven't upgraded it to the latest, more secure version. It can leave your systems exposed to known vulnerabilities, making it easier for hackers to infiltrate and compromise your data or launch malicious activities.



2. You Have Poor Password Habits

Is anyone on your team using their birthdate as a password, maybe an anniversary, or the name of their dog? That's a sign of poor password habits. All of that information could easily be found online on social media or other platforms. Cybercriminals know that and will exploit it to gain access to your systems.

On the other hand, you might be using a complex password of randomized characters and numbers. While that might sound great, it's also likely some members of your team have their password written down on a sticky note on their desk because they can't remember it. And that's also an example of poor cyber hygiene. A random person can simply walk inside your office and see the password.

Related: Making the Best Password: Tips, Tricks, and Common Mistakes

3. You Have Experienced a Breach Before

If your business has experienced any form of data breach in the past few years, you should know that you're still being targeted. Many business owners mistakenly believe that getting through one incident means they'll be safe for a while. The criminals have already taken what they can from your business; what more could they want?

Sadly, that's not the case. Cybercriminals always come back to previous victims. You've already shown the chink in your armor, and they already have a playbook to follow from the first attack. They could have even left themselves a backdoor to your systems to make their return visit much easier. In other words, your business is a low-hanging fruit.

So, if you've ever experienced an attack or security incident before, it's high time to update your defenses.

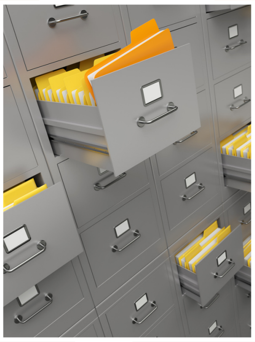
4. You're Struggling with Compliance

Compliance issues are another sign of poor cyber hygiene because they suggest a lack of adherence to established standards and regulations. They often indicate that your organization has inadequate security practices, such as weak access controls, improper data handling procedures, or insufficient safeguards against cyber threats.

It might be tempting to think that some compliance issues aren't your fault, that it's just that the standards are too high. Unfortunately, cybercrime has grown more sophisticated over the years. Old standards are no longer a match against the new wave of modern cyber-attacks. That means if you neglect to prioritize and maintain compliance, you're actually endangering your business.

5. Anyone on Your Team Can Access Sensitive Information

Who can access your critical data? If you answer everyone connected to your network, that indicates that you lack controls for handling sensitive information. That means a would-be hacker only needs to penetrate one device to gain access to the keys to your kingdom.



Ways to Strengthen Cybersecurity for Your Business

These are the most effective ways to help your organization improve your cybersecurity efforts:

Change Your Mindset

When it comes to cybersecurity, it's vital to shift from a reactive to a proactive approach. The consequences of a breach are too great to leave it all up to chance. That's why you need to ensure that you find threats before they pose any danger to your business.

Get a Third-Party Security Assessment

It's not easy to see gaps in your own defenses. Getting a third party to conduct a security assessment will help you see vulnerabilities that you might not have even thought about. They will try to poke holes in your security, so you can find where your weak points are.

Educate Your Team

You can have the best cybersecurity solutions available in the world, but if you don't educate your team, it could still leave you open for an attack. According to the 2022 Global Risks Report released by the World Economic Forum, 95% of breaches experienced by businesses occurred due to human error. That's why ensuring your team has proper awareness and training can significantly help improve your cybersecurity posture.

Implement Strict Password Management and Multi-Factor Authentication (MFA)

Having a strict password management policy in place can help ensure that your team isn't being careless with their passwords. However, you should also consider implementing MFA. It's a highly effective, low-cost method to protect against password-related attacks. That means it could prevent cybercriminals from getting into your network even if they do get a password to one of your accounts.

Install Patches Regularly

Ensuring that all your software is up-to-date not only allows you access to new features but will help improve your security efforts. Often, software updates include removing bugs and repairing security holes that have been discovered.

Unfortunately, doing this regularly is easier said than done. Depending on the number of devices you have and the number of software you use, it could be difficult to track everything. That's why, when possible, try to automate the process or reach out for help from managed IT companies.

Use Access Controls and Encryption When Handling Sensitive Data

Ensure that you control who gets access to sensitive information within your organization. It adds layers to your security that will make it very difficult for cybercriminals to move around within your network. In addition, encrypt your data so that it doesn't get intercepted easily when you're handling them.

Get Help from Experts

Hire an MSSP to help with your overall cybersecurity efforts. Managed cybersecurity services will help you maintain your cybersecurity by taking care of all the nitty-gritty security stuff you might not have the time or expertise for. A managed cybersecurity provider will monitor your network, keep an eye out for any suspicious activities or threats, and make sure your security measures are up to the task.

With an MSSP on your side, you can focus on running your business while they handle the heavy lifting of building you a solid defense against cyber-attacks. Not to mention, they can also help you meet and maintain your compliance goals.

Need Help Strengthening Your Cybersecurity?

It's crucial to spot the warning signs of weak cybersecurity because it allows you to address your vulnerabilities so you can strengthen your defenses. Finding out you have weak spots when a security incident occurs is already too late, given the risks and consequences of a successful attack. Thankfully, this book helps you identify whether your security efforts need improvement.

ITS has helped hundreds of businesses build and bolster their cyber defenses. If you need help checking your network for vulnerabilities, schedule a free IT security assessment with one of our experts.

INTELLIGENT
TECHNICAL SOLUTIONS

Schedule a FREE Assessment with our Cybersecurity Experts!

www.itsasap.com
(855) 204-8823

Chicago | Detroit | Las Vegas | Los Angeles |
Oakland | Olympia | Phoenix | Portland | Reno |
Sacramento | San Francisco