përvojë digital
Strategy • Innovation • Transformation

in partnership with

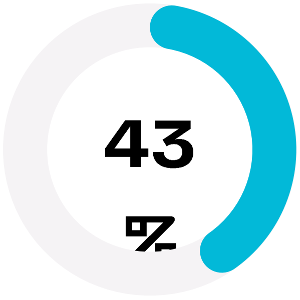
DIGITAL GUARD SOLUTIONS

CYBERSECURITY BEST PRACTICES FOR SMALL BUSINESS OWNERS

Why Cybersecurity Is Non-Negotiable for Small Businesses

Hello, intrepid business owners and aspiring moguls! Welcome to the ultimate guide that you didn't know you needed but absolutely do—navigating the tricky waters of cybersecurity for small businesses.

Guess what? It's not just the corporate giants who need to worry about hackers and data breaches. If you're running a small business, you've got a target on your back, too.



Did you know that **43%** of cyber-attacks are aimed at small businesses, but only **14%** are prepared to defend themselves? Yikes! That's like going into a boxing ring blindfolded.

Wild West of Cybersecurity

Hold onto your hats, because the cyberworld is more like the Wild West. From ransomware attacks that can lock you out of your own systems to phishing schemes that trick your employees into giving away sensitive info, the threats are numerous and evolving. Even scarier? COVID-19 has accelerated the frequency of cyber-attacks as more businesses go remote..

You might think, "Why would hackers care about my small business?" Well, your size makes you an easy target, and the data you hold is a goldmine for cybercriminals. Trust us; you don’t want to be low-hanging fruit. And it's not just about financial loss. A cyber-attack can erode your customers' trust and take a wrecking ball to your reputation.

Let's get real. Failing to prepare is essentially rolling out the red carpet for cybercriminals. The aftermath? Downtime, loss of customer data, hefty fines, and potentially, the complete collapse of your business. According to Cybersecurity Ventures, damage related to cybercrime is projected to hit $6 trillion annually by 2021. Trust us; you don’t want to contribute to that statistic.

So, as you flip through the pages of this ebook, remember: Cybersecurity is no longer optional—it's a necessity. We’ve prepared a comprehensive guide that covers everything from identifying risks and creating policies to best practices and team training. Plus, we’ve thrown in checklists and worksheets to make your journey as smooth as possible. Ready to become a cybersecurity champ? Let’s dive in!

Why Cybersecurity Matters

Hey folks, you're here because you've got a dream, a vision, and a business to run! But here's the deal: Even if your business isn't as big as Apple or Amazon, you're still a target for cyber criminals. Yep, you read that right! Cybersecurity is like the underappreciated superhero of the small business world. Let's dive into why it's not just a concern, but a necessity.

Current Threats

Phishing Scams

Raise your hand if you've gotten a weird email asking for sensitive information. Phishing is one of the oldest tricks in the cyber criminal's book.

Why You Should Care?
32% of all breaches involve phishing attacks.

Ransomware

Think kidnappers, but for your data. Once they've got your data, you'll have to pay a ransom to get it back.

Why You Should Care?
There's a ransomware attack every **14 seconds**. Could you be next?

Insider Threats

Yes, sometimes the enemy is within. Disgruntled employees or careless team members can expose vulnerabilities.

$11.45 MILLION

Why You Should Care?
Insider incidents cost companies an average of **$11.45 million** annually.

Future Threats

AI-Powered Attacks

Imagine a cyber attack, but on steroids. That's what artificial intelligence can offer to hackers.

Why You Should Care?
AI can automate hacking attempts, making it easier for cyber criminals to launch large-scale attacks.

Internet of Things (IoT) Vulnerabilities

As more devices connect to the Internet, more vulnerabilities are exposed.

41 BILLION

Why You Should Care?
By 2025, there will be over **41 billion** IoT devices. Each is a potential entry point for hackers.

Supply Chain Attacks

This involves hacking one business to get to another. Even if you're secure, what about your vendors?

Why You Should Care?
60% of small businesses go out of business within six months of a cyber attack, and supply chain attacks are on the rise.

Key Cybersecurity Threat Statistics

43%

of cyber attacks target small businesses.

$200,000

The average cost of a data breach for small businesses is $200,000.

19%

Reduction Chum

So, Why Does All of This Matter?

It's simple: your business, your livelihood, and your reputation are on the line. With the digital world only expanding, cyber threats are evolving faster than you can say "data breach." Getting ahead of this is not just smart; it's survival.

Identifying Risks

Hello, detectives! Grab your magnifying glasses because it's time to hunt down those pesky cybersecurity risks lurking around your business. Before you even think about solutions, you've got to know what problems you're solving, right?

Types of Risks

Data Leaks

Confidential customer data or company secrets could be exposed, either accidentally or intentionally.

Malware Attacks

Software specifically designed to disrupt, damage, or gain unauthorized access to your computer system.

Unsecured Networks

Using unsecured Wi-Fi networks opens up a world of risks, including the potential interception of data.

Outdated Software

Using outdated software can leave you exposed to vulnerabilities that have been patched in newer versions.

Risk Assessment Worksheet

You've got to treat your business like a fortress, and every fortress has weak points. Time to find yours!

01 What kind of data do you store?

- Customer Information
- Employee Records
- Financial Data

02 Who has access to this data?

- Full-time Employees
- Part-time Staff
- Third-party Vendors

03 What security measures are currently in place?

- Firewall
- Encrypted Data
- Regular Software Updates

04 What's your current backup strategy?

- Cloud Storage
- Physical Servers
- Frequency of Backups

Creating a Cybersecurity Policy

Alright, game-planners! Once you've identified your risks, it's time to create your cybersecurity playbook. This isn't just another document to file away and forget; it's your go-to guide for keeping your business safe.

Key Elements of a Cybersecurity Policy

Scope and Purpose

What does the policy cover? Is it for internal use, external partnerships, or both?

Definitions

What does the policy cover? Is it for internal use, external partnerships, or both?

Roles and Responsibilities

Who is responsible for what? Is there a designated "security guru" in your team?

Security Protocols

List out step-by-step procedures for different scenarios like a data breach, unauthorized access, or lost devices.

Security Protocols

How will you train your team? Will you do regular updates and drills?

Cybersecurity Policy Worksheet

01 Scope of Policy

- Outline what areas your policy will cover.

02 Key Definitions

- Write down essential terms and their meanings.

03 Roles and Responsibilities

- Assign roles to team members.

04 Protocols and Procedures

- Document what needs to be done in case of different types of cyber incidents.

05 Review and Update Frequency

- Decide how often your policy will be reviewed and updated.

Best Practices

Welcome to the nitty-gritty, friends! This is where we roll up our sleeves and get into the action items that will make your business a cybersecurity fortress.

Password Management

Passwords are like toothbrushes: don't share them, and change them often. They're like the keys to your online kingdom. Make 'em strong, unique, and don't write them down on sticky notes!

Tips: 1

- Use a passphrase instead of a word. E.g., "BlueSky$RainyDay!"

Tips: 2 Password Manager Checklist:

- At least 12 characters
- Mix of letters, numbers, and symbols
- Avoid personal info like birthdays

Password Manager Checklist

□ Research and select a trustworthy password manager.

□ Import existing passwords.

□ Enable password auto-update features.

Two-Factor Authentication (2FA)

Take security to the next level! 2FA is your second line of defense if someone tries to break into your accounts.

Tip: 3 - 2FA Checklist

□ Enable 2FA on all mission-critical accounts (email, bank accounts, etc.).

□ Test 2FA to ensure it's working correctly.

□ Inform team members to do the same

Firewalls

Picture firewalls as the moats around your digital castle. They keep the bad guys out!

Firewall Best Practices

- Use both hardware and software firewalls for double protection.
- Regularly update and maintain them

Firewall Checklist

□ Set up a hardware firewall for your business network.

□ Install software firewalls on individual devices.

Updates and Patches

Updates are like vitamins for your software: they keep things running smoothly and securely.

□ Enable automatic updates where possible.

□ Schedule monthly checks for firmware and software that require manual updating.

Antivirus (AV)

Antivirus software is your digital bodyguard. It scans your systems for malware, viruses, and other nasty stuff that could compromise your data. If your computers are the lifeblood of your business, then antivirus is the white blood cell army fighting off infections.

AV Checklist

□ Verify system compatibility. Make sure the antivirus you choose is compatible with your operating system and hardware.

□ Choose software with real-time scanning. Select a solution that offers real-time scanning. This ensures that files are checked as they are created, opened, or executed.

□ Read at least 5-10 reviews before making a selection. Read reviews from trusted sources and look at customer ratings to gauge effectiveness and customer satisfaction.

VPN Applications

A Virtual Private Network (VPN) provides a secure tunnel for your data to travel through, keeping it safe from hackers and snoops. Imagine sending all your business letters through a pneumatic tube that only you and the receiver can access. That's what a VPN does for our digital communications.

VPN Checklist

□ Assess bandwidth requirements. Some VPNs restrict the amount of data you can use. Ensure the one you choose can handle your business needs

□ Review the number and locations of servers. The more server locations, the better. This offers more choices for routing your traffic, which can help with speed and reliability.

□ Trial the software for user-friendliness. If it's complicated, you're less likely to use it. Find a VPN that's user-friendly.

Training Your Team

Okay, leaders, let’s get your team into cybersecurity shape! A well-trained team is your first and best line of defense against cyber threats.

Create Awareness

Before diving into protocols, make sure your team knows the stakes.

- Share statistics on cyber threats targeting small businesses.
- Discuss real-life case studies or news about recent breaches.

Training Modules

Consider implementing a series of training modules that cover:

- Identifying phishing emails
- Securely managing data
- Properly using the company’s network and devices

TIP - Training Checklist

□ Create or purchase cybersecurity training modules.

□ Schedule quarterly training sessions.

Simulation Drills

Put your team to the test with simulated cybersecurity incidents.

- Phishing email tests
- Password cracking attempts

Ongoing Training and Updates

Cybersecurity is an ever-evolving field, so regular updates and refresher courses are a must.

TIP - Ongoing Training Checklist:

□ Plan semi-annual refresher courses.

□ Send out monthly cybersecurity updates and tips via email or internal communications.

Backup, Backup, Backup

Hey, have you ever lost a term paper or a super-important presentation? Frustrating, right? Now, imagine losing all your business data. Yeah, we don't want that. Backups are your business's lifebuoy!

Types of Backups

- **Local Backups**

Save your data on physical devices like external hard drives. Easy access, but if the building's in trouble, so is your data.

- **Cloud Backups**

Data is stored offsite, often in multiple locations. Safer, but you'll need a good internet connection to access it.

- **Hybrid Solutions**

Why not both? Use local backups for quick access and cloud backups for disaster recovery.

Backup Best Practices

Frequency: The more often, the better. Daily is ideal.
Encryption: Always encrypt your backup files.
Testing: Regularly test to make sure your backups can be restored.

TiP - Backup Checklist

□ Decide the types of backups you'll use.

□ Schedule automatic backups.

□ Regularly test backup restoration.

Monitoring and Auditing

Welcome to the watchtower, folks! Monitoring and auditing are like your cybersecurity CCTV cameras. They help you spot when something's fishy.

Monitoring

- **Real-Time Monitoring**

Software tools can alert you instantly about suspicious activities. If someone tries to access sensitive data, you'll know.

- **Logs**

A record of activities that take place on your network and systems. Logs are your go-to for post-incident investigations.

Auditing

- **Internal Audits**

Conducted by your own IT team or an internal audit group. Good for a general health check.

- **External Audits**

Conducted by third-party professionals. They'll provide an unbiased review of your cybersecurity posture.

Backup, Backup, Backup

Monitoring and Auditing Best Practices

Regular Checks:
Consistently review system logs and real-time monitoring dashboards.

Access Control:
Limit who can review sensitive logs and audit reports.

Documentation:
Keep records of all audits and relevant findings for accountability.

TiP - Monitoring and Auditing Checklist

□ Select real-time monitoring software.

□ Schedule regular internal and external audits.

□ Define the process for documenting and responding to incidents.