



# SMALL BUSINESS, BIG TARGET

WHY CYBERCRIMINALS LOVE SMALL BUSINESSES—  
AND WHAT YOU CAN DO TO STOP THEM



[www.it21st.com](http://www.it21st.com)

(855) 4-IT21ST or 855-448-2178

[info@it21st.com](mailto:info@it21st.com)

10880 Wilshire Blvd, Suite 1101  
Los Angeles, CA 90024

2945 Townsgate Road, #200  
Westlake Village, CA 91361

## Table of Contents

<b>Chapter 1: The Cybercrime Landscape. The New Reality for Small Businesses .....</b>	<b>5</b>
The Different Faces of Cybercrime .....	5
The Cost of a Breach .....	6
Cybercrime is Becoming Increasingly Sophisticated.....	6
Why Are Small Businesses Attractive Targets? .....	7
♦ Checklist: Are you a target? .....	8
<b>Chapter 2: The Cost of Ignoring Cybersecurity .....</b>	<b>9</b>
The Hidden Danger of "It Won't Happen to Us" .....	9
The Financial Fallout .....	9
Direct Costs .....	9
Indirect Costs .....	9
The Reputational Ripple Effect .....	10
Legal and Compliance Consequences .....	10
The Emotional and Human Impact .....	11
The Myth of "Too Expensive" .....	11
<b>Chapter 3: Human Error as the Weakest Link. Why human error is the number target 12</b>	
Common Human Errors that Can Lead to Breaches.....	12
The Psychological Factors of Human Error .....	14
How to Turn Your Staff Into Your First Line of Defense .....	14
Case Study - The Mistake that Led to the Lesson Learned .....	15
♦ Quick Checklist: Improve your Human Firewall.....	16
<b>Chapter 4: Laying the Right Foundation – Cybersecurity Basics Why Basics are More Important than Technology .....</b>	<b>17</b>
Firewalls – Your first guard. ....	17
Antivirus and Endpoint Security .....	17
Strong Passwords and Multi-Factor Authentication (MFA) .....	18
Data Backups – Your Business Best Friend .....	18
Software Updates and Patch Management .....	19
Email Security Tools .....	19
Don't Forget About Physical Security .....	19

Cybersecurity Awareness Culture .....	20
<b>Chapter 5. Protecting your Crown Jewels – Data and Devices. ....</b>	<b>22</b>
What are your Crown Jewels?.....	22
How to Protect your data and devices.....	22
Data Encryption .....	22
Device Security .....	22
Access Control.....	22
Regular Backups .....	23
Encrypting Email/files .....	23
Case Study: The Stolen Laptop .....	23
<b>Chapter 6: The Ransomware Epidemic .....</b>	<b>24</b>
Ransomware: The Fastest Growing Threat .....	24
How Ransomware Works.....	24
Why are Small Businesses Ideal Victims? .....	24
Real World Example .....	24
<b>Chapter 7: Cloud Security - Safe in the Sky Second Misconception: The Cloud.....</b>	<b>25</b>
Cloud Risks .....	26
<b>Chapter 8: The Cybersecurity Roadmap - From Reactive to Proactive .....</b>	<b>27</b>
The Problem with Being Reactive.....	27
The Roadmap Steps.....	27
Case Study .....	27
Compliance is not optional.....	28
Why Trust Matters .....	28
A few compliance quick wins: .....	28
Shifting the Narrative.....	28
Real-Life Example.....	28
<b>Conclusion – Don't be the easy-target! .....</b>	<b>29</b>
<b>Appendix: 10 Things To Do Now To Build Your Cybersecurity .....</b>	<b>30</b>
<b>Resources Section .....</b>	<b>30</b>

# INTRODUCTION

I decided to write this eBook to help Small Business to understand that Cybersecurity is for any size business and not only big companies. Organizations of every size should be taking cybersecurity seriously.

Large companies usually have resources; teams; and infrastructure committed to ensuring that they are protected against these cyber threats, while small businesses often have little (on budget, staffing, access to sophisticated tools, etc.) to no possibilities in maintaining similar protection. These limitations, combined with I have common cyber-focused knowledge and understanding of vulnerabilities, make a small business (especially a very small business!) a much easier target for cybercriminals. With the right knowledge and information, we are hoping to help small business owners protect themselves as they try and avoid being the next target.

Every day, cybercriminals are swooping in on small businesses, knowing that most small businesses do not have the level of quality backing/plans as large corporations. Whether it is ransomware, phishing, or anything else; one cyber breach could result in damaged reputation, customers, and a business entirely.

Small Business Big Target unveils the most common risks small business present and provides simple, readily available actions to protect what you have worked so hard to build.

Inside you will find information on:

- How to identify red flags of cybercrime before it is too late
- Steps to take that will be both security-focused at an affordable price and level
- Creating a culture of security with your team

Your business may be small, but your risk is real—it's time to combat the threat! Let's get started.

Ali Nader

Managing Partner | **IT21ST, LLC**

855- 4IT-21ST x101



# Chapter 1: The Cybercrime Landscape. The New Reality for Small Businesses

For many years, small business owners thought cybercrime was something that only affected large corporations, government entities, and banks. After all, why would hackers target a small accounting firm, a local retail shop, or a family-run manufacturing company? That mindset was at least one of the most dangerous myths in contemporary business.

The reality is harsh: **Cybercriminals are increasingly targeting small and medium-sized businesses (SMBs), which often have weaker security measures compared to larger organizations.** Indeed, according to Verizon's 2024 Data Breach Investigations Report, **over 46% of cyberattacks across the world now involve a small business.** Hackers have recognized that many SMBs are less sophisticated than Fortune 500 companies' security measures, but SMBs still process valuable data, such as credit card information, personal customer information, payroll and even proprietary designs.

Cybercrime is no longer a sporadic threat - it is an everyday threat, and the existing mosaic of cyberattacks is expanding every year.

---

## The Different Faces of Cybercrime

### Phishing Attacks

The primary entry point for most cyber-attacks starts with an email phishing attempt. These types of emails often masquerade as a trusted source, such as a bank, vendor, or even your co-worker. Clicking a link or an attachment can grant access to sensitive materials or even install malicious software.

### Ransomware

Ransomware is malicious code that prevents access to your business data or encrypts it, demanding you to pay ransom to receive that access. Ransomware attacks are one of the fastest cyber-crimes in terms of growth. **Cybersecurity Ventures projected that ransomware damage will cost businesses more than \$265 billion annually by 2031.** Small businesses are at particular risk since they often do not have secure backups.

### Business Email Compromise (BEC)

Remember, you are not the only target to fraudsters. In a BEC scam, the hacker can impersonate your CEO or trusted partner, prompting your employee to wire money, or provide sensitive data. In 2023 alone, over \$2.9 billion in losses were reported to the FBI as a result of BEC scams. For small businesses, if even one fraudulent wire transfer occurs, the business is severely endangered.



## Insider Threats

Not every attack comes from outside the organization. Sometimes it is actually the employees themselves that are the cause (innocent or otherwise). Lost laptops, sharing passwords with co-workers, or intentionally stealing customer data are all viable breaches.

## Supply Chain Attacks

Hackers don't actually target businesses directly. A hacker accesses a vendor or software vendor that allows them to breach many businesses at the same time. The 2020 Supply Chain Attack with SolarWinds demonstrates how horrific this kind of attack can be. Even small businesses that rely on third-party IT vendor relationships can be at risk.

**Real-world example:** A small medical practice in Texas was a victim of a phishing scam in 2023 that ultimately tricked a receptionist into inserting her login credentials in a fake portal. The attackers were able to gain access to patient records, and the practice is still suffering the costs of a HIPAA investigation.

---

## The Cost of a Breach

The financial damages from a cyberattack are incredible. According to IBM's 2024 Cost of a Data Breach Report, the average breach costs small businesses more than \$4.5 million. While many large corporations can insulate themselves from the losses associated with cyberattacks, many small to mid-sized businesses (SMBs) are not well-insulated.

But it's not just about money. Here are some of the additional costs that are impossible to account for:

- ✓ **Reputation damage:** Customers will lose trust in companies if their data is at risk.
- ✓ **Downtime:** Ransomware can shut down operations for days or weeks.
- ✓ **Legal fines:** Businesses not complying with data protection legislation (HIPAA, PCI-DSS, GDPR) can incur fines for non-compliance.
- ✓ **Emotional distress:** Business owners often do not realize what a toll it will take on the company and, most importantly, on them personally during a crisis.

---

## Cybercrime is Becoming Increasingly Sophisticated

First and foremost, it's successfully identifying that cybercriminals are not lone-in-the-dark hackers living in their basements anymore. Often, the attacks you hear about are led by **organized criminals with teams**, tools, equipment, and even customer support. And very few are standing in an alleyway waiting for you to arrive from the ATM. Some criminals use AI-based phishing kits to produce convincing scams, at scale!

In summary, attacks are becoming:

- ✓ **Less expensive to launch** - Hackers are selling pre-packaged “cybercrime kits” on the dark web.
  - ✓ **Faster to distribute** - Tools are becoming automated giving hackers the ability to scan the internet to find any unpatched technology in minutes.
  - ✓ **Harder to spot** - Malicious emails can be indistinguishable from legitimate business communications.
- 

## Why Are Small Businesses Attractive Targets?

There is nothing about size that limits hackers - hackers discriminate based on opportunity. Small businesses have unique attributes that make them an attractive target for criminals primarily because:

- ✓ **Weak defenses:** No dedicated IT security.
- ✓ **Valuable data:** Customer, financial, or healthcare data.
- ✓ **Gateway to larger targets:** Many small vendors are connected to larger clients through supply chains.
- ✓ **False assumption of safety:** Many owners still have a belief that they are too small to be noted.

Put simply, cybercriminals perceive small and medium-sized businesses for what they are -easy targets! They are the low hanging fruit in the cybercrime world.

### Key Takeaways for This Chapter

- ❖ Cybercrime is no longer perceived as a future threat — it is a daily risk to small businesses.
- ❖ Cybercrime comes in many forms: phishing, ransomware, insider threat, leverage of a third-party vendor in an attack on your business, etc.
- ❖ At a minimum, Cyber-attacks can cause business failure or bankruptcy, reputation loss, loss of customers, loss of client and employee data, legal costs, fines, and emotional distress.
- ❖ Cybercriminals are organized, well-resourced, and becoming very sophisticated.
- ❖ Small businesses are prime targets because they underestimate the risk of cyber-attack and do not invest in cyber-defenses.

---

### Checklist: Are you a target?

Ask yourself:

- ✓ Do you keep customer or employee data in a digital format of any kind?
- ✓ Do you use any type of online banking, payroll, or web-based software service to operate your business in any way?
- ✓ Do your employees access e-mails and files from mobile devices?
- ✓ Do you rely on third-party vendors to support your IT or software, in any way?

👉 If you answered **yes** to any of these questions, your business is a target, and the rest of this book seeks to help you protect your business.

---



# Chapter 2: The Cost of Ignoring Cybersecurity

## The Hidden Danger of "It Won't Happen to Us"

Many small business owners view cybersecurity as an expense that they can put off. It's easy to think that cyberattacks only happen to large corporations -- the ones that make the news. This thought process can be fatal.

The reality is that, when small businesses face a cyberattack, they often times experience catastrophic outcomes. The National Cybersecurity Alliance states that **60% of small businesses close within six months of a serious cyber incident**. Why? Because they face financial, reputational, and operational costs that are challenging to recover from against most planning.

Looking the other way on cybersecurity is not only a risk -- it's a death sentence.

---

## The Financial Fallout

A cyberattack can drain a small business in ways that small business owners never considered:

### Direct Costs

- ✓ **Ransom Payments:** Attackers may ask for thousands, perhaps even millions, for access to data locked down.
- ✓ **IT Recovery Cost:** When systems are breached, you might need to hire individuals to Rebuild your systems, not just fix them, put data back on systems, and secure networks.
- ✓ **Fines & Penalties:** If customer data is compromised as a result of a breach, non-compliance with PCI-DSS, HIPAA, GDPR, etc. could result in significant fines.

### Indirect Costs

- ✓ **Downtime:** If your systems are down, your business is down. For a lot of small businesses, just one week down could mean tens of thousands of dollars in lost income.
- ✓ **Loss of Contracts:** Often times larger businesses cut ties with vendors who have a breach because of the risk that it can create for their own company.
- ✓ **Higher Insurance Premiums:** If a company has a history of breaches, they will likely have to pay higher premiums for cyber liability insurance.

 Case in point: In 2023, a small manufacturing company in the Midwest suffered from a ransomware

attack. The ransom was \$50,000; however, between downtime, lost orders, legal fees, and rebuilding the system, the company spent over \$700,000.

---

## The Reputational Ripple Effect

A cyberattack is not just a technology incident; it is a **trust incident**. Anytime data is collected and stored, customers, employees, and partners expect that data to be safe. When it is no longer safe, trust is gone.

- **Loss of Customer:** Research has shown that companies ultimately lose as much as 65% of their customers after their data is made available. Many will not return.
- **Negative Publicity:** Local newspapers, online reviews, and social media will amplify your brand damage, therefore creating a challenge to attract new clients.
- **B2B Damage:** Larger partners likely will force strict security measures on your future contracts. One breach could eliminate your business from potential contracts that are now dangerous.

Trust can take years to establish and seconds to lose. Many companies will never recover.

---

## Legal and Compliance Consequences

Depending on your type of business, you could also face legal issues due to ignoring cybersecurity.

- **Healthcare (HIPAA):** Breaches related to patient data can incur yearly fines as high as \$1.5 million.
- **Finance (PCI-DSS):** If your business touches credit cards and you do not meet their standards, you could be penalized heavily or lose your ability to take credit cards.
- **Global Impact (GDPR/CCPA):** If you conduct business with customers in Europe or customers in California, you must comply with their heightened privacy regulations, whether your company is small or large.

Cybersecurity is not simply an IT issue anymore but also, a compliance / legal issue.

---

## The Emotional and Human Impact

Business owners often miscalculate the **emotional distress of a cyber-attack**. In addition to financial ramifications and legal consequences, consider the emotional toll on you and your employees:

- Lack of sleep worrying about losing years of hard work.
- Telling loyal customers that their private information has been compromised.
- Preparing to lay off employees or close the business entirely.

The stress endured from an attack can be just as debilitating as the financial ramifications.

---

## The Myth of "Too Expensive"

Some small businesses are reluctant to invest in cybersecurity, believing that the level of investment is too expensive. But look at the numbers:

- **Average annual investment for a quality cybersecurity program:** \$5,000 – \$15,000 (dependent upon size).
- **Average cost of a single breach:** \$4.5 million (IBM, 2024).

In other words: *Paying to put prevention in place is always less expensive than paying to recover from a breach.* Cybersecurity is NOT a luxury; it can be one of the best financial investments a small business can make.

---

### Key Takeaways for This Chapter

- Neglecting cybersecurity is crippling and can lead to business closure.
  - The actual costs involved with a breach include direct costs, lost time, lost contracts, legal costs, and reputational damage.
  - Customers and partners will likely never trust you with their information again after a breach.
  - Compliance does not just pertain to larger businesses - and non-compliance can quickly become costly.
  - The financial and emotional cost of a breach far outweighs the minimal investment in cybersecurity.
-

## 🔥 Quick Checklist: Are You Facing Potentially Expensive Oversights?

- ✓ Do you have an ongoing, secure backup of your data?
- ✓ Do you have cyber liability insurance?
- ✓ Do you have a written incident response plan?
- ✓ Do you have training for your employees to help them identify phishing and fraud?

👉 Upon answering "**no**" to any of these items, the potential cost of neglecting cybersecurity could be greater than the cost to fix these gaps today.

---

## Chapter 3: Human Error as the Weakest Link. Why human error is the number target

Most business owners envision hackers hacking into their computers using sophisticated tools to mount a cyberattack. The reality is simple; attackers almost always take the path of least resistance and human error is a better avenue than brute strength.

Verizon's 2024 data breach investigations report provides an important takeaway. **74% of breaches are attributed to the human element (mistakes, human acts or falling for scams)**. Hackers know there is a better chance of tricking an employee than outwitting a firewall. Small businesses can also be especially problematic as employees are usually performing a variety of tasks and cybersecurity training is often limited. The human element is often the weakest link.

---

### Common Human Errors that Can Lead to Breaches

#### 1. Phishing Emails

Phishing is still the #1 way for cybercriminals to get in. Attackers send emails that look like they come from a legitimate source – the bank they do business with, a vendor or even an email from a coworker. With one careless click, a malicious link or malicious attachment can lead to a cyber breach and a compromised system.

- Example: A small real estate firm in Florida lost \$185,000 when an employee clicked on a fake wire transfer request that looked like the CEO's email address.

## 2. Weak Passwords and Password Reuse

Employees often reuse passwords for various accounts, usually personal and business accounts. When one password is stolen, the attacker will use it everywhere.

- A NordPass study states that “123456” is still in the top 10 most frequently used passwords globally in 2024.

## 3. Falling for Social Engineering

In addition to malware and malicious software, cybercriminals use social engineering by employing some form of psychological manipulation. They may impersonate IT support, a vendor or even law enforcement, convincing an employee to reveal passwords or transfer money. These scams, called **Business Email Compromise (BEC)**, cost people nearly **\$2.9 billion in losses in 2023** according to the FBI IC3 Report.

## 4. Neglecting Updating

A seemingly simple action like putting off updating software/access by clicking “Remind me Later” could expose them to known vulnerabilities. Attackers are constantly searching the internet for unpatched systems.



## 5. Lost or Unsecured Devices

As employees work remotely or on the road, losing technology may expose data that was not protected with encryption nor secured with strong passwords.

---

## The Psychological Factors of Human Error

Hackers are expert manipulators. They craft their attacks to take advantage of natural human behaviors. They use:

- ✓ Urgency: “You will have 24 hours before your account is locked.”
- ✓ Fear: “Your weekly IRS Alert: Immediate Action Required.”
- ✓ Curiosity: “Here’s the document you asked for.”
- ✓ Trust: Emails that appear from a boss, vendor you trust.

In an emotional state, employees tend to react instead of deliberate, exactly what attackers want!

---

## How to Turn Your Staff Into Your First Line of Defense

The good news; while people can be the weak link, they can also be the strong layer of defense, when they are trained and supported with the right culture!

### 1. Security Awareness Training

Short and sweet education sessions (even just 10 minutes once per month) may produce bigger returns. Employees must learn how to detect phishing emails, they must learn how to verify requests that may be out of the norm, and they must know who to report suspicious activities to.

### 2. Simulated Phishing Tests

You should always be sending out simulated phishing emails to your employees that are harmless to click into in order to see if they will. Your organization must view the simulated phishing tests as a learning opportunity instead of a punitive action!

### 3. Strong Password Hygiene and Multi-Factor Authentication (MFA)

All accounts must require strong and unique passwords. MFA should be utilized, when possible (i.e., codes sent to mobile phones, authentication apps, and/or security keys), MFA defeats 99% of credential-based attacks (Microsoft).

### 4. Culture of Pause and Verify

Employees must feel comfortable pausing and verifying before fulfilling urgent requests. For



example, pausing for 30 seconds to verify on the phone an \$8,000 invoice or email could save your organization \$8,000 as the cost of inaction.

## 5. Clear Reporting Process

Organizations need to establish for employees a clear path of who to report suspicious emails, texts, or messages. Timing matters - if an employee doesn't report the incident in a timely manner, the incident will still take place, and the consequence will be more significant.

---

---

## Case Study - The Mistake that Led to the Lesson Learned

Last year, a small marketing agency in California almost lost \$25,000 due to phishing scheme. An employee received an invoice from a vendor, which appeared to be a legitimate invoice, and she was prepared to pay the invoice immediately. Fortunately, she said she would check with her manager and that company took pause and prevented a \$25,000 loss.

Habitat Marketing Agency took a lesson from the incident, and didn't punish the employee, but rather used that moment to roll out new phishing awareness education, and then immediately created a new policy that required a second approval for all wire transfers; that one change probably eliminated their chance of losing six figures based on that incident.

---


---

### Key Takeaways from This Chapter

- ❖ Human error/decisions are the #1 cause of digital breaches with constituting three-quarters of all incidents.
  - ❖ Human errors/decision making mistakes - clicking to phishing incidents, weak password hygiene, social engineering, system updates not taking place; lost devices, etc.
  - ❖ Hackers are human and use human emotions against humans to trick employees: urgency, fear, curiosity and trust.
  - ❖ With the right training, simulated phishing tests, maintaining a strong password policy, MFA, and a culture of pause and verify - the employee can be your organization's strongest line of defense.
- 
-

## Quick Checklist: Improve your Human Firewall

- ✓ Do you train your employees regularly on cyber security awareness at least quarterly?
- ✓ Do you have phishing simulated phishing tests that measure your employee's preparedness in the real world?
- ✓ Do you have and enforce strong passwords and MFA on all business accounts?
- ✓ Do your employees know, at the very least, who to report if they receive a suspicious message and if they should do this immediately?

 If any of your answers to the questions of the above are **"no"** you still have significant risk vulnerabilities in human error.

---

---



## Chapter 4: Laying the Right Foundation – Cybersecurity Basics

### Why Basics are More Important than Technology

When small business owners think about “cybersecurity,” too often they picture expensive security software, difficult to install security camera systems or some other type of fancy technical solution. The truth is that most cyberattacks are successful not because hackers are smart, but because they ignore the basics.

According to the 2024 Verizon Data Breach Report, **almost 80% of attacks that were successful** could have been completely avoided with basic security practices. The bottom line is that if you focus on not getting hacked, you're better off and likely far cheaper than trying to keep up with fast-moving technology leadership plans.

This chapter will cover these basic elements: those must-have protections that every small business can implement right now without needing a whole IT department.

---

#### Firewalls – Your first guard.

Firewalls are like your digital security guard. It inspects and monitors incoming and outgoing data traffic. Firewalls will help identify unauthorized traffic or intrusion, and it also allows you to perform legitimate business activities.

- **Hardware Firewalls** – found in any business-grade router, but not typically consumer-grade routers. A hardware firewall should always be used to protect your cloud network and will need to be regularly kept up-to-date, so keep that in mind when you need to replace your router.
- **Software Firewalls** – installed on individual devices to add another layer of protection that also should regularly kept up-to-date.


*Quick Tip:* If you are using a consumer-grade router given to you by your internet service provider, it may or may not come equipped with a powerful firewall built-in. You may wish to consider upgrading your office network to a business class firewall device.

---

#### Antivirus and Endpoint Security

Malware is still a threat. The modern threat landscape does more than scanning for viruses. Modern antivirus tools flag ransomware, spyware, and other suspicious behavior before it is allow to propagate.

- ✓ Antivirus and endpoint security productively prevent and contain all malicious behavior, and should be installed on every single company-owned device (e.g., desktops, laptops, tablets, smartphones).
- ✓ Update, please! A solution is worthless if it's outdated. Always choose a security solution that deploys updates automatically without user initiation, because the hackers are always using voluminous exploit kits against old and outdated software.

 Stat: AV-TEST collected more than 500,000 new malware samples every day in 2023. Therefore, even the most cautious of users are vulnerable without antivirus in place.

---

## Strong Passwords and Multi-Factor Authentication (MFA)

Weak or reused passwords remain one of the most common entry points into a system. If someone receives leaked credentials, it may not only unlock their email account but payroll or banking as well.

- Password Best Practices: We recommend creating passwords with at least 12 characters (longer is better) with a combination of upper & lower-case letters, numbers, and symbols.
- No Reuse: Users should have a unique password for every account.
- Password Managers: Programs to ensure secure storage of passwords such as LastPass, 1Password, and Bitwarden.
- Use MFA everywhere: It is now very simple and secure to require a second method of verification (e.g., sending a text code or using an authenticator app). Implementing MFA stops 99% of credential-based hacks (according to Microsoft).

## Data Backups – Your Business Best Friend

Backups are not sexy, but they are your best preventative insurance against ransomware and accidental data loss.

- Follow the 3-2-1 Rule: 3 copies of your data, on at least 2 media forms, 1 copy off-site (or in the cloud, which makes it even easier).
- Restore Testing: If you cannot restore quickly, a backup is useless. Restore tests should be done at least quarterly.
- Automate Backups: Automation protects against employees forgetting, and significantly lowers the odds of human error.

For example, a small architecture firm based in Oregon was attacked by ransomware but able to restore their data in under twenty-four hours simply because they had daily backups on the cloud. The competitor across the street was not as lucky and ended up paying an \$80,000 ransom!

---

## Software Updates and Patch Management

Hackers love outdated software. The infamous breach of Equifax (affecting 147 million people) was the result of an unpatched vulnerability.

- Make sure automatic updates are enabled on everything-- operating systems, applications, security tools.
- Companies with lots of devices should use a patch management system to push updates company-wide.
- Firmware updates-- these are important too. Keep all on devices on routers, printers, and IoT up to date.

## Email Security Tools

Since phishing is the number one entry point, it's good to give email some extra love.

- ✓ **Spam Filters & Threat Protection:** block suspicious emails before they get to the employee inbox
- ✓ **URL scanners:** some systems provide URL scanning and automatically check for malicious links in emails
- ✓ **Attachment sandboxing:** opens email attachments in a safe zone before being delivered.

Email security tools can significantly minimize the instances of phishing emails that employees even receive.

---

## Don't Forget About Physical Security

Not all cybersecurity happens virtually. A lost laptop, unattended workstation, or unlocked server room can eliminate even the best of protections provided by software.

- ✓ Make it a requirement for all laptops or mobile devices to be encrypted

- ✓ Automatically lock workstation screens after a few minutes of inactivity
  - ✓ Limiting access to networking and server rooms to only those who need it
- 
- 

## Cybersecurity Awareness Culture

While technology is important to your cybersecurity posture, it will not be effective if employees circumvent the technology. Security must become the company's culture, it's daily activities and conversations:

- ✓ Develop a policy that encourages staff to recognize phishing emails and immediately report them.
  - ✓ Encourage positive behaviors related to cybersecurity as opposed to punishments for mistakes.
  - ✓ Cybersecurity should be on the agenda for anytime team meetings occur.
- 
- 

### Key Takeaways in This Chapter

- ✓ Most breaches occur because the simple things are ignored.
  - ✓ Firewalls, anti-virus protection, backups, strong passwords, and regular updates are just part of the picture.
  - ✓ User MFA and a password manager, drastically reduces the chances of credential theft.
  - ✓ The widest attack surface is email. It is worthwhile investing in your company spam filters to help employees identify junk mail, and the awareness trainings to help employees identify phishing attempts.
  - ✓ Cyber security is about more than the technology; you are trying to create a culture of awareness.
- 
- 

## 🔥 Quick Checklist: Cyber Security Foundations Basics

- ✓ Do you have a business firewall?
- ✓ Do you have anti-virus / endpoint protection on all devices? Are they managed and updated on a regular basis?



- ✓ Are your employees using unique, complex passwords with MFA?
- ✓ Are you backing your data up automatically, in the cloud, and testing it regularly?
- ✓ Are you updating your devices promptly to apply security patches?
- ✓ Is security a habitual behavior across your workplace?

👉 If the answer is 'No' to any of these questions, you have a weak foundation; a decent attacker will exploit it.

---

---



# Chapter 5. Protecting your Crown Jewels – Data and Devices.


## What are your Crown Jewels?

All small businesses have some information or asset that is critical to the success of the business or mission; for example, client data base, payroll documents, financial records, proprietary information, contracts, or even laptops and phones that contain all of that. A hacker may also refer to these things as their Crown Jewels. Losing control of this information will mean losing all of the above.

Why is the data so valuable?

- ✓ *Financial Data* - credit card, bank accounts and tax documents.
- ✓ *Customer information* - names, addresses, social insurance numbers and health data.
- ✓ *Intellectual property* - designs, formulas, trade secrets and proposals.
- ✓ *Operational data* - inventories, employee availability, supplier contracts etc.

To the hacker, an obtain data is a currency. It may be sold for profit, placed on ransom, and may be used as a vehicle to launch an attack on your clients.

 Stat: According to IBM's 2024 Cost of a Data Breach report, personally identifiable information was the most common category compromised accounting for 52% of breaches.

## How to Protect your data and devices.

### Data Encryption

You should encrypt data both at rest (stored on devices) and in transit (email, cloud, apps). If a laptop is stolen, by encrypting files, the thief won't be able to read them.

### Device Security

- ✓ Have all laptops and phones require a passcode, fingerprints and/or facial recognition.
- ✓ Provide a means to remotely wipe all data in the event that they are lost.
- ✓ Ensure that you lock screens if your devices are idle after a few minutes of inactivity.

### Access Control

Not all employees need access to all things.

Reach out to us to set up a role-based access-control system so that employees see something, not everything.

## Regular Backups

As discussed in Chapter 4, data backups are typically an insurance / investment against ransomware attacks or accidental deletions.

## Encrypting Email/files

If you are communicating sensitive communications; for those specific scenarios either secure email alternatives - or watermark/encrypting for file transfers.

---

---

## Case Study: The Stolen Laptop

A sales manager at a small consulting company had his laptop stolen from his car. As the laptop was not encrypted, the thief had access to client proposals, financial spreadsheets, and even saved email credentials. This breach ruined the firm not only financially but also severely impacted on a major client relationship.

After this incident, the firm implemented encryption, MFA, and mobile device management on all staff. One slip-up changed the entire security approach for the firm.

**Key Takeaway:** Your crown jewels are not data — they are your reputation, the trust of your customers, and the future of your business. Protect them in the same way.


---

---

# Chapter 6: The Ransomware Epidemic

## Ransomware: The Fastest Growing Threat

Ransomware has ballooned to a multibillion-dollar criminal industry. The scheme is simple — hackers encrypt the files on your system and then demand payment for the encryption key.

 Stat: Cybersecurity Ventures, a ransomware cost prediction generates to be \$265 billion from 2021 to 2031 annually.

## How Ransomware Works

- ❖ Phishing email or malicious/unintentional link installs malware on the computer.
- ❖ The malware quietly propagates through the network.
- ❖ Files are encrypted, and the operation comes to a halt.
- ❖ A ransom note displays and demands a ransom, usually in Bitcoin.

## Why are Small Businesses Ideal Victims?

- ❖ Limited defenses.
- ❖ No tested backups.
- ❖ Likely to pay quickly to get operations resumed.

## Real World Example

In 2023, a small medical clinic in Colorado paid \$120,000 to recover their patient appointment scheduling system, which had been locked. After paying, they discovered that it only recovered some of their data. They learned later that other data, including one of their patient's records, had been sold on the dark web. Prevention & Response

- ❖ Backups: Your number one defense.
- ❖ Patch & Update: Ransomware often uses old vulnerabilities to attack.
- ❖ Network Segmentation: Keep backups and sensitive data off of every day systems.
- ❖ Incident Response Plan: Know ahead of time who to call, how to isolate systems, and when to call law enforcement.

---

**Key Takeaway:** You never know if you will get your data back by paying ransom. Prevention and Backups are your best line of defense.

## Chapter 7: Cloud Security - Safe in the Sky Second

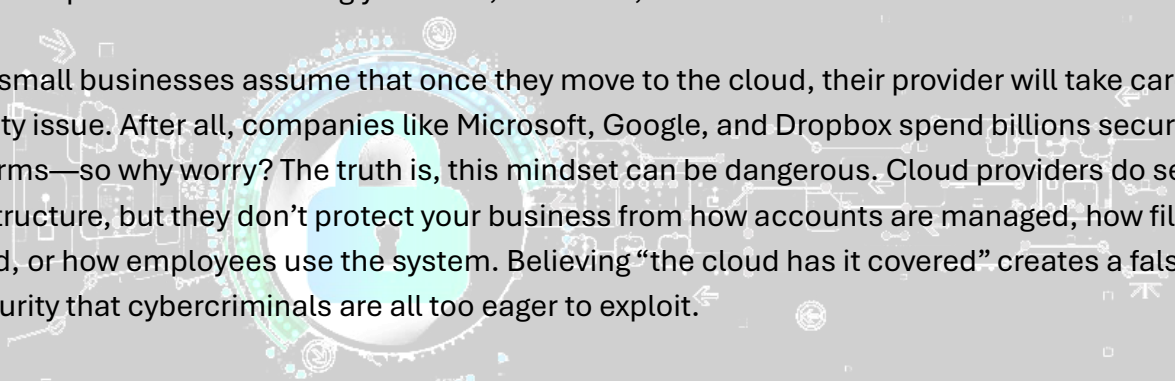
### Misconception: The Cloud

Many small businesses believe the cloud provider (Microsoft 365, Google Workspace, Dropbox, etc.) handles all security issues. In reality, **cloud security is a shared responsibility**.

This is where the concept of *shared responsibility* comes in. While the provider ensures the platform itself is secure, the business remains responsible for managing access controls, setting strong authentication policies, monitoring user activity, and protecting data from internal threats.

For example, if an employee's account is compromised through a phishing attack, Microsoft or Google cannot prevent the damage unless proper safeguards, like multifactor authentication and security monitoring, are in place. Understanding this division of responsibility is critical—because assuming “the cloud has it covered” can leave dangerous gaps in your defenses. So essentially,

- ❖ The provider is responsible for securing the infrastructure.
- ❖ You are responsible for securing your data, accounts, and access.



Many small businesses assume that once they move to the cloud, their provider will take care of every security issue. After all, companies like Microsoft, Google, and Dropbox spend billions securing their platforms—so why worry? The truth is, this mindset can be dangerous. Cloud providers do secure the infrastructure, but they don't protect your business from how accounts are managed, how files are shared, or how employees use the system. Believing “the cloud has it covered” creates a false sense of security that cybercriminals are all too eager to exploit.

Think about it this way: your cloud provider locks the doors and windows of the building, but you're still responsible for who you let inside. If an employee falls for a phishing email, reuses a weak password, or shares sensitive files without safeguards, the provider won't be the one cleaning up the damage—you will. That's why small businesses must take an active role in cloud security by enabling multifactor authentication, monitoring user activity, and training

## Cloud Risks

- ❖ Stolen credentials (phishing).
- ❖ Misconfigured permissions (i.e. access to public files, sharing externally).
- ❖ Insider threat (employees compromising data).
- ❖ Cloud Security Best Practices
- ❖ Disabled MFA on all cloud accounts.
- ❖ Regularly review access – Not removing ex-employees as soon as they leave.
- ❖ Not encrypt sensitive files prior to uploading.
- ❖ Lack of Data Loss Prevention (DLP) tools for shared files to minimize accidental sharing.

According to Gartner, by 2025 99% of cloud security failures will be the customer's fault and not the service providers.

**Key Takeaway:** The cloud is secure and powerful...if you properly configure it.





## Chapter 8: The Cybersecurity Roadmap - From Reactive to Proactive

Too many small businesses take action only after an event. In this case, it is too late. A roadmap can help to move from reactive panic over keeping your business secure to proactively preparing to secure your business.

### The Problem with Being Reactive

#### The Roadmap Steps

- ✓ **Risk Assessment**  
Identify your most valuable assets and biggest vulnerabilities.
- ✓ **Policies & Procedures**  
Write clear rules on passwords, backups, device use, and incident response.
- ✓ **Employee Training**  
As covered earlier, train your “human firewall.”
- ✓ **Technology Tools**  
Firewalls, antivirus, MFA, backups, monitoring.
- ✓ **Incident Response Plan**  
Who do you call? How do you contain the attack?
- ✓ **Partnering with Experts**  
Consider outsourcing to an MSP (Managed Service Provider) to maintain proactive defenses.

#### Case Study

A small law firm had partnered with an MSP to get 24/7 monitoring. After 6 months, the monitoring system flagged an unusual account activity suggesting a hacker was trying to brute-force the firm's email accounts. In less than 5 minutes that incident was contained and prevented a breach.

*Key Takeaway:* **Cybersecurity is not a one-time project - it is a continual strategy.**

## Compliance is not optional

Depending on your industry, you may legally be obligated to secure customer data. However, if you are not mandated for compliance, adopting a compliance posture will build trust in your contacts.

- ❖ **Healthcare:** HIPAA fines up to \$1.5 million/year.
  - ❖ **Finance and Retail:** PCI-DSS appropriate for credit processing including credit cards
  - ❖ **Privacy Laws:** GDPR for Europe, CCPA for California
- 
- 

## Why Trust Matters

In the current digital economy, customers want to know their data is safe. Simply being able to demonstrate compliance (and any certifications) can win you business.

### A few compliance quick wins:

- ✓ Write down your security policies.
- ✓ Provide ongoing employee education.
- ✓ Have audit logs.
- ✓ Review supplier compliance as well.

**Key Takeaway:** Compliance is not just hoop jumping; it's part of your brand promise.

---

---

## Shifting the Narrative

While many businesses believe that cybersecurity is an expense, for some it becomes a sales opportunity.

- ✓ Clients prefer vendors that can specifically show they protect the data provided.
- ✓ Some contracts have security requirements and being proactive will keep you a step ahead of the competition.
- ✓ Being known for protecting clients' data will develop trust leading to referrals and customer loyalty.

### Real-Life Example

A small accounting firm in Chicago, proactively posted their cybersecurity practices (MFA, encrypted client portal, employee compliance training) on their website. Within a year, the firm won two large contracts because the competition could not demonstrate a similar security practice.

---

---

**Key Takeaway:** Cybersecurity can help you avoid losing your business but can also help grow your business.

---

## Conclusion – Don't be the easy-target!

Cybersecurity is part of the strategy of any organization now and should be a top business priority. The reality is that small and medium size organizations are becoming an attractive target because of security weaknesses recognized by cybercriminals. A ransomware attack or a phishing attack can compromise your data, interrupt your operations and jeopardize the future of your business with a single breach.

The good news is that protecting your business is not complicated. By understanding the threats, myths and implementing appropriate countermeasures, you can minimize your exposure. Cybersecurity is not an 'event' or a 'project' that you can cross off your list. It is a continuing process and needs the right degree of vigilance, education and technology to overcome the threats.

At the end of the day, the most dangerous mindset you can have is to say, "it won't happen to us". Regardless of the size of your business, you are a target. The issue is not if cybercriminals will try to attack your business, but when and how ready will you be to thwart the attack.

There is no better time than now to start. Review your current measures and close or manage any gaps; you may want to consider establishing a relationship with a reputable IT service provider to assist you in mitigating risks, remaining aware of threats and, subsequently, managing your cyber-resiliency. The price of prevention is always cheaper than the price of cure, and your business, reputation and future is worth it.

On behalf of IT21ST, thank you for reading and considering your trusted source for your cybersecurity and IT services.

## Appendix: 10 Things To Do Now To Build Your Cybersecurity

1. Enable MFA on email and cloud accounts.
  2. Enforce strong and unique passwords.
  3. Back up to the cloud at least daily.
  4. Educate employees to recognize phishing schemes.
  5. Patch and update all systems regularly.
  6. Encrypt laptops and mobile devices.
  7. Restrict access to sensitive data.
  8. Implement an anti-virus/firewall and maintain it.
  9. Test your incident response plan.
  10. Work with a trusted IT / security provider.
- 
- 

## Resources Section

- ✓ Verizon 2024 Data Breach Investigations Report  
<https://www.verizon.com/business/resources/reports/dbir/>
- ✓ FBI Internet Crime Complaint Center (IC3) - <https://www.ic3.gov>
- ✓ CISA Small Business Resources - <https://www.cisa.gov/small-business>
- ✓ National Cybersecurity Alliance (StaySafeOnline.org) - <https://staysafeonline.org>
- ✓ NIST Cybersecurity Framework - <https://www.nist.gov/cyberframework>
- ✓ Cybersecurity Ventures Ransomware Report - <https://cybersecurityventures.com>



# SMALL BUSINESS, BIG TARGET

WHY CYBERCRIMINALS LOVE SMALL BUSINESSES—AND WHAT YOU CAN DO TO STOP THEM

