



## **Click, Scan, Hack: The Cyber Threats You Don't See Coming**

How everyday actions put your business at risk—and what to do about it

Presented by  
**Ben Struebing**



(855) 845-9208



info@cybernex.io



www.CyberNEX.io



# Cyber Threats Are Knocking—Will You Answer?



60% of small businesses that experience a cyberattack go out of business within **6 months**.

**What would be the impact to your business if you lost \$100K today?**

If hackers targeted your business today, would you know what to do?  
Stick around and find out how to stay one step ahead.

Understanding how hackers target businesses

Real-world attack scenarios and how they happen

Simple, practical steps to prevent cyber threats

Interactive Q&A at the end



# Why SMBs Are Being Targeted

Modern cyber threats are evolving rapidly, and SMBs are increasingly in the crosshairs of attackers

Increased Use of  
Technology and  
Digital Systems

Sensitive Data

**Viewed as Easy  
Targets**

Remote Work  
Increases  
Vulnerabilities

Advanced  
Threats Are  
More Accessible

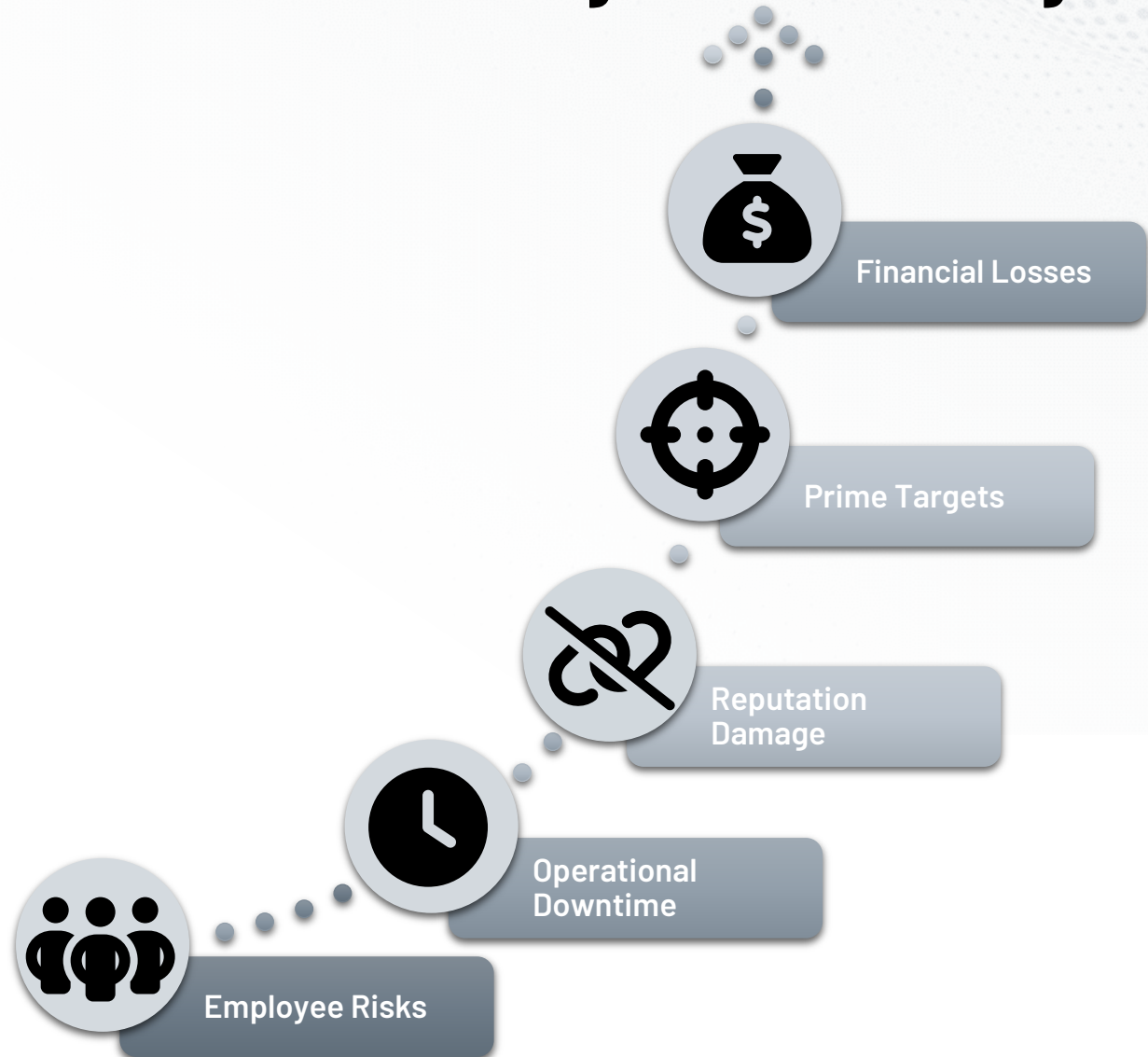
Supply Chain  
Exploitation

Lack of  
Cybersecurity  
Awareness



The Risks Have Never Been Higher

# Why Businesses Must Care About Cybersecurity





# Understanding Today's Cyber Threatscape



# Data Breach

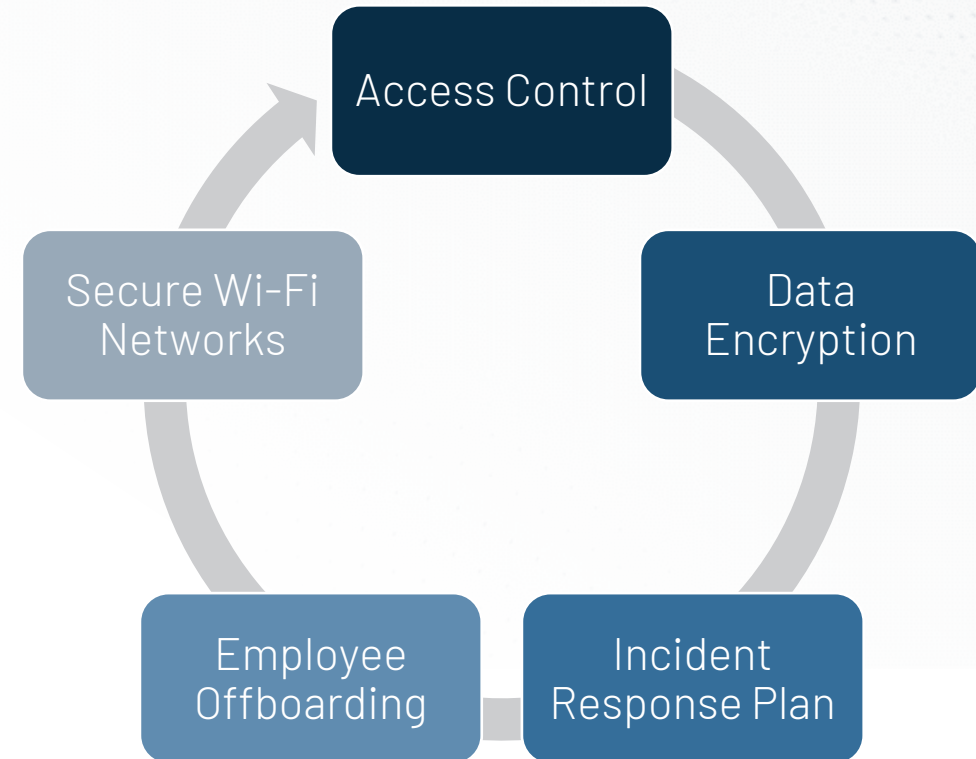
*"Data is the new oil." – Clive Humby*



## Your Business Runs on Data – And Hackers Know It

- Data includes customers, finances, employees, source code and inventory.
- Since 2019, 50% of companies report a breach annually.
- A data breach = financial loss, legal trouble, and reputational damage.
- Protecting your data is protecting your business.

## ADDRESSING THE THREAT

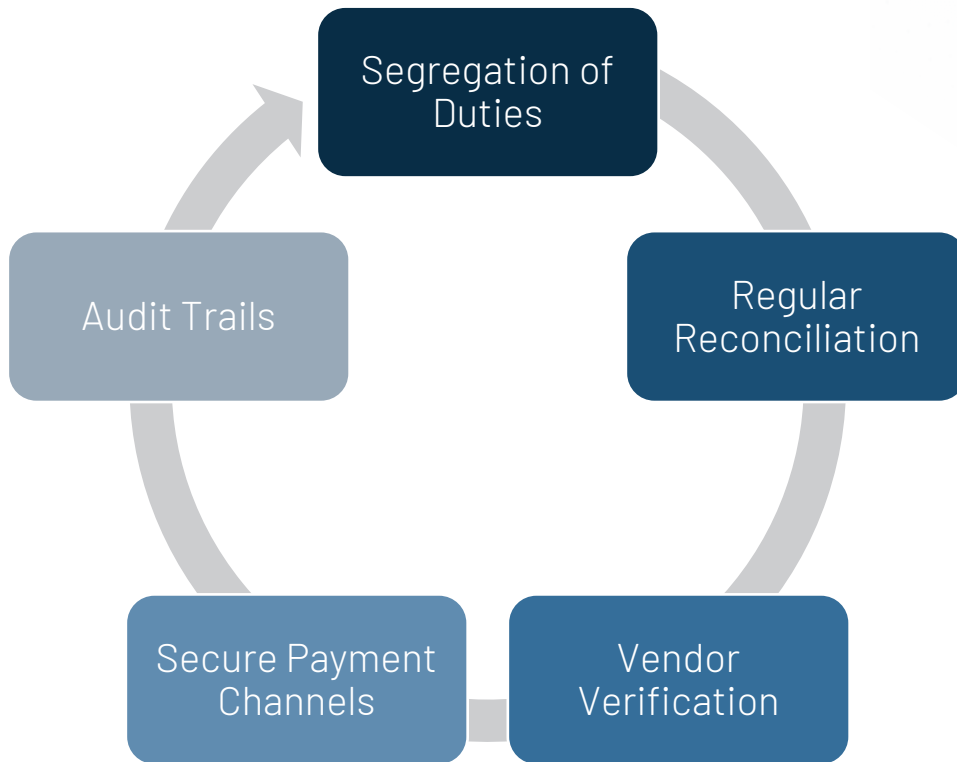




# Financial Fraud

*"Stealing isn't so easy; often, it's hard work. Otherwise, we'd all be doing it." – Elfriede Jelinek*

## ADDRESSING THE THREAT



## Cybercriminals Don't Rob Banks—They Rob Your Business

- Fraud now happens through **hacked financial systems**.
- Attackers **steal funds, divert payments, and exploit invoice scams**.
- **Wire fraud and unauthorized transactions** can cost businesses millions.
- Protecting your financial data is no longer optional.

# Reputation Damage

*"It takes 20 years to build a reputation and 5 minutes to ruin it." – Warren Buffet*



## A Single Attack Can Destroy Years of Customer Trust

- 90% of customers check reviews before visiting a business.
- Fake reviews, social media attacks, and leaked documents can destroy trust.
- Negative publicity, customer distrust, or the dissemination of false information can seriously harm your business' reputation.

## ADDRESSING THE THREAT

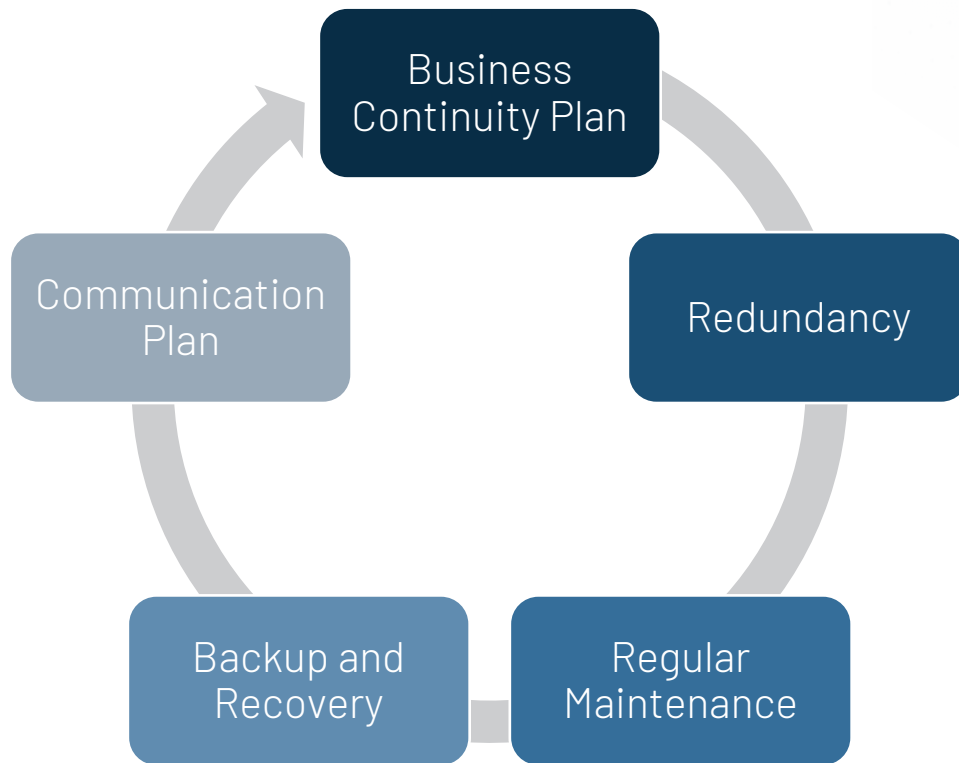




# Operational Disruption

*"Watch the little things; a small leak will sink a great ship." – Benjamin Franklin*

## ADDRESSING THE THREAT



## Cyberattacks Can Shut Your Business Down—Literally

- Ransomware & DDoS attacks can cripple critical systems.
- Lost access = lost revenue, downtime, and productivity.
- Every minute offline costs money—are you prepared?

# Compliance Regulations

*"If you think compliance is expensive – try non-compliance." – Paul McNulty*



## Compliance Isn't Optional—It's Essential

- Regulations depend on **industry, location, and data type**.
- **HIPAA** for health data, **PCI DSS** for payment security, **CMMC** for government, and more.
- **Non-compliance = legal trouble, fines, and loss of contracts**
- Protecting sensitive information isn't just good security—it's the law.

## ADDRESSING THE THREAT

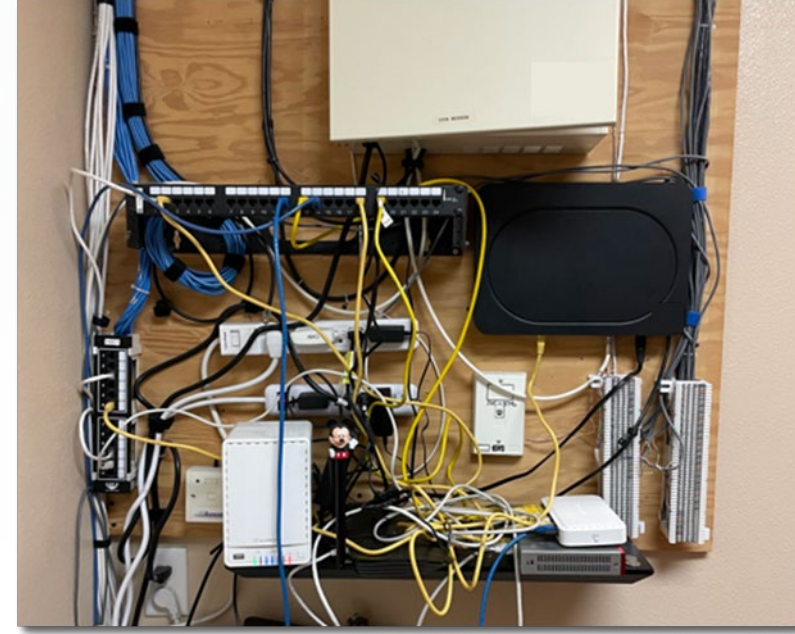
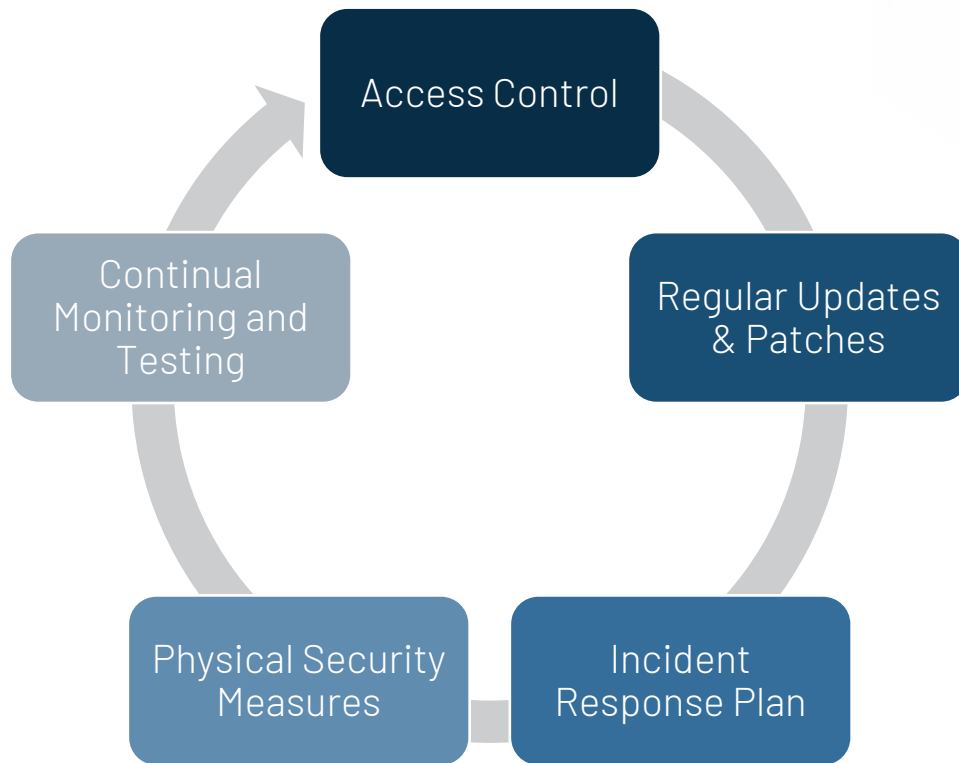




# Physical Security

*"Cyber security is much more than a matter of IT." – Stephane Nappo*

## ADDRESSING THE THREAT



## Cybersecurity Isn't Just Digital—Physical Security Matters Too

- Unauthorized access to hardware = major cyber risk.
- Physical breaches can lead to data theft, malware, or full network compromise.
- Strengthen security with access controls, surveillance, and hardware protection.
- A holistic approach = stronger protection for your business.



# Third-Party Vendors

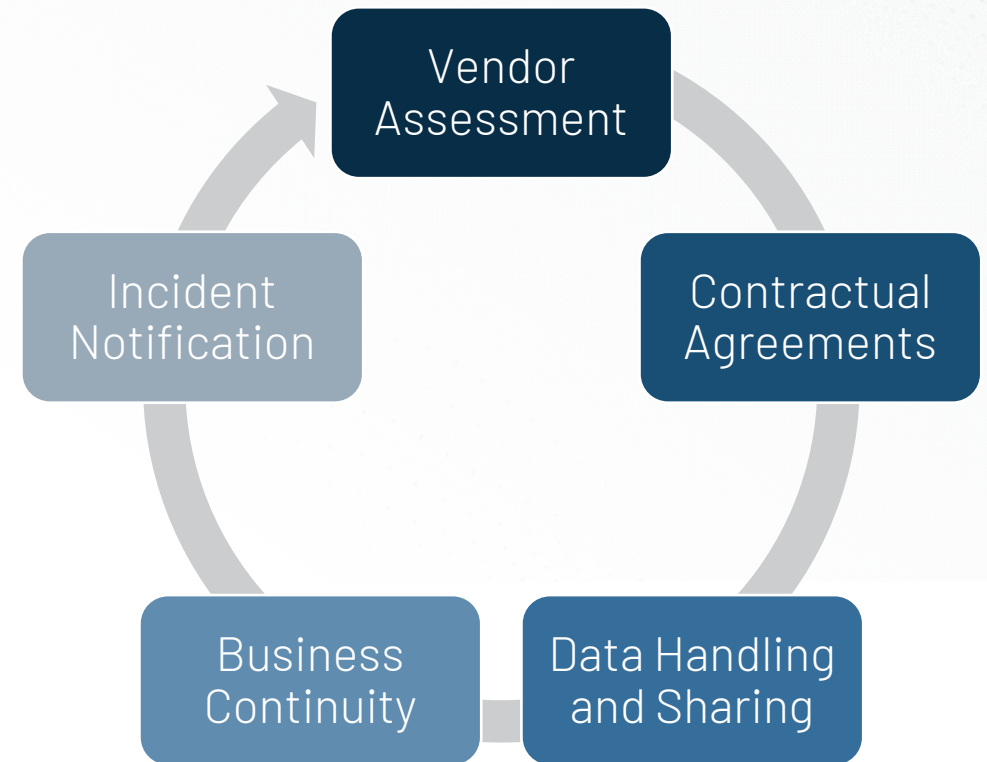
*"More connections to more devices mean more vulnerabilities... if you control the code, you control the world." – Marc Goodman*



## Your Security is Only as Strong as Your Weakest Vendor

- Third-party vendors can introduce cyber risks you can't control.
- Weak security in their systems = a backdoor into yours.
- Supply chain attacks are rising—how well do you trust your vendors?
- Verify vendor security before they become your weakest link.

## ADDRESSING THE THREAT





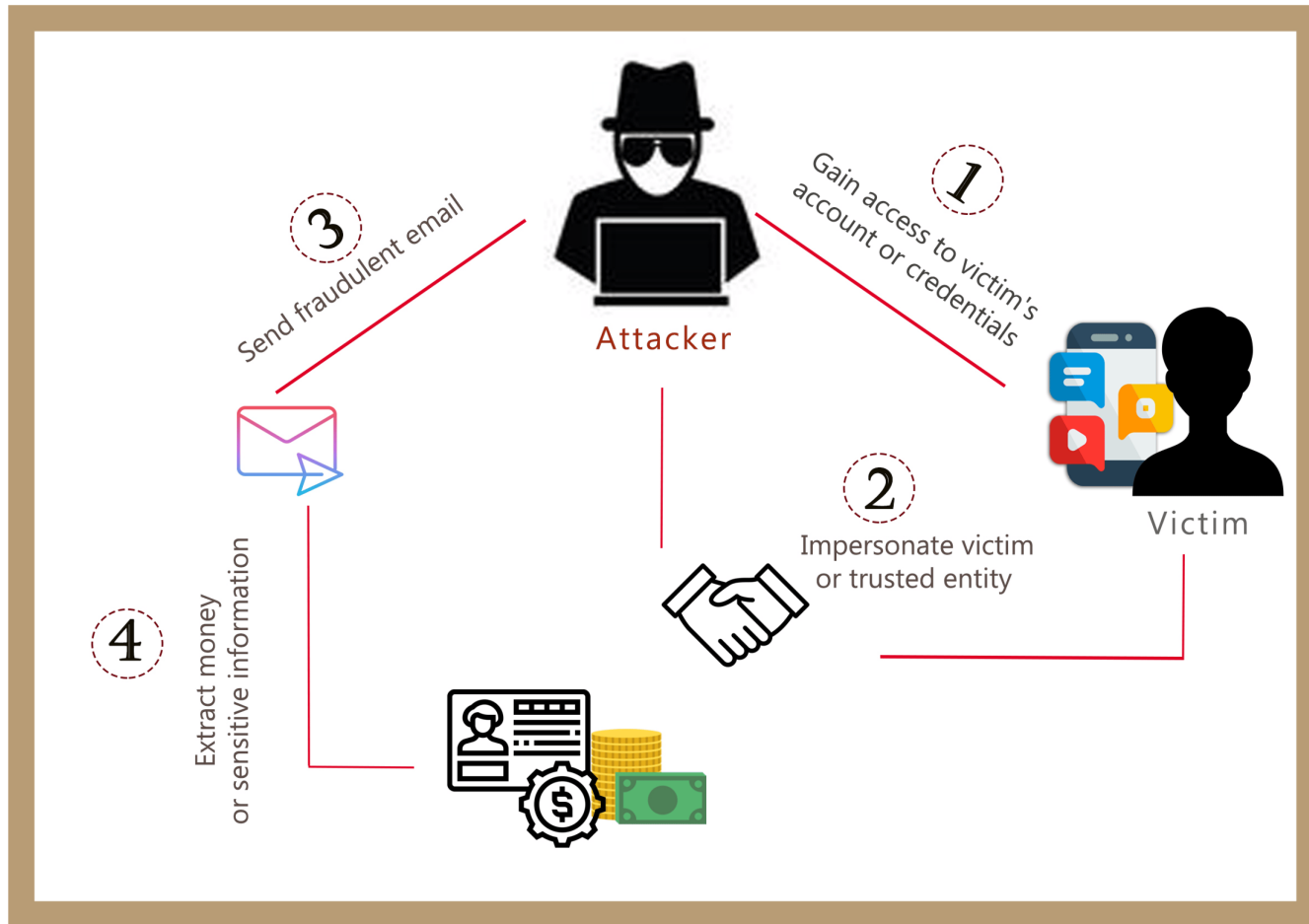
How It's Done:

# Inside the Mind of a Hacker

Real-World Attack Scenarios and How Cybercriminals Exploit Businesses Like Yours

## Case Study

# Business Email Compromise – How Hackers Trick Employees into Wiring Money



## Scenario

A finance employee at a marketing agency wires \$75,000 to a fraudulent account after receiving what appears to be an urgent email from their CEO.

## Prevention Tips

- **Implement a two-person approval process** for any financial transactions.
- **Verify requests** for wire transfers via a phone call or in-person confirmation.
- **Use email security settings** (SPF, DKIM, DMARC) to block spoofed emails.
- **Educate employees** to recognize fake urgency tactics in emails.



## Case Study

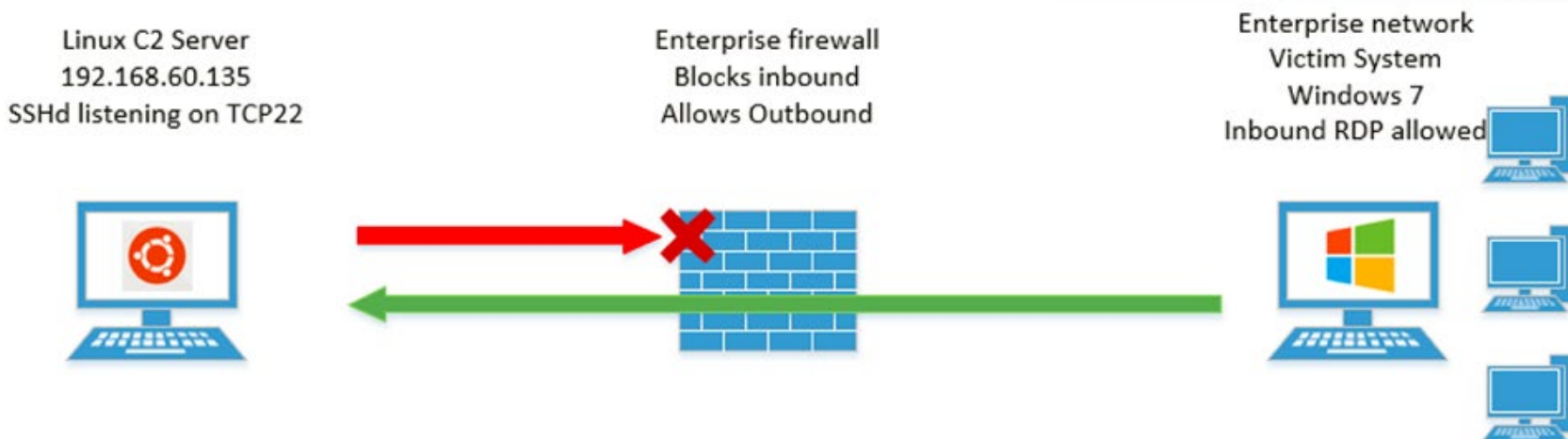
# The Misconfiguration Mistakes That Let Hackers Walk Right In

### Scenario

A mid-sized company invested in tools for cybersecurity — firewalls, VPNs, and cloud storage — believing they were protected. But small misconfigurations left massive security gaps that hackers easily exploited.

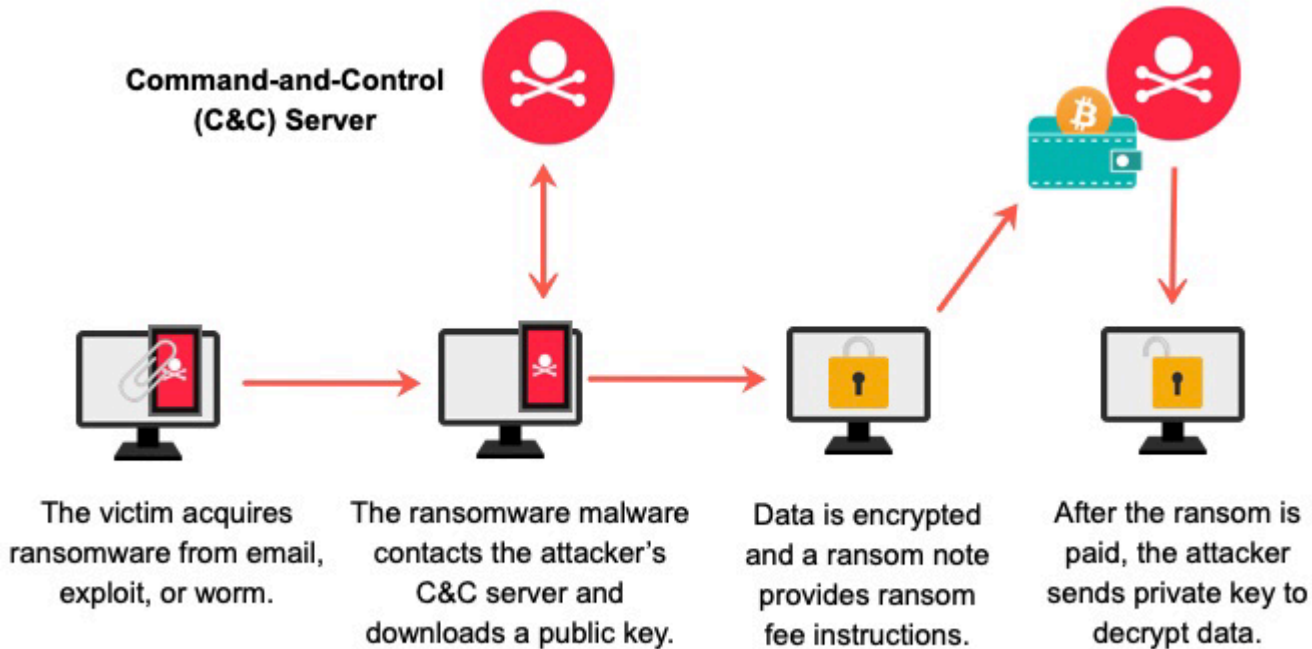
### Prevention Tips

- Change default admin credentials immediately on all security tools.
- Regularly review firewall, VPN, and remote access settings to remove unnecessary exposure.
- Never expose RDP to the internet—use VPN or zero-trust solutions, and enforce MFA for all remote access.
- Automate security checks to detect misconfigurations before hackers do.



## Case Study

# Ransomware – How an Entire Business Gets Locked Out



## Scenario

A small law firm unknowingly downloads ransomware, and all their client files become encrypted overnight, with hackers demanding a \$50,000 ransom to unlock them.

## Prevention Tips

- Never open unexpected **email attachments**—verify them first.
- **Use endpoint protection** that detects and blocks ransomware behavior.
- **Back up** critical files daily (to a cloud + offline storage) so data can be restored without paying a ransom.
- **Restrict admin** access so ransomware can't spread across the entire network.

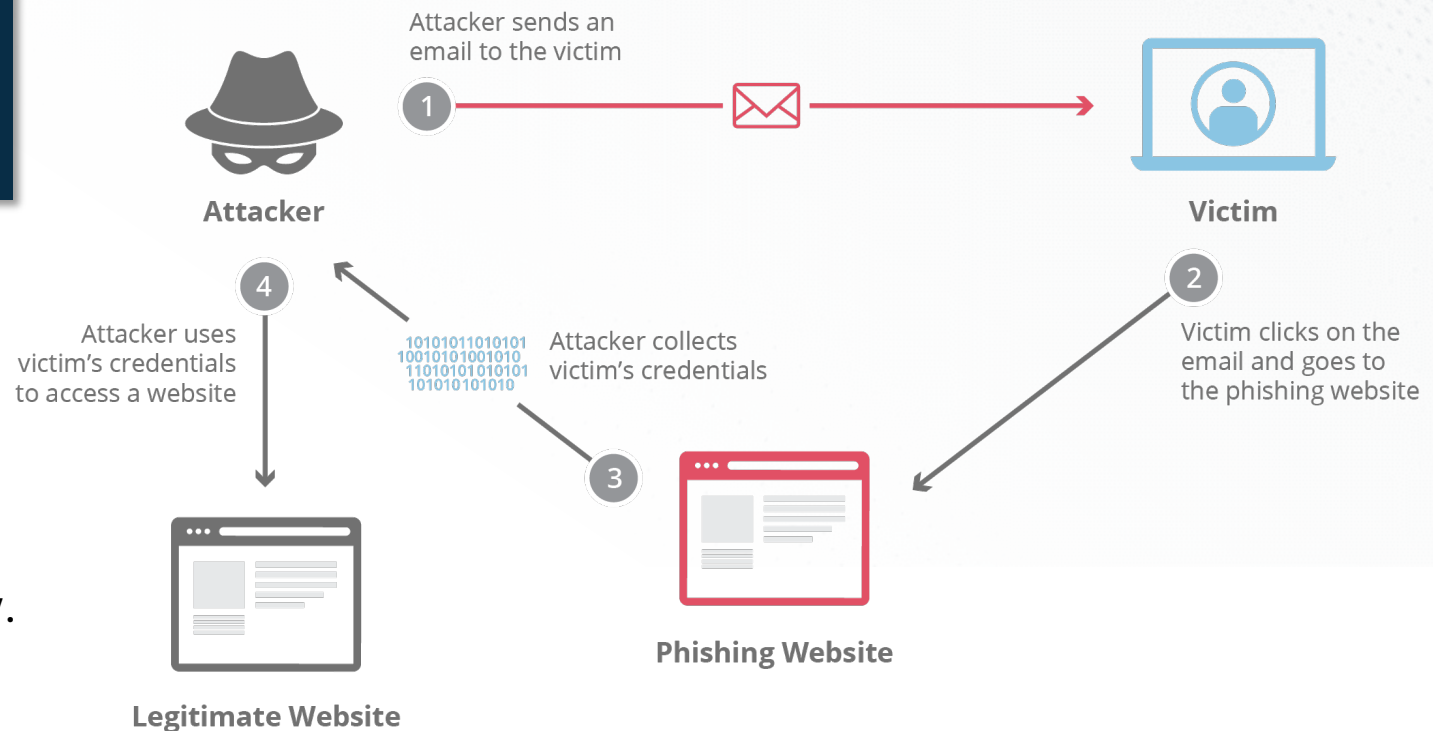
# Phishing Attack – How Hackers Steal Your Login Credentials

## Scenario

A business owner receives an email appearing to be from their bank, requesting urgent action to prevent account suspension.

## Prevention Tips

- **Train employees** to recognize phishing red flags (urgent language, misspellings, suspicious links).
- Always **verify requests** for sensitive information by calling the company directly.
- **Enable MFA** so stolen passwords alone aren't enough to gain access.
- Use **email security tools** that detect spoofed domains and phishing attempts.







## Case Study

# MFA Isn't Bulletproof: How Hackers Still Get In

Multi-Factor Authentication (MFA) is essential, but hackers have found ways to bypass it. Here's how they do it—and how to stop them.

### MFA Fatigue Attack

- Hackers attempt multiple logins.
- Triggers endless MFA push notifications
- The victim, annoyed or distracted, accidentally approves one—granting the hacker full access.

### Real-time Phishing

- Victim enters credentials on fake login page
- Site forwards to real website
- Victim enters their MFA code, which hacker captures in real-time

### SIM Swapping Attack

- Tricks or bribes a phone carrier employee to transfer the victim's number to a new SIM card.
- Attacker now receives all SMS-based MFA codes
- They reset passwords for **email, banking, and social media**, locking the victim out.



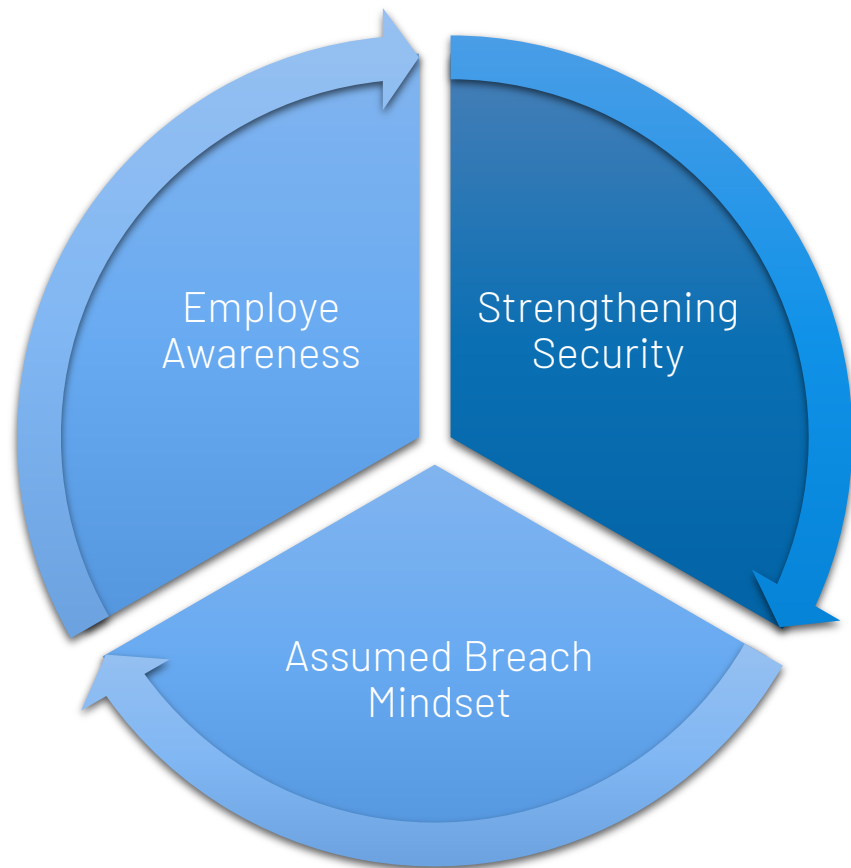
**Simple Steps, Big Impact**

# **Cyber Strategies That Actually Work**

You don't need a massive security budget—just the right strategy. Here's how to defend your business against cyber threats.



# Cybersecurity Strategies Every Business Should Use



## **Use Strong, Unique Passwords & MFA**

- Tools to use: Password managers, MFA apps (Google Authenticator, Duo).

## **Regular Data Backups (Cloud & Offline)**

- Best practices: Daily backups, cloud storage + physical copies.

## **Keep Software & Devices Updated**

- Auto-update features and patch management solutions.

## **Protect Business Email & Financial Transactions**

- Email security tools to filter out phishing attacks.

## **Invest in Cyber Insurance**






- What it covers and how it helps mitigate financial risks after an attack.

**Cybersecurity doesn't have to be complicated.**

**These simple steps can significantly reduce your risk and protect your business from cyber threats.**



# MFA Type Comparisons

MFA Type	Security Level	How It Works	Risk of Bypass?	Best Practices
FIDO2 Security Keys (YubiKey, Passkeys)	 Strongest	Hardware-based authentication requiring a physical key.	<b>Nearly impossible</b> – Not susceptible to phishing or MFA fatigue.	Use for critical accounts (admin, finance, email).
Biometric Authentication (FaceID, Windows Hello, Fingerprint)	 Very Secure	Uses facial recognition, fingerprint, or iris scanning for authentication.	<b>Difficult</b> – Can be fooled by deepfake attacks or cloned fingerprints in rare cases.	Use with device-based security (e.g., Secure Enclave, TPM). Combine with password or PIN for layered security.
Authenticator Apps (Google Authenticator, Microsoft Authenticator)	 Moderate	Generates temporary time-based one-time passcodes (TOTP).	<b>Moderate</b> – Can be phished via real-time man-in-the-middle attacks.	Avoid entering codes on unfamiliar login pages. Enable phishing-resistant MFA when possible.
Push Notifications (Okta, Duo, Microsoft Authenticator Approvals)	 Moderate	Approve login requests via a smartphone notification.	<b>Moderate</b> – Susceptible to MFA fatigue attacks (bombarding users with requests).	Use number-matching MFA instead of simple "approve" buttons. Train users to report excessive MFA prompts.
SMS-Based MFA	 Weak	Sends a one-time passcode via SMS to verify login.	<b>High Risk</b> – Vulnerable to SIM swapping and real-time phishing attacks.	Avoid SMS MFA for critical accounts. Use backup codes or an authenticator app instead.

# How to Protect Your Business Today

## 1. Assess Your Cybersecurity Readiness

### Quick Self-Check:

*"Could your business survive a cyberattack?"*

### Cyber Risk Checklist:

Identify gaps in your security strategy.

<https://tinyurl.com/yamxy76f>

## 2. Take Action Today



### Know Your Risks:

Make a quick list of what matters most to your business—customer data, financial access, intellectual property—and where it lives. That's your crown jewels.



### Limit Admin Access:

Not everyone needs full access to everything. Restrict admin rights to only those who truly need them—it reduces exposure.



### Enable MFA on Key Accounts

Turn on multi-factor authentication (MFA) for email, banking, and file storage platforms. It's one of the simplest, most effective defenses.


**The Best Time to Secure Your Business Was Yesterday.  
The Next Best Time is Now!**



## **Click, Scan, Hack:** **The Cyber Threats You Don't See Coming**

How everyday actions put your business at risk—and what to do about it

Presented by  
**Ben Struebing**

 (855) 845-9208

 [info@cybernex.io](mailto:info@cybernex.io)

 [www.CyberNEX.io](http://www.CyberNEX.io)

