



# CYBERSECURITY

---

## ESSENTIALS

---

for

# BUSINESS OWNERS

OWN IT.  
SECURE IT.  
PROTECT IT.



# TABLE OF CONTENTS

INTRODUCTION 3

PHISHING & SPEAR PHISHING 6

DISTRIBUTED DENIAL OF SERVICE (DDOS) 7

MAN IN THE MIDDLE (MitM) ATTACKS 8

MALWARE ATTACKS 9

DRIVE-BY ATTACKS 10

PASSWORD ATTACKS 11

WE CAN HELP! 12

OWN IT.  
SECURE IT.  
PROTECT IT.





# INTRODUCTION

Cybercrime and cyber-attacks are becoming **more prevalent** with each passing day.

The cybersecurity situation for small and medium businesses continues to worsen, with 3 in 4 SMBs now ranking a cyber incident as the #1 threat to their business this year, ahead of inflation (54%). The threat environment is intensifying at an alarming rate.

Current data shows that 42% of SMBs say AI-driven attack speed has made traditional patching and response obsolete, while 46% saw AI-generated phishing and 26% a ransomware incident in the past year. Without adequate protection, these attacks pose existential risks, as 40% of SMBs say an attack costing just \$100,000 or less would shut them down for good.



# 75%

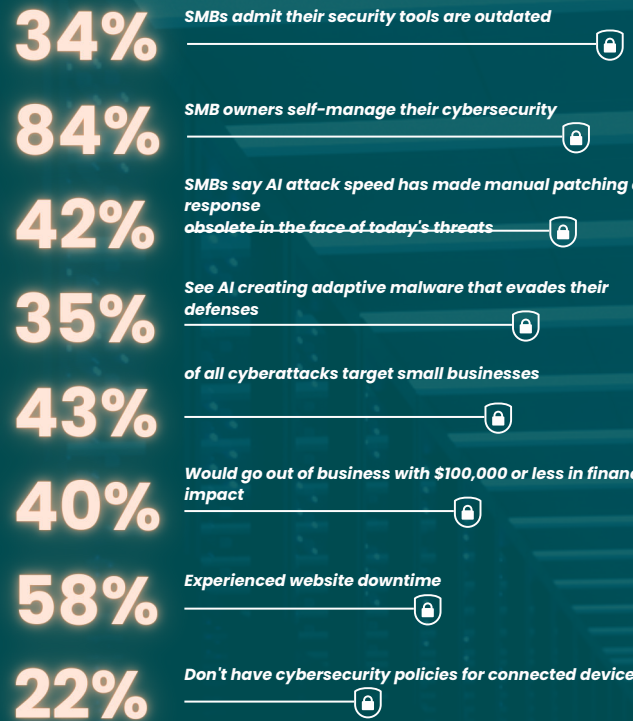
of SMBs rank a cyber incident as the #1 threat to their business this year.

Cybercrime presents a critical danger to SMBs. It causes operational disruption, data breaches, and network outages that 73% of SMBs faced this year. For 40% of SMBs, a cyber incident costing just \$100,000 would force closure. Around 34% admit their security tools are outdated.

Cyber-attacks continue to threaten businesses across various platforms, **with 73% reporting Wi-Fi or network outages and 58% experiencing website downtime.**

Organizations increasingly rely on digital tools but struggle with protection strategies. Many lack adequate defensive measures, with **22% having no cybersecurity policies for connected devices, 18% not requiring regular software updates, and only 32% running security awareness training for staff.** As digital adoption grows, so does the risk of data compromise, **with 23% using easily-guessable passwords like pet names or family members' names.**

As technologies advance, cybercriminals develop more sophisticated evasion techniques, **with 42% of SMBs admitting AI-driven attack speed has outpaced their ability to respond.**



Ransomware distribution continues to rise, with 26% of SMBs experiencing such attacks in the past year as business data increasingly moves beyond company control.

**Malware now targets businesses** with increasingly complex approaches, **with 35% of SMBs seeing AI-built malware that adapts to evade their defenses.** Criminals now focus on defeating recovery methods, making traditional security practices inadequate.

The threat extends beyond traditional networks, **with 55% suffering third-party or vendor interruptions that disrupted their operations.**

**Email phishing** remains cybercriminals' preferred attack method, with 46% of businesses reporting AI-generated phishing attempts and the human element involved in 62% of breaches. Standard security tools often miss sophisticated social engineering tactics.



**47% of businesses under 50 employees have no cybersecurity budget at all.**



DO NOT USE AND  
DO NOT PLAN TO

DO NOT USE  
BUT PLAN TO

Advanced threats like malware can penetrate systems without triggering conventional security alerts, operating covertly for months. Historical cases include major organizational breaches where attackers maintained persistent unauthorized access.

The necessity for robust cybersecurity approaches becomes more critical each day. **34% of SMBs admit their current security technology is outdated.** However, a substantial divide exists between recognition and action. **Approximately 28% admit the person managing their cybersecurity lacks adequate training, creating serious protection gaps.**

This produces a precarious environment where companies face increasingly complex attack methods. **Without structured defenses, 40% of SMBs would permanently close with \$100,000 or less in attack-related damages, yet many neglect fundamentals like regular data backups (16% never perform them).**

Here the importance of specialized security providers becomes indispensable. **Professional Managed Security Service Providers offer SMBs expert guidance and implement real-time monitoring and intrusion detection, which 67% of SMBs now have in place but 84% still watch themselves, against threats like the deepfake fraud that 29% experienced last year.**

Security service providers must offer SMBs comprehensive protection that strengthens defenses and reduces vulnerabilities. These experts help close the gap between inadequate measures and necessary safeguards. Business owners increasingly recognize professional security value, yet only 16% of SMBs bring in outside help, while 84% self-manage their security. With 57% of owners admitting security demands have delayed or cost them growth, many are considering partnerships to close gaps like the 34% who run vulnerability scanning and the 32% who run penetration testing.



**9 in 10 employees say their organization would consider switching to a new MSP if they offered a solution that met their needs.**



When surveyed about the primary advantages of engaging with security service providers, **55% of small and medium businesses** indicated that protecting their customers' sensitive data was the top priority, closely followed by **52%** who viewed it as a way to help their business safely grow and scale.

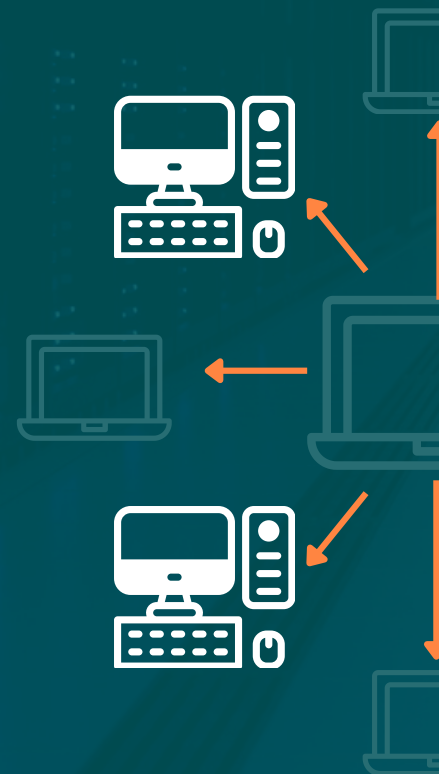
Security service providers can serve as essential allies for SMBs against cyber threats, as **23% of owners admit they don't understand their own cybersecurity risks.** Professional security teams can establish protective systems and create incident response strategies for potential breaches. These experts help companies navigate emerging security challenges and equip them to address sophisticated attack methods with improved resilience. **A dedicated security partner can safeguard your business from the 50% risk of losing customers following a successful breach.**

## PHISHING & SPEAR PHISHING

Phishing campaigns distribute deceptive messages with **harmful content intended to compromise confidential data**. These attacks direct victims to fraudulent websites capturing login credentials, payment information, and critical corporate data. Modern attempts combine **sophisticated deception and psychological manipulation** techniques. Cybercriminals impersonate **legitimate entities that recipients typically trust**. These attacks use customized content appearing genuine and credible. Consequently, businesses struggle to defend against targeted attempts. With the human element involved in 62% of breaches, phishing remains a predominant security threat.

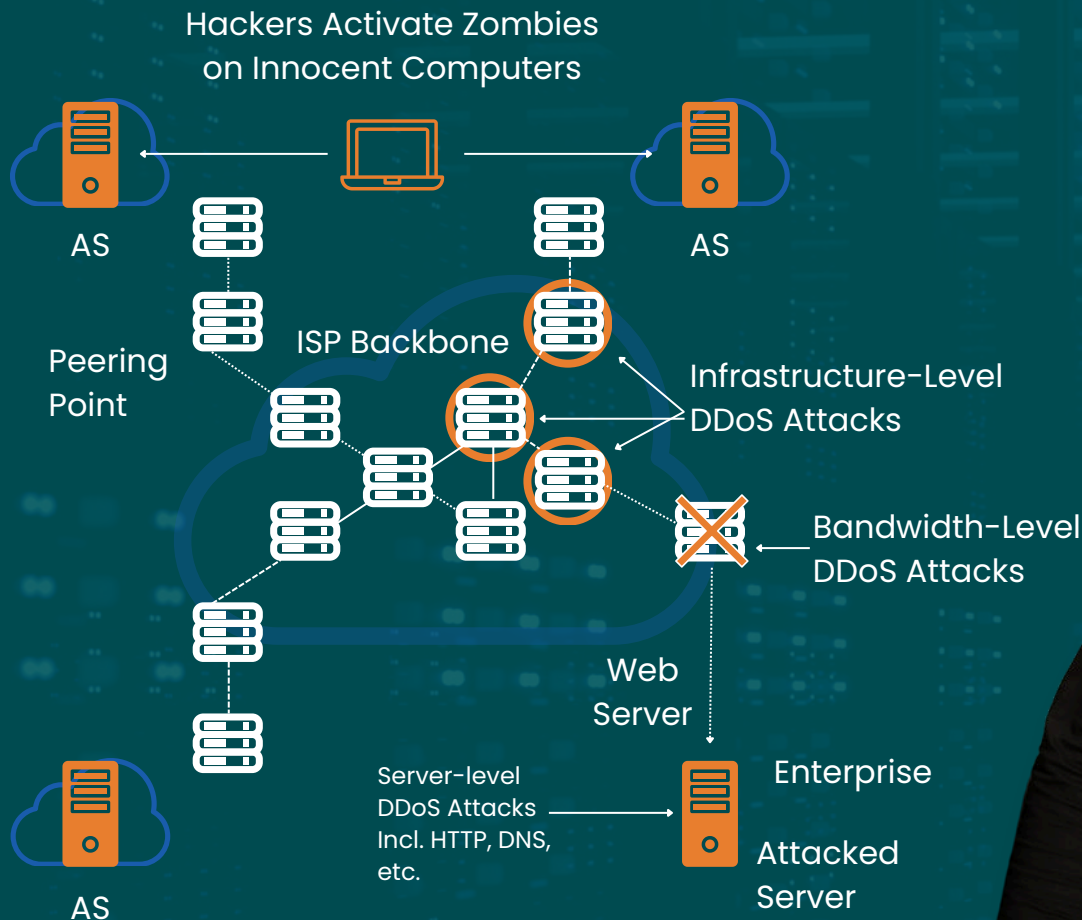
In the past year,  
breaches involving a  
third party rose

**60%**  
to 48% of all breaches.



# COST PER HOUR OF A DDOS ATTACK

\$8K  
TO  
\$74K



## DISTRIBUTED DENIAL OF SERVICE (DDOS)

Distributed Denial-of-service (DDoS) attacks compromise the infrastructure of servers, networks, websites, or computer systems to **render them inoperable or impair functionality**. These attacks typically utilize a command system that controls multiple compromised devices across a distributed network. DDoS operations **overwhelm** targeted systems through continuous streams of data packets, service requests, or traffic surges. This prevents legitimate users from accessing necessary resources.

While attackers may not directly extract data during these incidents, they effectively disable critical systems so they **cannot deliver essential services**. For small businesses, these attacks pose significant threats, potentially **disrupting critical operations** and **causing business interruptions that hit 73% of SMBs as network outages this year**, with network disruptions impacting productivity and customer trust.

**DDoS attacks are getting shorter: 89% now last under 10 minutes, with an average of 20 minutes.**



## MAN-IN-THE MIDDLE (MitM) ATTACKS

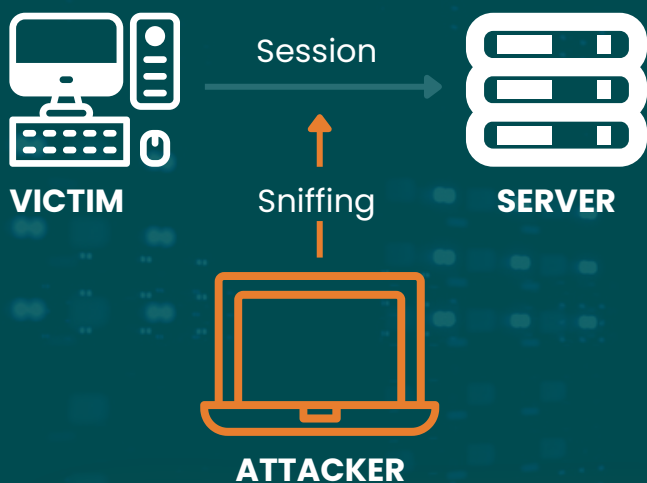
Man-in-the-Middle attacks happen when malicious actors position themselves between **user systems** and **business networks**. Attackers employ **credential interception** to compromise communication channels and access sensitive information. A frequently used technique involves **identity deception**, where attackers masquerade as authorized users to gain illegitimate access to services. **With only 32% of SMBs running security awareness training for their team**, these sophisticated attacks often succeed against unprepared organizations.

**Only 34% of small businesses have a formal incident response plan.**



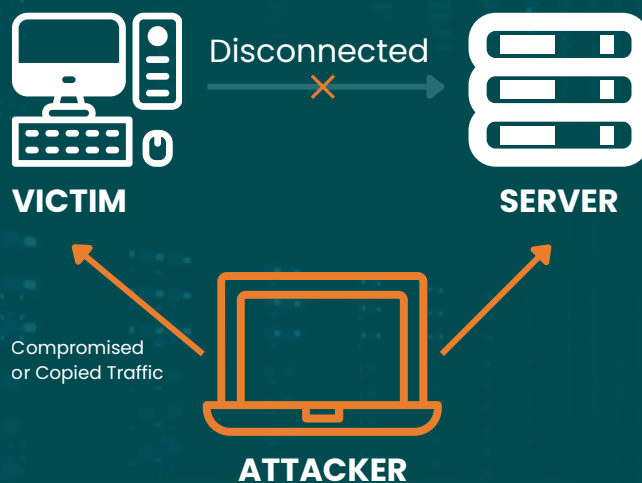
### STEP 1

#### Hijacking the Session



### STEP 2

#### Assuming the Victim's IP Address



# 31 PERCENT

OF INTRUSIONS BEGIN WITH AN

# EXPLOITED FLAW

## MALWARE ATTACKS

Malware or malicious software is engineered for **undermining system security** for **specific objectives**. Users often inadvertently install these threats which can then spread throughout networks. With 35% of SMBs now seeing AI-built malware that adapts to evade defenses, these digital threats represent a significant concern that can manifest through various sophisticated mechanisms, **mimicking legitimate applications**.

# 247 DAYS

DAYS TO IDENTIFY AND  
CONTAIN A BREACH



# 67%

of SMBs Have Real-Time  
Monitoring or Intrusion  
Detection in Place, Yet 84%  
Still Manage Security  
Themselves



### Macro viruses

Macro viruses target the **initialization sequence** of an application to compromise programs such as **Microsoft Excel** or **Word**.



### File infectors

File infectors find their way in your system through executable codes like **.exe extensions**. The infector becomes active when you **access the .exe file** or the **executable code**.



### Trojans

Non-replicating viruses that gain **unauthorized access** to a system. Trojans often camouflage themselves in the form of **legitimate software**.



### Logic bombs

Logic bombs are pieces of malicious codes that get initialized when **predefined conditions are met**. Attackers can program logic bombs to serve a range of purposes.



### System or boot-record infectors

These infectors attach to **executable codes** residing in parts of a disc. Boot record infectors can connect to a hard disk's Master Boot Records and even boot sectors of USB flash drives. **The infectors are initialized when someone boots using the compromised disk or drive**.



### Worms

Worms don't need a host file to propagate themselves on a network or system. **They are self-contained forms of viruses**.



### Polymorphic viruses

Polymorphic viruses **replicate endlessly to sabotage systems**. They use dynamic encryption keys every time to **avoid detection**.



### Droppers

Droppers help viruses **find their way into your networks and systems**. Most often, your antivirus will not detect droppers as they don't contain the malicious code: **they just lead to it!**



### Stealth viruses

Stealth viruses hide under the **guise of system functions**. They also infect your computer's defenses to **stay undetected**.



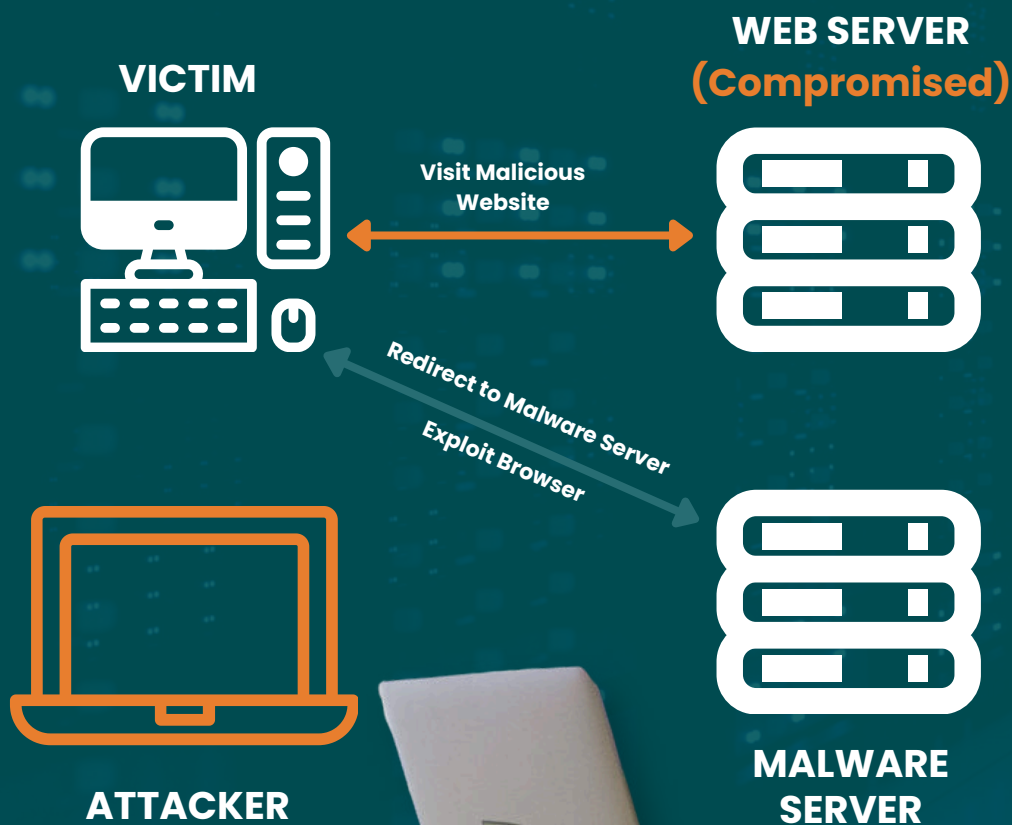
### Ransomware

Ransomware can take the form of any virus that **holds a victim's data hostage for ransom**. Ransomware attacks often encrypt data or files and **demand money in exchange for decryption keys**.

## DRIVE-BY ATTACKS

Drive-by attacks leverage **multiple digital channels** to infiltrate business systems. Attackers embed harmful code within advertisements, website elements, and software applications. Unlike traditional cyber threats, these attacks require minimal user interaction to activate. **Simply visiting a compromised website can trigger the infection process!** These sophisticated threats represent a growing vector for malware distribution. They exploit technical weaknesses in digital assets to gain unauthorized access. Common vulnerabilities include outdated software, with 34% of SMBs admitting their security tools are outdated. These attacks operate **silently** and are **typically undetectable to users**. This makes technical identification nearly impossible without specialized tools. Only automated patching keeps up: 42% of SMBs say AI-driven attack speed has made manual updating obsolete, and vulnerability exploitation is now the #1 way attackers get in, at 31% of intrusions.

**43%**  
of all Cyberattacks  
Specifically Target  
Small Businesses



**94 PERCENT**  
of Malicious Emails Are Phishing



# IN 2026, 48 PERCENT

of all data breaches now involve a third party,  
a share that rose 60% in a single year

## PASSWORD ATTACKS

Password-based breaches allow threat actors to obtain **illegitimate entry** to company systems and data resources. Colleagues within your organization might simply observe or search your workspace to discover credentials. This explains why security experts advise **against physical recording of access information**. Sophisticated adversaries employ network monitoring, encryption-breaking technologies, and automated guessing systems to compromise your authentication methods.

Multiple defensive strategies can protect against credential theft. Implementing automatic **account suspension following authentication failures significantly increases security**. Deploying **multi-factor verification** represents a critical protection measure that **14% of SMBs still fail to implement, even though credential abuse still appears in 39% of breaches, more than any other single vector**.

**ONLY 16%**  
of SMBs Bring in  
Outside Help  
With  
Cybersecurity,  
While 84% Still  
Manage It  
Themselves



## 23 PERCENT

of SMB Employees Use Either Their Pet's  
Name, a Series of Numbers, or a Family  
Member's Name So Their Passwords  
Are Easy to Remember



# WE CAN HELP!

We can help you navigate the complicated world of **IT & Cybersecurity** so you can better protect your **Data** and your **Business**.



[cinchops.com/cybersecurity](https://cinchops.com/cybersecurity)



[shane.stevens@cinchops.com](mailto:shane.stevens@cinchops.com)



(281) 269 – 6506



Shane Stevens  
CinchOps

*Shane Stevens*

#### CinchOps Serves Clients Throughout the Greater Houston Area

Unlock IT solutions tailored to your business needs by [scheduling a tech chat](#). Gain insights, explore customized strategies, and start your journey with your new IT business partner.

Doing business with us is a cinch!

#### Sources & Attribution

All statistics are from the following sources unless otherwise mentioned:

- VikingCloud - 2026 SMB Threat Landscape Report; Verizon 2026 Data Breach Investigations Report; IBM Cost of a Data Breach 2026; Microsoft Email Threat Landscape Q1 2026; SentinelOne DDoS Statistics 2026; TechInsurance 2026