Protecting Your Company from Cybercrime

Common Threats and Best Defenses

A guide for small and mid-sized companies

FocusDataSolutions

> The truth is that small and mid-sized businesses are less likely to have the time, budget and expertise to adequately defend against an attack. But given the trends, it's more important than ever that small businesses know the risks and employ effective strategies to protect themselves and their customers.

Table of Contents

Introduction

There is no question that cybercrime poses a real and growing threat to the United States, and it's not just a government or big business problem. Increasingly, small and mid-sized firms are very attractive targets for cybercriminals. Their defenses are generally weaker, and smaller companies provide an entry point to larger firms with whom they do business.

71%

Small companies – those with fewer than 100 employees – were the **target of 71% of cyberattacks** in 2011. Verizon, 2013.

In 2012, the **largest growth in targeted attacks involved small companies** with less than 250 employees. Symantec, 2013.

300%

Overall, cyberattacks on small businesses **rose 300 percent** in 2012 from the previous year. Symantec, 2012.

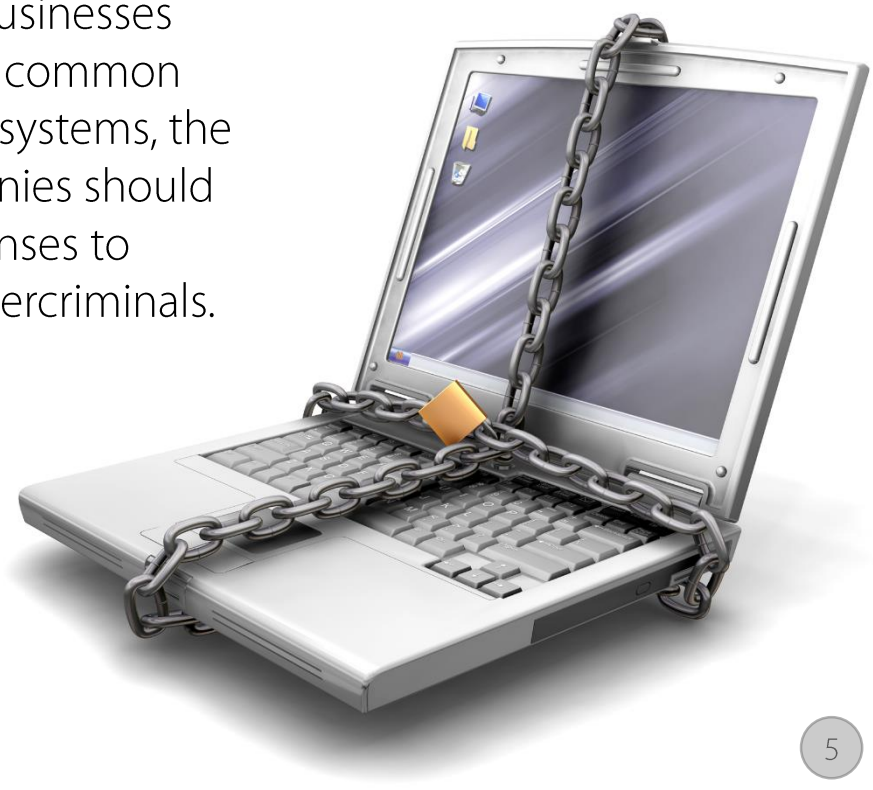
In 2013, 30% of targeted spear phishing attacks were aimed at small businesses with less than 250 employees. **One in five small businesses received a spear phishing email** in 2013, and the number of spear phishing campaigns rose by 91 percent that year. Symantec, 2014.

1/5

So, what are the threats and how can a business defend itself?

There are a multitude of ways that cybercriminals access sensitive information, and the world of cybercrime is a dynamic one with new threats emerging all the time. It is not as important to be technologically sophisticated enough to understand every threat as it is to put into place good defense mechanisms.

This guide will help businesses understand the more common ways criminals attack systems, the vulnerabilities companies should address, and the defenses to employ to thwart cybercriminals.



How Do Criminals Attack?

To figure out how to best protect your business, you may want to have some understanding of the methods criminals use to compromise and steal company data or resources. The list below is not comprehensive, but it covers the most common ways an attacker might harm a small business.

Denial of Service (DoS)

These deliberate attacks seek to shut down access to services by overwhelming a website or server with a multitude of requests.

Internal Bad Actors

A disgruntled or mischievous employee or person with access to a system may corrupt a network or share sensitive data with unauthorized recipients.

Pharming

This attack may corrupt a server or a computer's host files to redirect a user to a fake website without the victim realizing it and then steal valuable personal or private information. Sometimes these attacks take the form of domain name system poisoning that modify a server.

Malware

This term stands for **mal**icious soft**ware** that attacks a system in a variety of ways. The term encompasses all sorts of insidious attackers: a **virus**, **worm**, **Trojan horse**, **spyware**, **adware**, **keylogger**, **botnet/bot**, **rootkit**, and **ransomware**. *(See Page 8)*

Phishing

An attack that seeks to gain personal or private information, often by sending an email request that appears to be from a legitimate source (spoofing refers to when the email address of the sender appears to be originated from a different source than it truly is) and obtaining sensitive information or directing a victim to a website where the information is collected. In spear phishing, the email appears to come from an individual in the company or in a position of authority.

Physical Asset Theft

The theft of devices that contain valuable information, such as laptops, thumb drives, mobile devices, and the like.

Structured Query Language (SQL) Injection

SQL is the programming language used to manage data in a database. SQL attacks use malicious code to compromise a database and access the sensitive information it contains.

Wi-Fi Eavesdropping

Hackers may hijack information over the airwaves when connecting to sites that don't use encryption. Of greatest concern are unencrypted Wi-Fi hotspots. There are people called wardrivers who drive around searching for unsecured Wi-Fi networks to target.

Types of Malware

Virus

Viruses are initially contracted via software and then they can spread from one computer to another over a network or the Internet, or through removable devices, such as CDs or thumb drives. The virus could corrupt, steal, or delete data on your computer.

Rootkit

Software that gains administrator access to modify system functions and avoid detection by security measures.

Trojan horse

As the name suggests, this is software that seems legitimate, but hides its malicious intent. It pretends to be a useful program, but when run, it can allow hackers backdoor access to computers.

Spyware

Once installed on a computer, spyware allows a hacker to monitor a user's activity, such as keystrokes, without their knowledge and may affect the user's ability to control their computer.

Adware

Software program that may come with spyware to display unwanted advertising on your computer.

Keylogger

Software that records keystrokes, which may then be uploaded to a remote server where it is analyzed to steal passwords, credit card numbers, or other private data.

Botnet/Bot

Software robots that affect a group of computers (zombies) that are controlled by a botnet originator to create damage through activities such as distributing spam to the email contact addresses or overwhelming a server or website through a denial-of-service (DoS) attack.

Worm

A malicious software program that like a virus can replicate itself, but it does not rely on human action so it is very speedy in its rate of infection.

Ransomware

Software program that restricts access to a computer unless a ransom is paid.

How Do Criminals Get In?

To plan an effective defense against cyberattacks, businesses should look at their operations to see where they might be leaving doors open for thieves. An organization's weaknesses can make cyberattacks more likely. Understanding these vulnerabilities can help a business develop the right internal policies to close off points of entry that a cybercriminal might exploit.

Untrained Employees: Opening corrupted emails, clicking on bad links, creating weak passwords, using remote devices and Wi-Fi hotspots – you can see how unaware or careless employees can pose a risk for a business' cybersecurity.

Excess Authorized Users: The more people that have network access to sensitive information, the more likely it will be improperly handled and shared.

Remote Network Access: Allowing employees to access the network remotely creates more ways that hackers can find their way into a system through unsecure connections and more opportunity for unauthorized users to access or compromise company data by using or stealing an off-site computer.

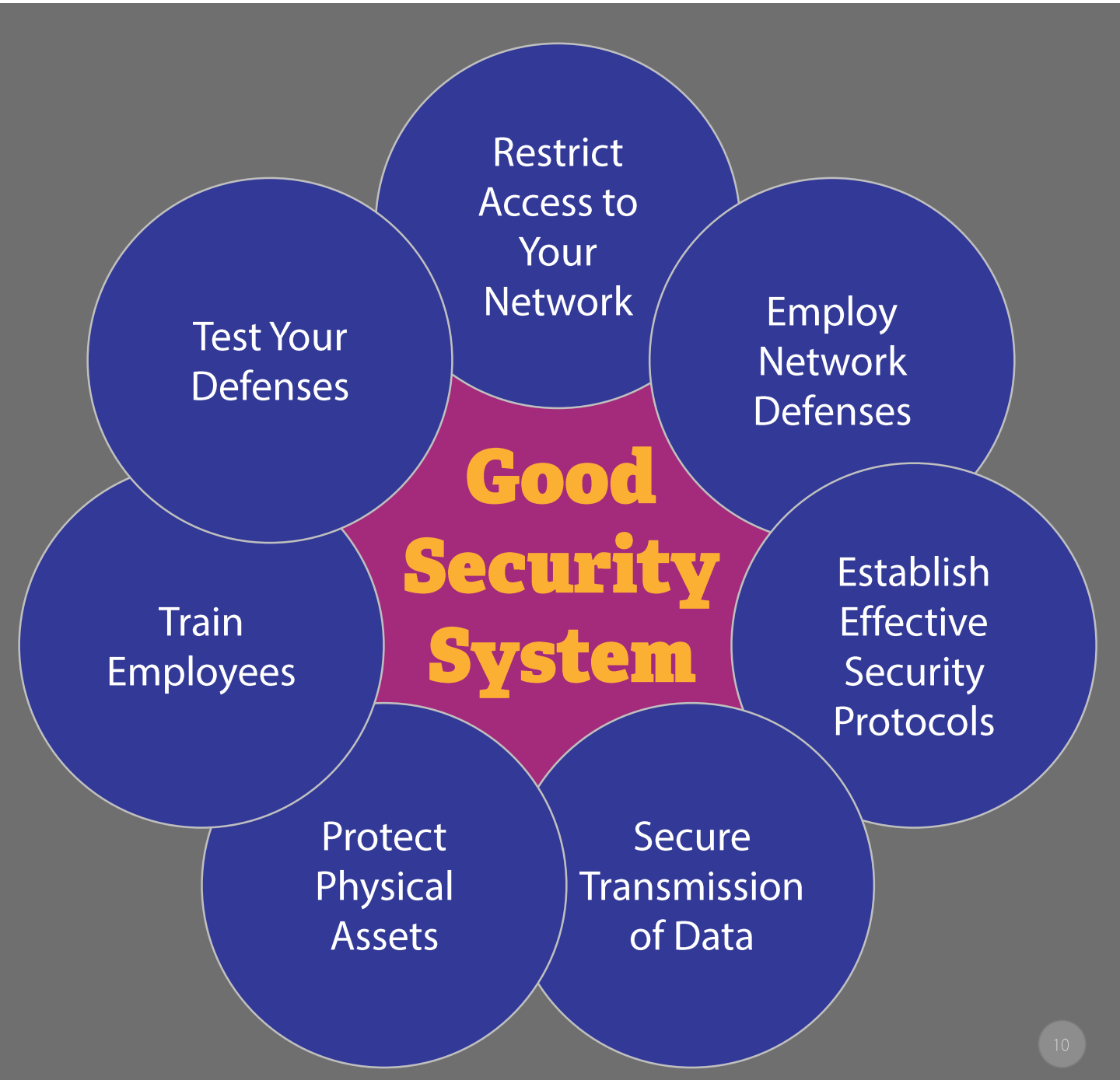
Vendors: Using third-party vendors can create another access point to your network or an avenue by which a company's data may be compromised if information is shared with or communicated to a vendor.

Personal Mobile Devices: This is a growing concern as more companies implement bring your own device (BYOD) policies *(See Page 14)*. Employees may use unsecured connections or their device may become infected when off the network and then infect the company's system when reconnected.

Email: Not only is email a vehicle to proliferate malware, it is a means for communicating information, even confidential, outside of the organization or to unauthorized parties.

Now that you know how criminals attack and how they get in…

What Does a Good Security System Look Like?

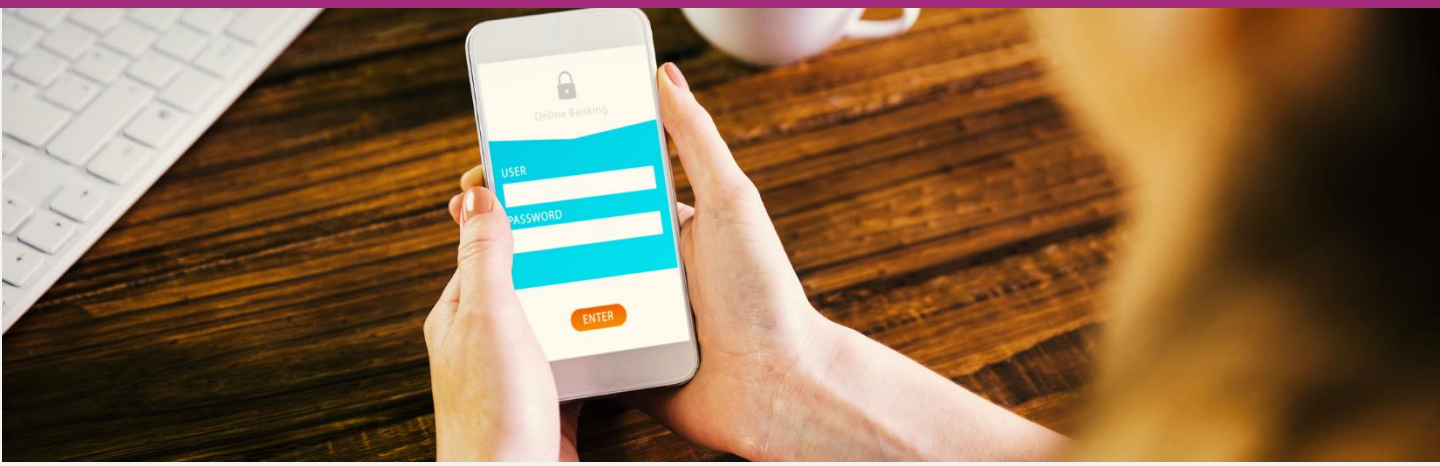


1 Restrict Access to Your Network

- ✓ Physically lock away your server and other technical equipment to eliminate unauthorized access.
- ✓ Employees should have access to information on a need-to-know basis. Only authorized employees should have access to sensitive data.
- ✓ Limit administrative access to trusted IT staff and key personnel.
- ✓ Password protect computers and other network equipment.
- ✓ Restrict third-party access to the network.

2 Employ Network Defenses

- ✓ Use proper networking equipment, such as firewalls, to impede network access.
- ✓ Segment your network and keep sensitive information in a secure location on the network (e.g., intellectual property, personal information, passwords, point-of-sale systems).
- ✓ Monitor activity on your network using effective intrusion detection and prevention tools.
- ✓ Secure remote access to the network via Virtual Private Networks.
- ✓ Be sure to have up-to-date software, malware, virus and spam-filtering services on all computers and servers.
- ✓ Apply software updates as they're issued and have a process in place to update and patch third-party software.
- ✓ Use strong authentication procedures (consider multi-factor authentication) to limit access to data.
- ✓ Disable user credentials after a number of failed log-in attempts.
- ✓ Employ application of front-end hardware to protect network perimeter and analyze traffic before it gets to servers.



3 Establish Effective Security Protocols

- ✓ Enforce strict password guidelines – require employees to use complex passwords that are changed at least every three months.
- ✓ Back up data daily and test backups to ensure recoverability.
- ✓ Don't open emails from unknown or suspect sources or click on links embedded in suspect messages.
- ✓ Establish a protocol to address security vulnerability reports in a timely manner.
- ✓ Enforce restrictions on personal devices *(See Page 14).*
- ✓ Establish policies for what devices can enter and exit the workplace (e.g. laptops, thumb drives, CDs, digital cameras) and put restrictions on storage and use.
- ✓ Establish Internet use guidelines and email policies.
- ✓ Delete all unused email accounts or other types of accounts when employees leave or services change.
- ✓ Verify that any vendors who have access to sensitive information have secure methods for storing and transmitting it. Put security standards in contracts and verify compliance by vendors.
- ✓ Monitor non-employees that are in the office space, even if for seemingly legitimate purposes (e.g., repairmen).
- ✓ Don't collect information that you don't need and don't keep information longer than necessary.

4 Secure Transmission of Data

- ✓ Securely transmit personal or sensitive information at every point.
- ✓ Use strong cryptography and employ widely used, industry-tested methods to secure data.
- ✓ Ensure proper configuration of encryption technology.

Considerations for a Bring Your Own Device Policy (BYOD)

- What devices are allowed?
- What level of IT support will the company provide?
- Is there cost sharing and who owns what on the device?
- What company data can be accessed on the device? Email, calendars, contacts, documents…
- What are the security requirements? Password protection, screen locks, security tools…
- Are there restrictions on apps?
- What if the device is lost or the employee leaves? If the device is wiped, employees need to ensure personal information is backed up.

5 Protect Physical Assets

- ✓ Protect paper, physical media, and devices. Store documents securely with a clean desk policy.
- ✓ Put standards in place for data that is in route or off site.
- ✓ Dispose of data and equipment securely (shred, burn, pulverize, wipe).

6 Employee Training

- ✓ Provide routine security awareness training.
- ✓ Explain security protocols and enforce them.

7 Test Your Defenses

- ✓ Perform "penetration tests" on a regular basis. This is where you, or your advisor, attempt to penetrate your network to test your defenses.
- ✓ Plan for an independent security review at least once a year, depending on the size and scope of your technology.
- ✓ Have a verifiable backup and disaster recovery plan and practice it consistently.

What Do You Want To Achieve?

Focus Data Solutions matches your ideas with the right IT management and technology solutions. Our team promises to create the results you need to drive your ideas forward. We work with service firms, associations and non-profits who share our commitment to communication, collaboration and trust in all business relationships.

1020 N. Fairfax Street, Suite 400, Alexandria, VA 22314
703-836-0080- www.focusdatasolutions.com