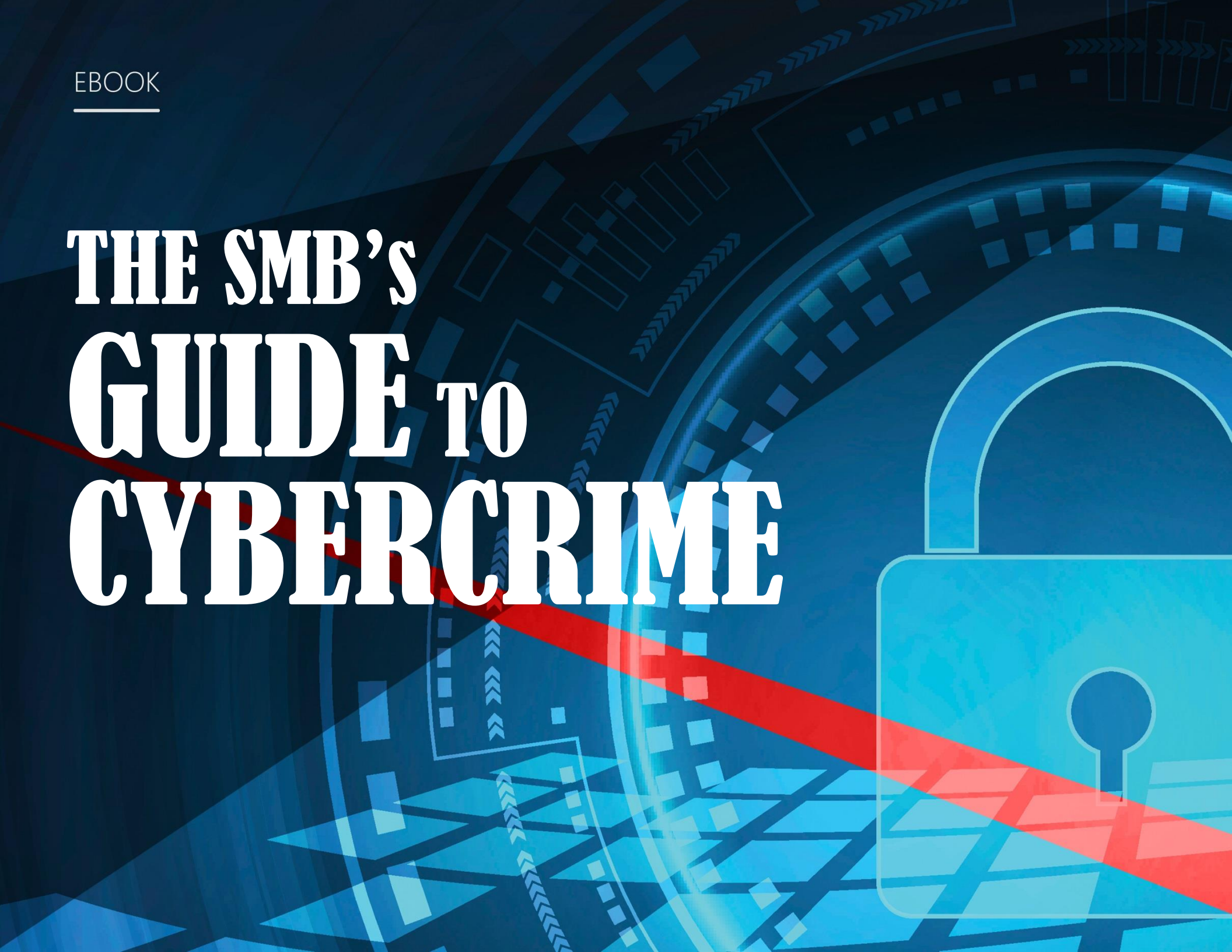
EBOOK

THE SMB'S GUIDE TO CYBERCRIME



SMBs are at risk for cyberattacks, just like their larger counterparts – new data shows that they've become a bigger target for today's cybercriminals. Here are some surprising statistics:

- **The most prevalent attacks against SMBs are web-based and phishing/social engineering.**
- **Phishing campaigns targeted small businesses 43 percent of the time.**
- **In the last five years there's been steady increase in attacks targeting SMBs.**
- **50% of SMBs have been breached in the past 12 months.**
- **59% of SMBs have no visibility into employee password practices.**
- **65% of SMBs that have a password policy don't strictly enforce it.**

Small and mid-sized businesses (SMBs) are now a priority target for cybercriminals.

WHY?

Because many don't have the protections in place to mitigate an attack. Being victimized is no longer a question of "if" but "when." You must protect your business using a multi-tiered approach — Here's what you need to know.

The best protection from Malware:

- **Be careful about what email attachments you or your staff open.**
- **Be cautious when surfing the Web, and stay away from suspicious websites.**
- **Install and maintain an updated, quality antivirus program.**

CYBERATTACKS COME IN MANY FORMS – HOW TO PROTECT AGAINST THEM.

A cyberattack is designed to steal and exploit confidential data, such as credit-card or financial resources, protected health information, and industry secrets. The end goal is to make money by selling the data, or holding it hostage.

The following are some cyber threats to be aware of. You should educate yourself and your staff about these most frequently used attacks, and how to protect your business from them.

Malware: This stands for "malicious software," a computer program with the intent to cause damage or gain unauthorized access. Malware is specifically designed to gain access or damage a computer without the knowledge of the owner. Some types of malware include spyware, keyloggers, worms, or any type of malicious code that infiltrates a computer.

The best protection from Phishing — Don't open a link or respond to an email if:

- When you hover your mouse over the top of the URL the hyperlinked address doesn't look legitimate.
- The URL contains a suspicious domain, like happy.com.maliciousdomain.com instead of happy.com.
- The message contains incorrect spelling and grammar.
- The message asks for personal or confidential information.
- What they offer seems too good to be true.
- You didn't initiate the response from the sender.
- The sender asks you for money, or offers to give
you some for an action.
- The message makes unrealistic promises.
- The message appears to be from a government agency.
- Something just doesn't look right.

The best protection from Ransomware:

- Always update and patch your software.
- Keep an antivirus software running.
- Create backups of your data that can be restored.
- Be cautious of suspicious pop-ups and emails.

Phishing: This is the most commonly used form of cyber theft. It involves collecting sensitive information like login credentials and credit card information through a legitimate-looking (but ultimately fraudulent) website, and sending it to unsuspecting individuals in an email.

Ransomware: Ransomware is a type of malware that infects your computer and locks your data. It demands a ransom from you to get your data back, or threatens to publish your private information unless you pay as demanded.

The best protection from a Password Attack:

• **Make sure your password is strong.** Go to How Secure Is My Password to see if you're using a strong password. Your passwords should be unique, long, and be a mix of letters, numbers and symbols.

• **Don't use one of these most popular passwords.** Check out the full list and don't use any of these.

• **If you use Google for anything be sure to enable Two-Step verification.** In addition to your username and password, you'll enter a code that Google will send via text or voice message to make it more difficult for someone to guess your password.

• **Consider using a password manager.** Password managers like LastPass and 1Password are great for managing your passwords and creating new, secure ones. You won't have to remember a password for each site, just your master password.

• **Your best protection from an APT** is to identify what content is top priority for protection and put safeguards in place. With an APT attack, criminals take considerable time to select the information that will be the most rewards for the infiltration.

Password Attacks: These come in three forms:

1. A Brute-Force Attack, which involves guessing at passwords until the hacker gets in.
2. A Dictionary Attack, which uses a program to try different combinations of dictionary words.
3. Keylogging, which tracks all of a user's keystrokes, including login IDs and passwords.

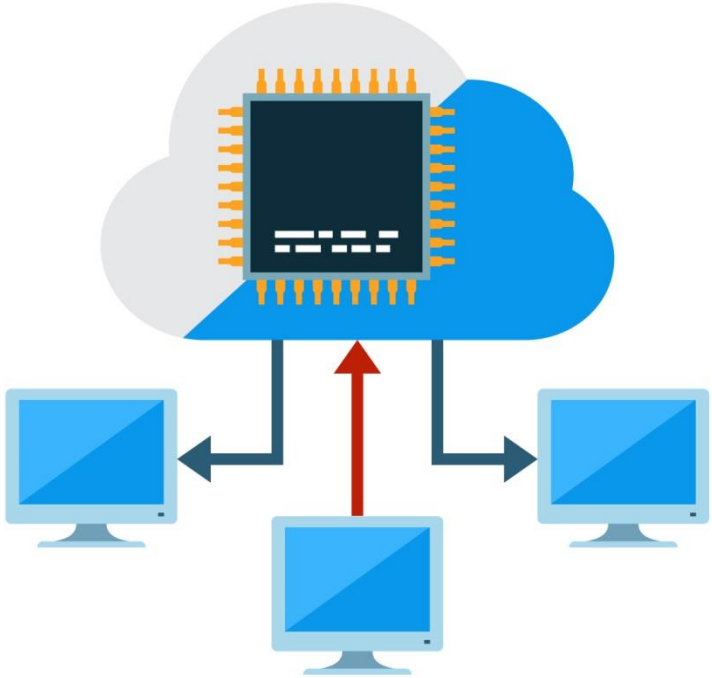
APT: Advanced persistent threats, or APTs, are long-term targeted attacks that break into a network in multiple phases to avoid detection.

The best protection from a DDoS is to with add network capacity. You can do this with cloud services and on-demand server capacity. By having more capacity, your business network will better stand up against a DDoS.

The best way to prevent an Inside Attack:

- **You should have a protocol in place to revoke all access to company data immediately upon an employee's termination.**
- **Know where your critical data is located and protect it with multi-layered security controls.**
- **Assess and re-asses the effectiveness of your data security controls to develop recommendations around both technology controls and processes that can enhance the overall protection of sensitive data from an inside attack.**
- **Develop monitoring checklists, and train staff to manage the updated security process.**
- **Establish a communication plan to manage the processes around discovering and protecting your confidential data.**

DDoS: A distributed denial of service attack is when cybercriminals intentionally overloaded your system with requests, with the goal of shutting down your website or network system.



Inside Attack: This is when someone in your organization with administrative privileges, misuses his or her credentials to gain access to confidential information. Former or disgruntled employees must be considered as the possible source.

The best way to protect your business from Cyber Espionage:

• **Use the latest operating system software.** The latest versions typically offer the most protection, and a 64-bit operating system can represent a difficult target to exploit.

• **Use a comprehensive IT security solution** that starts with a deep vulnerability assessment. It should manage software upgrades and patches, employ a whitelist of applications that are allowed to run your workstations, and include software that monitors Internet access.

• **Critical files and folders should be encrypted** and accessible only through authorized channels. In addition, it may be a good idea to develop a zero-day action plan, and test defenses prior to an attack.

• **Work with IT professionals** to build multi-layered security measures into your system management.

CYBER ESPIONAGE:

This is now the common type of cybersecurity attack against industries such as manufacturing, the public sector, and education. It happens when an attacker gains unauthorized entry to a network and accesses proprietary documents or confidential data. Common targets include:

• **Intellectual property** – Top-secret projects, formulas, plans or other kinds of private data. Anything an attacker could sell or use to their own benefit.

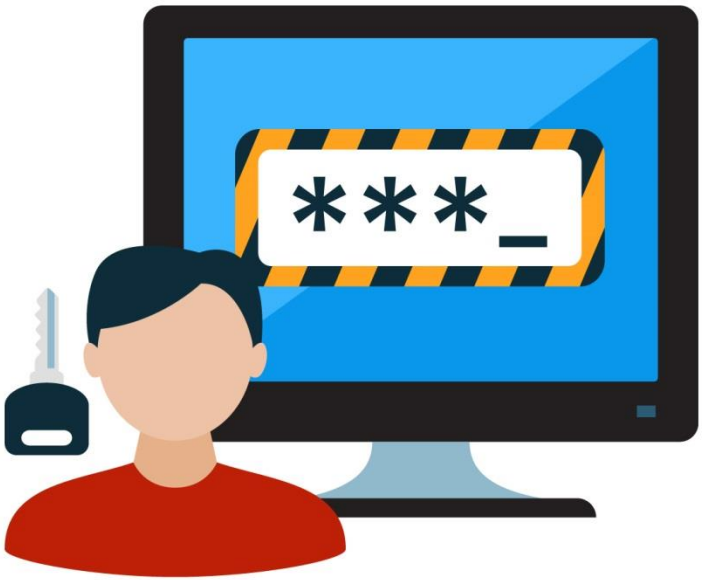
• **Internal data** – Operations, salaries, research and development.

• **Client and customer information** – Who are the clients of this organization? How much are they paying, and for what services?

• **Marketing and competitive intelligence** – Short and long-range marketing goals and competitor knowledge.

According to over 1,000 IT service providers, the lack of cybersecurity awareness amongst employees is a leading cause of a successful cyberattack against SMBs.

Your first line of defense is to train your employees to recognize the strategies cybercriminals use today.



nachman NETWORKS
Networks Done Right

OTHER SOLUTIONS

Train Your Employees

Employee training is a top cybersecurity protection program and the only way to ensure all staff understand the cyber threats they face. Make your employees aware of the ways cybercriminals can infiltrate your systems, teach them to recognize signs of a breach, and educate them on how to stay safe while using your business network.

It's always best to have an IT professional provide this training to ensure you've included important points unique to your business. And, don't forget about refresher training and training new employees.

Cybersecurity Insurance

Don't overlook cybersecurity for your small businesses. Your business liability policy won't cover losses or legal fees associated with a data breach. You need a separate policy to cover these damages. Talk to your insurance agent. Many insurance carriers are now offering tailor-made coverage for smaller companies to meet their budgets and risk-exposure levels.

So, as you can see, in today's world of cybercrime your business needs a multi-tiered approach to security. We can help. Contact Nachman Networks in Northern Virginia for a complimentary Cyber Security Assessment for your business. (703)600-3301 or sales@nachnet.com