SMALL BUSINESS UNDER ATTACK

A guide to understanding your risks and protecting your future.

INTRODUCTION:
TARGETING SMALL BUSINESS

No matter what size your business, you can't ignore cybercrime. You can't ignore hackers and the increasingly sophisticated malware they are continually unleashing on the internet. You can't be complacent and think you're not a target. Everyone is a target.

Too many small businesses still believe that their data has no value. That they are too small for cybercriminals to bother targeting them. The harsh reality is that your data is valuable. Cybercriminals who successfully steal personally identifiable information, medical records and trade secrets sell them for a tidy profit every day.

If you handle sensitive data such as Social Security numbers and credit card information or have any intellectual property you want to ensure doesn't fall into the wrong hands, you need to understand the risks you face and the solutions available to defend your data.

Hackers never give up looking for undiscovered vulnerabilities and keep conjuring new, creative ways to break into networks. No business is immune. And any belief that you are not a target may very well have severe consequences, such as compromising employee and customer data; losing intellectual property and crushing your competitiveness in the market; suffering a data breach that destroys your reputation; incurring penalties for non-compliance with federal and state regulators; insurmountable remediation costs; losing customers and partners... The list goes on, but the point is clear; data breaches can be devastating to a small business.

About 55% of small and medium business (SMBs) participating in the Ponemon Institute's 2016 *State of Cybersecurity in Small and Medium-Sized Business* study said their companies had suffered a cyberattack and 50% reported "they had data breaches involving customer and employee information in the past 12 months." Only 14% of participants rated as highly effective their "ability to mitigate cyber risks, vulnerabilities and attacks."

Even if cybercriminals aren't necessarily interested in your company's data, they often try to use small businesses as unwitting pawns to breach larger organizations. That's what happened in the 2013 cyberattack on retail giant Target, which exposed credit card and personal data of more than 110 million consumers. Hackers reportedly broke into the company's

network after stealing the credentials of a company that provides heating and air conditioning services to Target.

Investigators believe the Target attack started with a phishing email sent to Fazio Mechanical Services, the HVAC company, which according to owner Ron Fazio had a data connection with Target for electronic billing, contract submission and project management.

Phishing has become a favorite cyberattack method. It's easy and inexpensive for attackers and often succeeds because it preys on users' trust and curiosity. It also plays a major role in ransomware infections: 93% of phishing emails currently contain ransomware, according to researchers.

Phishing and ransomware are just two examples of cyber threats against which SMB companies need to defend. Phishing and ransomware have received a lot of focus in the last couple of years because of their prevalence, but cyber threats are numerous and varied – and you need to deploy systems, implement policies and educate users to combat them all.

Other threats for which you need defenses – and which are discussed more in-depth in this guide – include web-based threats, such as clickjacking and drive-by downloads, and exploit kits.

Included in this guide is a discussion on how to implement BYOD (bring your own device) policies to avoid creating new vulnerabilities by letting employees connect their own smartphones, tablets and laptops to the network. We also share security best practices for SMB companies, and address some of the common mistakes users make that can create cyber risks for your business.

The sad reality of doing business in a modern, connected world is there is no shortage of cyber risks. The cost of cybercrime keeps rising, and is projected to reach $2 trillion by 2019. A cyberattack costs companies an average of $4 million. These are scary numbers, but you are not completely defenseless against cyber risks. That's what we intend to show you in the following pages.

WHAT YOU NEED TO KNOW **ABOUT PHISHING**

Phishing vexes a lot of organizations because you can't solve the problem by just throwing technology at it. Preventing phishing attacks requires a combination of robust email security and user training.

The human factor is the tough part. Even when users understand the risks of clicking on suspicious attachments or URLs, some still do it. In a recent study, about half of the subjects in an experiment clicked on links from strangers in e-mails and Facebook messages – even though most of them claimed to be aware of the risks.

It really takes a sustained effort to educate users to stop doing what they intuitively know they shouldn't do but do it anyway.

And that's one of the reasons phishing is so successful. Rather than trying to hack into secured systems, cybercriminals sneak into the path of least resistance by tricking distracted or trusting users into opening the door for them.

Fraudsters have no shortage of material for bait. A phishing email may pass itself off as an Apple Store message, a message from a Facebook friend, a package delivery notification, a resume from a job applicant or myriad other disguises. The victim clicks on an attachment that proceeds to download malicious code onto their machine, potentially infecting the whole network, or visits a website that asks for private data, which the user provides thinking it's a legitimate request.

Three Phishing Approaches

Phishing currently breaks down into three main categories. Regular phishing casts a wide net, with cybercriminals sending emails to large groups in an attempt to ensnare as many victims as possible.

A second, more refined approach – spear phishing – targets specific groups or individuals. Spear phishing usually consists of attempts to steal private information such as social security numbers, credit card numbers and financial account information.

This technique is, by far, the most successful on the internet today, accounting for greater than 90% of attacks. Spear phishers gather personal information about victims from social media and other sources to use in bait emails to increase the chances users will believe them.

A third technique, called whaling, focuses on bigger targets, such as C-level executives, politicians and celebrities. "Whaling emails and websites are highly customized and personalized, often incorporating the target's name, job title or other relevant information gleaned from a variety of sources," according to TechTarget.

Protect Yourself

To prevent phishing attacks, you need to train users to identify and avoid phishing emails. Beyond that, you need email security with advanced features designed specifically to combat this threat.

Such features include a sender policy framework, which checks if incoming email was sent by authorized hosts; auto-whitelisting, which automatically adds and removes listings based on preset criteria; and a regularly updated spam filter that recognizes and sifts out potential phishes.

Phishing is the most successful attack vector used by cybercriminals and the primary method used to deliver ransomware. Failing to address phishing opens you to a cyberattack.

RECOGNIZE & FEND OFF **WEB-BASED THREATS**

Phishing poses a serious cyber risk to SMB organizations, but it's far from the only one. Cybercriminals still use plenty of other methods to break into networks and steal data. The hacker bag of tricks contains plenty of web-based threats such as website hijacks, drive-by downloads and plug-in exploits.

Hackers use web-based attacks to download malicious code onto networks to alter files, disrupt network operations and steal information. Common web-based attacks you need to know about include:

CLICKJACKING – Hijacking a legitimate website link and redirecting users to an infected website, where users either share confidential information unknowingly or trigger an intrusive action such as turning over a computer's camera or microphone to hackers.

DRIVE-BY DOWNLOADS – Secretly downloading malware onto a system when the user visits a website. Typically, the malware hides in the background until it's ready to do its nefarious work, which could be stealing information or turning the machine into a bot controlled remotely by hackers.

WATERING HOLE ATTACKS – Compromising a group of users through infected websites that targeted group members are known to visit. Once a user visits one of the websites, malware is downloaded or sensitive information is stolen to gain network access.

PLUG-IN VULNERABILITIES – Exploiting vulnerabilities in commonly used tools such as Java and file formats such as PDF, CSV and HTML to deliver malware.

SOCIAL ENGINEERING DATA THEFT – Using data shared willingly by users on social media to break into networks and to craft phishing emails that trick recipients into opening infected attachments or visiting compromised URLs.

MALVERTISING – Hackers can infect online advertising campaigns like banners that run through ad networks and are encountered on popular, trusted sites to infect unsuspecting users.

Preventive Steps

Preventing web-based threats requires businesses to stay on constant alert. For one thing, you need to educate users on safe web browsing practices that help prevent downloading malware onto their machines and your network.

You also must deploy and maintain security tools such as antivirus solutions, firewalls and web filters. Keep these tools up to date because unpatched files and systems make it easier for hackers to inject malware onto networks. Don't ignore patch management. Every time a software or security vendor releases a patch, be ready to test it and implement it to minimize the chances of a web-based attack.

Lastly, you need endpoint security to protect the edges of your network by keeping your browsers clean, performing fast malware scans, removing compromised mobile devices from the network, and performing threat analysis whenever suspicious code is identified.

By taking these steps, you minimize the chances of suffering a web-based cyberattack.

KEEP AN EYE OUT FOR **EXPLOIT KIT THREATS**

Web-based attacks sometimes involve exploit kits. These kits are an unfortunate side effect of the technology world's as-a-service evolution, giving cybercriminals yet another way to carry out their dirty deeds. Just as easily as well-intentioned businesses can leverage software-as-a-service (SaaS) or infrastructure-as-a-service (IaaS) to cut costs and build new efficiencies, those with less noble intentions can take advantage of malware-as-a-service (MaaS) to more easily execute their cyberattacks.

MaaS enables authors of exploit kits to monetize their "offerings" by making them available for sale or lease on the Dark Web to other cybercriminals who may or may not possess the skillset to create these tools themselves. Exploit kits have lowered the barrier of entry into cybercrime, helping to create a much larger threat landscape for businesses.

How Exploit Kits Work

An exploit kit essentially contains a library of known vulnerabilities in popular software applications like Adobe Reader, Skype, Internet Explorer, iTunes, Chrome, Firefox, Java and many others.

Exploit kits are unleashed via spam campaigns, or hosted on malicious or compromised websites. They can even be deployed via malvertising campaigns to compromise online ad networks. Users who click a link, browse to an infected site or open an infected email attachment unwillingly open themselves up to attack. The exploit kit scans the PC looking for vulnerable applications. If found, it can then open a backdoor onto the PC and your network.

But that's just the beginning. The exploit kit then calls back to a command and control server to accomplish its true mission: delivering a malicious payload through the door it has now opened onto your PC. That payload may be ransomware, a credential-stealing Trojan, code to turn your PC into a bot to power the spread of more exploit kits, or any number of online threats.

Exploit Kits are Big Business

With names like Angler, Neutrino, Nuclear and RIG, exploit kits have helped create a widespread criminal enterprise with lots of revenue potential. Cisco has estimated the Angler kit alone generates as much as $60 million annually.

Kit authors take a business-like approach to MaaS, even regularly updating their kits, much like software developers do with their applications, and offering their "customers" product guarantees. "Developers create tools that they sell or rent to customers through online black markets, complete with sales, money-back guarantees, and reputation systems to provide customers with assurances that they won't get ripped off," according to reports.

Exploit Kit Defenses

Since exploit kits typically attack unpatched systems and applications, the best defense is to keep up with security patches. While Zero-day attacks get lots of headlines, the vast majority of vulnerabilities exploited by these kits are already known and addressed by security updates.

Too many businesses simply do not patch applications as often as they should. There are certainly legitimate reasons to use older versions of applications – for running legacy applications that only work on older versions of Java, for example – but IT admins should take care to provide extra visibility into those systems. For all remaining systems, patching is absolutely critical.

Even threats posed by exploits developed to evade detection by antivirus engines are nullified if the systems they encounter are fully patched. To ensure patches are applied as they become available, consider an automated patch management solution, which empowers IT to manage all security updates.

Ideally, you want to deploy an endpoint security solution with integrated patch management. This gives you a single tool to defend against malware while eliminating vulnerabilities caused by unpatched, outdated applications. The following VIPRE for Business solutions include integrated patch management: VIPRE Endpoint Security, VIPRE Business Premium and VIPRE Internet Security Pro Small Office.

Each year, software and secure vendors issue dozens, possibly hundreds, of patches. It takes a lot of effort to keep up with them all. That's why you need a patch management strategy that includes automated tools. What you don't want to do is ignore security patches and leave your business open to cyber threats, including those delivered by exploit kits.

Patching Made Easy

VIPRE's integrated patch management capability enables you to seamlessly manage updates for more than 30 popular software applications, including:

- Adobe Acrobat
- Adobe AIR
- Adobe Flash Player
- Adobe InDesign
- Apple iCloud
- Apple iTunes
- Apple QuickTime
- Google Chrome
- Java
- Mozilla Firefox
- VMWare Workstation
- WinZip
- Wireshark
- Yahoo Messenger.

Learn more at
www.VIPREAntivirus.com/Business

FOLLOW BYOD **BEST PRACTICES**

The BYOD trend has complicated the responsibilities of IT administrators and security managers in defending their organizations against phishing, ransomware, web-based threats and other cyber risks.

Ever since BYOD (bring your own device) entered the IT lexicon, they've been dealing with how to protect business networks while letting employees use personal mobile devices in the office, at home and on the road.

It's not an impossible task, but it takes a solid understanding of the potential dangers BYOD presents to your organization. You need to understand the risks and their potential impact on the business. Then you can devise a strategy to address those risks by securing devices and preventing them from giving hackers a way onto your network. With a mix of robust security, management tools and user education, you can make BYOD work for you without exposing your data.

BYOD Popularity

Gartner predicts that by 2017, half of all companies will require employees to use their own devices at work. Clearly, the business world is embracing the BYOD concept, but how well are they handling it?

Not too well. A study by Bitglass found only 18% of education organizations and fewer than 60% of finance companies had implemented access controls in conjunction with their BYOD policies.

This is troubling, especially considering education and finance are favorite cybercrime targets. But whatever your industry, if you adopt a BYOD policy, do it safely. And that means taking steps such as:

- **Deploying mobile device malware protection**
- **Implementing strong user authentication and password policies**
- **Blocking unsanctioned applications**
- **Wiping devices that are lost or stolen**
- **Installing VPN applications for secure network communications**
- **Creating a separate gateway with optimized security controls for mobile devices accessing your network**
- **Educating users on configuring devices for maximum security and avoiding unsecure networks**
- **Auditing mobile devices to ensure compliance**

BYOD Dangers

If you neglect to secure mobile devices, you are playing with fire. New malware threats pop up constantly and many specifically target mobile devices. A single infected device can unleash a virus, worm or ransomware that could potentially shut down a network.

Recovery costs and lost productivity can quickly add up. Depending on the size of your company, you'd be looking at spending hundreds of thousands or millions of dollars to remediate something a much smaller investment could have prevented.

Protecting the Network

Any organization that embraces BYOD should seriously consider implementing a Mobile Device Management (MDM) solution that centralizes the security management of mobile devices to prevent malware and wipe data if needed.

As part of any mobile device management policy, you need to enforce user access policies by requiring strong passwords or passphrases to protect data, and controls to prevent access of unsanctioned applications and websites.

Mobile malware protection also is critical. At its most basic, mobile antivirus performs malware scans that prevent infections. But solutions have become increasingly sophisticated, even offering some of the same features as MDM, such as remote monitoring, device lock, alarm and wipe, as well as GPS capability to locate lost or stolen devices.

Productive and Secure

BYOD offers the benefits of giving users device choices, which makes them more productive and happier at their jobs. Just don't let BYOD compromise your security.

ASSESSING YOUR VULNERABILITY **TO RANSOMWARE**

As the ransomware epidemic continues to spread, ask yourself how vulnerable your business is to cyber-extortion. A vulnerability assessment is a good first step to strengthening your defenses.

What is Ransomware?

Ransomware is malware that infects your PC or network by encrypting your data, demanding a ransom to restore access to your files.

Fending off ransomware attacks requires a multilayered strategy. If all you've done so far is to rely on antivirus scans and the good sense of your users to not click on suspicious emails, you're doing less than the bare minimum. Yes, antivirus is a vital element in your malware defense, but it cannot do the job alone. And failing to educate users on the dangers of phishing amounts to business malpractice.

With that in mind, here are six questions to ask in assessing your ransomware vulnerability. Your answers should make it obvious in which areas of security you need to invest:

1. Are you training users on the dangers of phishing?

Considering 93% of phishing emails contain ransomware, this is a must. You need to invest in an education program that explains how phishing attacks occur and, through repeated training exercises, conditions users to spot and report suspected phishing emails.

2. Do you back up your business data regularly?

Surveys have found that as many as 53% of businesses don't back up every day, which in a digital context is the equivalent of playing with fire. Backing up is the most basic – and one of the most effective – steps to avoid having to pay a ransom to retrieve your data.

3. Do you have anti-phishing email security?

You should deploy policy-based email security at the server level to defend against phishing as well as spam, viruses and other threats. Your email security solution should include secure email inspection, cleansing and management.

4. Have you deployed endpoint security with specific ransomware protection?

As malware threats increase in sophistication, so should the tools to combat them. Endpoint security is integral to a layered defense strategy; you need to leverage an advanced solution that effectively helps prevent ransomware, and defends against the malware and attack vectors that cybercriminals use to spread this pervasive threat.

5. Are your mobile devices secure?

Your security strategy must take into account all the devices that access your network, which means all laptops, smartphones and

tablets should be secured. You also should consider encryption and strong authentication policies for added protection.

6. Do you have a patch management policy?

Ransomware authors often exploit vulnerabilities in Microsoft Office files, JavaScript downloaders and Windows Scripting Files (WSF) to carry out attacks. That's why testing and implementing patches when they are released is imperative. An automated patch management solution is your best bet.

If You Said No

If your answer to any of the above is no, you have a problem. If you want to avoid a ransomware attack, start working on turning those noes into yesses.

TEN SECURITY TIPS **FOR SMALL BUSINESSES**

Too many small and medium businesses spend their limited funds on security products only to see their investment – and best intentions – wasted when they fail to implement the most basic security practices.

The simple truth for any business is you are always just one bad user decision away from being infected by malware. Misconfigure your firewall, grant the wrong person administrator rights or fail to update your antivirus, and you open the door wide open to cybercriminals to steal your data.

Here are 10 security best practices to shore up your defenses:

1. Install Antivirus

We'll get this one out of the way first!

Your best defense against the vast majority of malware is your antivirus solution. Select an antivirus solution that performs strongly with independent tests such as AV-Comparatives. Look for advanced features that protect against prevalent threats like ransomware, and choose an endpoint security solution that offers protection at multiple attack points to defend against bad websites, phishing and spam, malicious URLs, Zero-days and other online threats.

2. Restrict Administrator Rights

Only authorized, knowledgeable IT admins should have administrator rights to your PCs. While restricting rights may feel inconvenient at times for small organizations, granting administrator rights to a broad user base is a big risk. To maintain the highest security standards, you need to ensure users cannot change critical settings, download and install whatever software programs they wish, or disable the security tools you've put in place. Moreover,

some malware is unable to execute and make malicious system changes if the user is logged in without admin rights, creating an additional layer of defense against malware users may encounter.

3. Install and Update a Firewall

Be it the Windows firewall or a third-party firewall application, be sure to install a firewall to defend against malicious network traffic. Firewalls monitor and control traffic in and out of your network. To protect against downloading malicious content or to stop communication to harmful IP addresses, a firewall is a critical line of defense. Always keep it updated or it will start to miss threats.

4. Implement Patches

Don't ignore those prompts to update popular software applications used in your organization. In many cases, prompts to update Adobe, Java, Chrome, iTunes, Skype and others are to fix newly discovered security vulnerabilities in those products. Cybercriminals exploit vulnerabilities to open a backdoor onto your systems to drop malware and infect your network. Implement an automated patch management solution to address this issue, or select an endpoint security solution with patch management included.

5. Enforce Password Policies

Users may view password updates as a chore, but password implementation and enforcement are a must. Require strong passwords or passphrases to maximize effectiveness, implement regular updates and instruct users not to share them.

6. Lock Those Screens

All computing devices, including laptops, tablets and smartphones, have screen-locking features for security purposes. Be sure to enforce a short lock-screen timeout as added protection, especially in environments where users can walk away from workstations without logging off.

7. Secure Wi-Fi Routers

Wireless routers and networks are notoriously easy to break into, so take extra precautions in securing them. Change the network names and passwords that come with each router, and don't forget to activate its encryption capabilities. Use a separate Wi-Fi network for business guests. Also consider not broadcasting your network ID for added protection against hackers trying to discover and access your network.

8. Secure Your Browsers

Configure web browsers to avoid inadvertent malware downloads by users. Steps to take include disabling pop-up windows, which can contain malicious code, and using web filters that warn you of potential malware attacks and harmful sites. Also, pay attention to browser privacy settings to prevent any private information from being siphoned by fraudsters and cyber-thieves, limit users ability to install browser plug-ins, consider disabling vulnerable applications like Adobe Flash, and always ensure you're using current and fully patched browsers when possible.

9. Use encryption

Many machines come with built-in encryption, both at the disk and file levels. Take advantage of each device's encryption capabilities to prevent data from getting into the wrong hands when laptops, external hard drives, USB drives and other mobile devices are lost or stolen.

10. Train and Recruit Your Users

Security isn't successful in a vacuum. Your users can be your biggest liability or your biggest asset. Engage your users and educate them on security best practices and why they are important. Train your users to spot threats, like malicious phishing attacks or strange PC behavior, and alert your IT leader immediately.

EDUCATE USERS **ABOUT THESE COMMON MISTAKES**

The need for proper cybersecurity training for users cannot be emphasized enough. User actions contribute to most breaches. For instance, 63% of confirmed breaches involve "weak, default or stolen passwords," Verizon revealed in its 2016 Data Breach Investigations Report.

But mishandling passwords are just one of many mistakes users make that can put your business at risk. The following is a list of nine common no-noes. Find out if your users are making them, and come up with an education plan to modify risky behaviors.

1. Sharing passwords, intentionally or not

Whether users share passwords with colleagues, friends and family intentionally or leave them on sticky notes by their computers, the effect is much the same: An unauthorized person can use the password to get into the network.

2. Using weak, or default, passwords

Users often don't bother to change default passwords, be it on websites, applications, machines or Wi-Fi routers, which creates vulnerabilities. Or they'll use easy-to-guess names or dates because they're easier to remember.

3. Opening suspicious emails

Even when users suspect an email is bad, many will still click an attachment or a URL, possibly unleashing a virus or ransomware in your network.

4. Sharing personal information

As with No. 3, users often act against their own instincts, providing information such as bank account numbers, credit card information and Social Security numbers when asked by email or a website reached through a suspicious link.

5. Turning off security controls

Be it firewalls, antivirus or pop-up blockers, turning off any security tool poses a serious and immediate risk. Yet, users sometimes do this because they view them as an inconvenience or waste of time.

6. Leaving machines unattended

Leaving laptops on and unlocked and walking away is a big no-no. Yet, users do this not only in the office but also in public places such as coffee shops.

8. Using social media carelessly

Social media-related risks abound, from revealing too much information to sharing employer dirty laundry to clicking malware-infected links.

9. Improperly sharing files

Users that transfer files from work to personal machines, either by email or using USB sticks could be flirting with malware infections, as well as violating applicable data privacy laws.

CONCLUSION

Every day, new cyber threats seem to pop up. Keeping up with them all is no easy task for SMBs, but you simply cannot ignore them because doing so puts your business at risk. Avoiding risk takes a combination of technology, well-crafted policies and user education. If you follow the advice put forth in this guide to secure your business, you minimize your chances of falling victim to a cyberattack.

ABOUT

VIPRE is the trusted antivirus and endpoint security protection for millions of home users, and tens of thousands of small and medium businesses. Its malware protection consistently earns the highest ratings possible from the world's leading independent authorities on antivirus performance. Easy to install and simple to use, VIPRE enables customers to quickly protect their data from more than 350,000 new online threats every day, including viruses, spyware, Trojans, ransomware, bad websites, harmful email and more. All VIPRE customers receive free U.S.-based technical support. To learn more, visit www.VIPREAntivirus.com and try it free for 30 days.