BALANCELOGIC
THE ANSWER FOR SMALL BUSINESS

what's your Cybersecurity Plan?

The small business guide

Contents

— INTRODUCTION

Small businesses count on cyberspace to leverage advantages.

The internet has created many opportunities for businesses. From tapping into the global market to effecting cost savings, small businesses count on cyberspace to leverage these advantages and maximize revenue.

The pandemic resulted in many small businesses moving their whole operations online—creating a field day for cyber threat actors. Unfortunately, as more businesses decide to make the switch, few companies – especially small enterprises – are adequately prepared to deal with the threat of cyberattacks.

Small businesses often lack the capital to invest in strong cyber defenses.

Many small enterprises may have a false sense of security, believing they are unattractive targets to criminals based solely on their size. The common belief that, “My business pales in comparison to Facebook or Google. Surely, hackers would not look my way,” is as misguided as it is wrong.

These cyber criminals may be looking for personal information to engage in identity theft and grow their wealth through extortion and blackmail, both of which make small businesses an enticing target. Small businesses, as cyber criminals know, often lack the capital to invest in a strong cybersecurity defense — which also makes hacking exceptionally easy.

Even if small enterprises yield lower returns in comparison to the rewards for breaching the cyber defenses of a major company such as Google, for instance, hackers can easily make it up by pillaging more small businesses to make up the difference.

Over the years, cyber criminals have turned to increasingly sophisticated methods to strike, becoming an insidious force able to slip into the inner workings of a business and, before anyone can detect them, quickly **wreak havoc.** Their methods are as varied as their motives. This book examines the many ways threat actors can infiltrate small enterprises and the tools you can use to slow them down.

> “It is easier to attack than it is to defend, so make sure you deploy defense in depth.”
>
> — BILL CAMPBELL
> CEO, BALANCELOGIC

60%

Ransomware

Ransomware is a crowd favorite amongst the hacks these criminals have in their toolbox. It is a malware that, once installed on a computer, encrypts the information ranging from files to operating systems, rendering them completely unusable and inaccessible until you obtain a decryption key. Or, more accurately, have paid the ransom for the decryption key.

This type of cyberattack is popular because criminals are able to do more than shut down a computer upon obtaining access. If the malware they use tweaks the organization's software, it can propagate throughout the network of devices, and put the entire the network of computers in the mastermind's hands. Talk about a nightmare.

In addition, once criminals have slipped their ransomware into the system, they can pull off shenanigans from blocking access to deleting system backups, making recovery difficult or even impossible. They may then proceed to taunt and pressurize victims to pay – not just for the decryption key to unlock their systems but also for their silence.

It gets worse. Throughout the disruption, ransomware can result in economic and reputational damages, making immediate recovery difficult for small enterprises.

As many as 60% of targeted small enterprises closed after a ransomware attack.

All businesses are targets for cybercrime, regardless of their size.

Any of these malwares could also contain codes to delete data – affecting the availability of your important assets and information and making these an immediate danger to your businesses' daily operations. Insidious malware may make your small businesses even more vulnerable to these threats because there are multiple avenues for these codes to be downloaded accidentally—especially if the computer is used both for work and personal purposes.

One such incident happened in 2011 in Chicago. Hackers planted malware into the cash registers of a newsstand. The malware swiped customers' credit card details and sent the information to the cyber criminals. **This single incident incurred almost $22,000 in losses for the small business owner** and serves as a stark reminder that all businesses are targets for cybercrime, regardless of their size.

Read on to learn more about different types of malicious codes.

Malicious codes encompass a range of malware that includes viruses, worms, Trojan Horses, and malicious data files.

TROJAN HORSES

True to its name, Trojan Horse is a computer file that conceals a malware. It's extremely common for "free" software to contain a Trojan Horse that tricks users into thinking that they are using legitimate software when, in reality, the files are actually wreaking havoc on their computer. One common example is the fake antivirus Trojan.

These Trojans often mimic legitimate security software to steal information from the unsuspecting victims and – due to their ability to make multiple system modifications – can be difficult to remove or disable.

VIRUSES

Viruses are codes that are able to damage computer systems and spread easily. Employees may spread them by using removable mediums like thumb drives, opening malicious email attachments, or simply visiting a malicious website.

For example, the ILOVEYOU virus in **2000 affected tens of millions of computers** worldwide and caused billions of dollars in damage.

MALICIOUS DATA FILES

Malicious data files are often non-executable but abuse the loopholes in the software program used to open it (like Microsoft Word or Adobe).

Masterminds who utilize these tactics insert and execute malicious scripts or code that often goes undetected. Once installed, hackers use these malicious data files to install even more malware on an unsuspecting victim's system. This gives hackers the ability to control the computer and steal, destroy files, shut down a computer, and even use it to attack another device.

WORMS

Worms are a type of virus that propagates independently across computers. Their primary purpose is to utilize all of the computer's resources, making it stop responding to the user.

> “It takes 20 years to build a reputation and few minutes of cyber incident to ruin it.”
>
> — STEPHANIE NAPPO

Denial of Service Attacks:
A Two for One Deal

A denial-of-service (DoS) attack occurs when a cyber criminal essentially cripples access to information systems, devices, or network assets. A typical DoS attack keeps legitimate users from utilizing services ranging from their emails and websites to any services that would involve an affected device or network. To do this, threat actors attempt to overwhelm a targeted device or network with so much faux traffic that the target can't react and crashes, keeping actual users from accessing the services.

A DoS attack is extremely expensive for any organization, as they lose both time and money when their server crashes and is inaccessible. In addition, DoS attacks may provide a cover for hackers to conduct further illicit activities.

For small businesses, the DoS attack could potentially serve as a decoy, diverting the attention of IT personnel. **While your staff is focusing on the attack, hackers are working overtime – stealing data that leads to further reputational and economic damage.**

Read on to learn about various types of DoS attacks.

DoS attacks may target more than one site or system at a time. An attack becomes a 'distributed denial of service', or a "DDoS," when it comes from multiple computers instead of just one. This is the most common form of DoS attack on websites.

SMURF ATTACKS

One form of a DoS attack, known as a smurf attack, occurs when malicious actors dispatch a ping with a spoofed IP address, usually the target server address. The ping goes to an intermediate IP broadcast network, where it is amplified since all requests are related to all the network hosts. Let's say an IP broadcast network had 100 network hosts. The targeted server would then receive a hundred requests, one from each host. By taking advantage of the number of hosts in the IP broadcast network, the amplification of the attack can be magnified. When sufficient pings are dispatched to the IP broadcast network, a **server gets overwhelmed and crashes** because it is unable to keep up with processing all the junk requests. This leads to legitimate requestors facing the DOS interface.

SYN FLOOD ATTACKS

Another type of DoS attack is known as a syn flood, in which the hacker dispatches an incomplete request to the targeted server. The incomplete request fails to meet the requirements of the 'three-way handshake,' which the IP network utilizes to establish a connection between the client or local host with the server. This means that the request is held up at the server port with no way to proceed – effectively blocking it from processing other legitimate requests. The hacker dispatches more spoof requests, eventually blocking all available ports and leading to a DoS for actual users.

In general, people are the weak link in security.

You're not likely to hand over your password to a hacker, but you may have done it without realizing it. Cyber criminals are savvy and use phishing scams to fraudulently obtain personal and financial information ranging from login details to credit card numbers.

Phishing emails take all kinds of forms: requesting users to download a file or a link; a claim to be someone the user knows; or even a company with a fake or spoofed logo that makes it appear credible. The email message is accompanied with a general sense of urgency pressuring the user to respond as the hacker wants. In each case, a link or a file are included in the email.

Once that link or file is opened, the hackers install malicious software (like ransomware or corrupted files) on the device that locks the user out or blocks access to their data. That's not all: the threat actors can also mine for personal details and passwords, often **granting themselves administrative authority** – which provides additional network access for even greater damage.

Threat actors notoriously use these types of attacks to breach the cyber defenses of government agencies and several other large-scale businesses, like the Solarwinds attack in 2020, in which a company unwittingly sent out a software update that included hacked code that left government agencies vulnerable for months afterward.

Phishing and Spearphishing

Social engineers use phishing access sensitive information, sometimes in a way to create fear and confusion and prompt someone to act.

Despite increasing public awareness, successful phishing scams are increasing exponentially because they are so difficult to detect.

What should you and your employees look for?

Details. For instance, a phishing email may appear to reference an existing client – but if you look closer, you might notice differences in how the name is spelled. Examples would be switching ‘l’ with ‘1’ or capital “i” with small ‘L’. Such small and barely discernible discrepancies enable these emails to slip past employees and lead to your company right into criminals’ hands.

These emails usually carry an urgent tone and beg the user’s immediate attention, threatening unpleasant consequences if ignored. Hackers do this to pressure the recipients into acting quickly, keeping them from looking any closer and making them overlook the possible red flags within the email.

Spear phishing and phishing have important distinctions.

Phishing emails are usually sent to a large group with the expectation that only a small percentage will take the bait. These types of email are sometimes easier to spot because they contains key characteristics, like being extremely and noticeably vague, which makes them slightly easier to notice.

Spear phishing, however, is more elaborate and is usually directed to one target with the explicit intention to fool them. This type of scam is usually harder to root out because they are often personalized and can have significant variations tailored for specific situations. This makes it harder for victims to identify a spear phishing email.

It's a Jungle Out There: The Guerrilla Tactics of Ransomware

To better protect and defend your small business, you first need to understand how these cyberattacks are possible.

The threat landscape has evolved over the years and today, hackers approach their mission in far more sophisticated ways than ever before. The old-school brute-force tactics, like going through all the different possible password combinations, are now more technical or more intricate (or both), using social engineering to **manipulate victims into handing over data**.

Business owners use devices to run their operations, and most cyberattacks stem from these. But how are they installed?

That depends.

Oftentimes, small businesses that fall victim to phishing scams receive an email with embedded malware that business owners unwittingly download themselves.

Malware may also be installed when business owners attempt to download a free software off the internet, thinking it will aid their business or daily life. In reality, it may actually be a Trojan horse. These tactics all incorporate some form of social engineering.

> **"Ransomware is unique among cybercrime because, for the attack to be successful, it requires the victim to become a willing accomplice after the fact."**
>
> —JAMES SCOTT

A Social Situation: Social Engineering Attacks

Malicious actors breach a small business's cyber defenses by putting some social engineering tricks to work.

Social engineering exploits human behavior to access to buildings, systems, or data instead of relying on technical hacking knowledge. Because it is based on human behavior, criminals may sometimes slip past even the most vigilant employees. The perpetrator relies on human empathy to convince unsuspecting employees to "assist" in their heist.

Phishing, which we covered on page 13, is one form of social engineering. Let's take a look at the multiple other social engineering tactics malicious actors use to scam small businesses.

BAITING

Conducted virtually and physically, baiting uses carefully laid traps that enable a hacker to either install malware into your systems or steal personal information.

You know the online ad that always captures your attention? It may be dangerous. When done virtually, hackers bait you using attractive online advertisements that redirect you to malicious websites or encourage you to download malware. Business owners who use the same computers for work and personal purposes should be extra careful when visiting sites to ensure that they do not accidentally pick up the malware while surfing the internet.

However, virtual baiting isn't just restricted to online advertisements. At one company, some employees received an email that contained an excel sheet titled, "2011 recruitment plan." The title intrigued some employees, who opened the excel file – which in reality was a malicious data file disguised to tempt and exploit the employee's curiosity. The result? **Hackers gained access to the entire network after the malware propagated itself.**

Physical baiting is also a threat for your small business. It can be hard to resist looking at a thumb drive you find in a parking lot—and threat actors know that. They may plant malware-laden plug-in devices, such as a thumb drive, someplace your employees would find it, like the parking lot outside of your business. The thumb drive may even look legitimate, with a label that indicates it is the property of your company. The employee picks it up and plugs it into their computer, triggering an auto-installation of malware on their computer and your network.

SCAREWARE

Scareware is another type of social engineering tactic that preys on fear and anxiety to trick victims. Scareware consistently causes false pop-ups to appear, often claiming that the device is already infected. It attempts to coerce the user to download antivirus software or directs them to another website to rectify the 'problem.' More often than not, the antivirus software is fake and is riddled with malicious code. Beyond allowing hackers to steal personal and financial information, the **code may be used to alter your computer's settings,** making it difficult (or impossible) to remove or disable the software.

Users commonly receive spam emails about bogus warnings, or are encouraged to buy or download suspicious software that looks legitimate. These emails also fall under the category of scareware, because they try to persuade vi ictims to believe in non-existent threats and take the "precautionary measures" the hackers are counting on.

PRETEXTING

Pretexting is an increasingly popular tactic used for phishing. Often, pretexting is the first phase of a larger crime that involves hackers pretending to need sensitive information to carry out their attack.

Scammers may adopt the persona of an authoritative figure -- maybe a company's executive or the police -- to justify demanding answers. The answers may contain the victim's identity and potentially be used to mislead another colleague. As employees are more likely to trust someone claiming to know one of their colleagues, these details give the hacker the credibility needed to attain the trust and manipulate the coworker. To make matters worse, **these details could be sold off on the black market for use in identity theft**.

Pretexting may come in the form of a phone call instead of an email. Be wary of calls requesting a wide variety of answers or details like home addresses and Social Security numbers. They may well be hackers working behind the scenes to commit a crime.

Scammers may adopt the persona of an authoritative figure.

Protecting Your Business

Now that we have covered the common ways cyber criminals carry out their scams, it's time to **learn to protect ourselves and our small businesses**.

How Vulnerable are You?

To better protect your small businesses from cyberattacks, you should first evaluate your risk.

The U.S. Small Business Administration (SBA) offers several free resources to assist you. Among them is a cyber planner that allows you to customize the various areas of security concerns that may render your business vulnerable. You complete a simple questionnaire and the website generates a very detailed report, addressing the appropriate measures you should take.

The Department of Homeland Security (DHS) offers a free vulnerability scan that helps protect your internet-connected devices from weak configuration and known vulnerabilities. In addition, weekly reports will enable you to effectively plan and manage your cyber security infrastructure.

Visit the Cybersecurity & Infrastructure Security Agency to learn more about these and other resources to protect your organization.

> **"Hackers only need a small opportunity to access your network and upend your entire business. It's up to you to make sure they don't get that chance."**
>
> -BILL CAMPBELL
>
> CEO, BALANCELOGIC

An Ounce of Prevention

Experts recommend that all businesses reinvest at least three percent of business revenue into boosting the cybersecurity of the business itself. Whether you engage an IT consultant or hire an IT specialist, having personnel that can immediately respond to an attack helps ensure minimal damages to your company.

Among small businesses, emails and employees are common ways hackers obtain sensitive information. Providing cybersecurity training for your employees – who are often the ones accessing the emails and answering phone calls or receiving guests – is imperative.

Software and Systems

Occasionally, companies that program software and systems offer patches for newly discovered vulnerabilities. Staying current on information about patches and immediately installing them to your respective software and systems is key to plugging any vulnerabilities that could give hackers a foot in the door to your network.

Anti-virus software, in particular, must always be kept up to date as patches both guard your devices from the latest known vulnerabilities and improve app functionality.

Most apps offer the option to automatically update when a new patch is released. Enabling that function will save you the hassle of combing through your software and updating it manually.

Payment systems must also be secured by working only with the most trusted and validated tools and anti-fraud services. These may involve working with banks and bearing additional security obligations to protect your business.

Knowing that **the average breach costs millions of dollars**, the effort is well worth the effort on your part.

Passwords

According to a former Deputy Director of Enterprise Information Security at the CIA, hackers obtain passwords through three different means: guessing, using algorithms to crack the code or to capture the passwords either digitally from a database, or by swiping a handwritten note that contains the password.

With that in mind, arm your employees' logins with the strongest tools possible. Whether it is two-factor authentication, biometrics, or security keys, these tools provide additional security in case hackers obtain one of the passwords.

In addition, urge your employees to use different passwords for different websites. At the very least, they need different passwords for work and personal purposes. If your employee's personal account is breached, your business accounts will still be protected.

Strength in Numbers ... and Letters

Strong passwords are critical to protect your most sensitive trove of information. The strongest passwords are often the longest ones with at least 10 characters. Including special characters, uppercase and lowercase letters will also enhance make your passwords more difficult for a hacker to guess.

Stay away from common passwords or ones that consist of information readily available. For instance, it may not be wise to use your birthday as a password because this information is easily obtained from your social media accounts.
You may find yourself in a quirky mood when you decide on 'qwerty' to be your password but rest assured, when criminals take over your computer, 'quirky' will probably be the last mood you would be in. Common passwords like '12345678', 'password' and 'abc123' should also not make the cut.

NordVPN compiled a list of commonly used and weak passwords – if you find your password on their list, change it immediately.

Assuming you have some of the most complex passwords and unique ones for different web- sites, don't store a list of them on your computer or on a piece of paper. Save them on another device that is not connected to your computer. If a hacker installs malware into your device, it is a simple matter for them to fish for the list of passwords – which means even your strongest passwords do you no good. Alternatively, try using a password manager to keep track of passwords.

Change is Good

Experts advise changing your passwords once every 60 to 90 days to keep any malicious actors guessing. After all, **one million passwords are stolen every week**. Changing your passwords often ensures that – even if yours gets stolen – the password will soon be deactivated. And yes, this also means that your new passwords should never be recycled from the past.

Be cautious when using public Wi-Fi – you're not the only one tapping into it.

Connecting to the Internet

Malware and corrupted files can be installed via links or infected drives, so always err on the side of caution. If you encounter any links that seem to be suspicious while surfing the internet, avoid clicking them and delete them right away. Even if the source is familiar to you, it's not worth the risk. A simple click might be the very thing that leads your company to a cybercrime that could cost you thousands of dollars.

It is also a good habit to refrain from picking up and using any thumb drives or portable media that you can plug into a computer that you found for fear that they might contain malware. Use thumb drives only if your computer's antivirus program allows an auto scan for viruses in USB drives upon insertion. Heads up: This function is often not switched on by default, so ensure the function is activated before plugging in the device.

Be cautious when using public Wi-Fi – you're not the only one who's tapping into it. Hackers can also connect and run interference through public Wi-Fi, so restrict the type of business you conduct while out and about. Digitally set up your device to limit who can reach and tamper with your machine.

If your business offers digital payment processing via debit or credit cards, always ensure the device used to receive payment is not connected to a computer that is used to surf the internet. Isolate payment systems from vulnerable programs that could be easily exploited.

Communications

Detecting suspicious emails can go a long way to protecting your commercial enterprise from hackers. Research conducted into 55 million emails reveals that **one in every 99 emails is a phishing attack**. The frequency of such emails indicates that it is imperative for you to learn to recognize these emails for what they are – or pay the consequences.

Encounter a suspicious email? Beyond reviewing the sender's name, you and your employees should always double check on the domain name for any discrepancies. Also pay close attention to any correspondence that requests confidential or private information. No banks, for instance, would request you to hand over personal details via an email. When unsure, always call the sender directly to make sure the request is legitimate.

When it comes to links or attached files, hover your cursor over the link or file and view the alternate text. If the alt text does not correlate with the link or seems in any way suspicious, follow your instinct and do not engage with the email by clicking links or opening files. Given the frequency of phishing emails, there is a good chance the email was meant to phish your company.

Cybersecurity Apps

Fortunately, when it comes to battling cyberattacks, you're not alone. Cybersecurity apps can help you counter hackers. These apps block threats and, in the event of a cyber breach, minimize the damage. Apps like Vipre help to prevent threats like malware and ransomware by encrypting your emails, providing comprehensive email, and endpoint security and privacy. Real-time threat intelligence provides immediate notification of a breach, allowing you to take action. In addition, pricing is scalable, depending on the number of devices the app is covering.

Norton 360 with LifeLock also protects your digital privacy. A secure VPN feature will ensure no private information is pilfered by hackers who connect through public networks. Its LifeLock feature also offers reimbursement for stolen funds in any cases of identity theft. LifeLock also possesses features like cloud backup for Windows, which ensures that any data lost in a cyberattack can be easily restored. There's also virus protection and ad-tracker blocker among its many other functions – providing an all-in-one solution for your cybersecurity needs.

There are many cybersecurity apps available online, each with its own pricing models. Educating yourself about the different capabilities of each app can help you select the one that best protects your business' digital vulnerabilities.

If the Worst Happens

Sometimes, even the best defenses are breached. If your business is the victim of a suspected cyberattack, notify the IT department and the manager immediately. If left unchecked, cyberattacks can escalate as some malwares are programmed to exploit digital weaknesses in software and devices and propagate across the system.

Next, disconnect the affected device from the internet and disable all remote access. Change passwords for all affected accounts and, if there are any pending updates for the antivirus or operating system, install the patches as soon as possible.

It may be a tempting to wipe all data and refresh the system. Don't. You won't just wipe your data – you will also destroy digital evidence. Preserving evidence is vital for you to figure out how the hackers got into your system and help you to take precautionary measures to ward off the same attempt again. If you are not well-versed in the what to do after a breach, consider hiring a cyber investigator to get more details for the attack. Firewall and email service providers and antivirus software might be able to point you in the right direction.

If you are covered by insurance, make sure to notify your insurance providers. Cyber Liability Insurance assists in breach and attack recovery efforts, helping you identify potential cyber exposures and defray costs addressed with future cyber incidents.

All businesses are targets
for cybercrime,
regardless of their size.

— CONCLUSION

The Bottom Line

The ramifications of a data breach include more than dollars. For a business, it could mean losing hard-earned credibility and trust with your clientele which, if anything, is even more devastating than a financial setback.

Money lost can be earned again—but without customers, your business may never recover.

If you have any questions or need cybersecurity assistance, please contact

Balancelogic Network & Cybersecurity Team
Sales@balancelogic.com
301-396-8455
Balancelogic.com

About Balancelogic For almost two decades Balancelogic has provided the answer to our client's challenges in all facets of their business. We are a leading provider of critical business support services with several departments including; Managed IT & Cyber Security Services, Marketing Services, Web Design Services, Graphic Design services, and voice solutions. Our competitive advantage lies not only on what services we provide, but also in how these services are provided. Our cross trained, experienced, and technically certified team, our well thought out and proven processes and the integration of the right technology allow us to offer an unparalleled experience to our clients.

balancelogic
THE ANSWER FOR SMALL BUSINESS.