A Comprehensive

Cybersecurity
Guide for Small & Medium Businesses

FROM THE MANAGED SECURITY EXPERTS AT TPX

Executive Summary

Cybersecurity isn't one thing but a series of actions to protect your business' computing and communications infrastructure and applications from digital attacks by cybercriminals located anywhere in the world. It's a never-ending battle against bad actors who intend to steal valuable data, disrupt operations and often hold your systems hostage for a profit.

It's not just large enterprises that are under assault – companies of all sizes are at risk. Small and medium businesses (SMBs) are particularly vulnerable because cybercriminals view them as easy targets with limited defenses.

In this Comprehensive Guide to Cybersecurity for SMBs, we'll cover what your business can do to minimize security risks.

Key Takeaways

Cybersecurity Is Essential for Businesses of All Sizes
If you think your company is too small to be targeted, think again. Nearly half (43 percent) of all cyberattacks are against smaller organizations.

Cybersecurity Is Not Just Technology
Successful cybersecurity protection is a three-pronged approach that leverages people, processes and technology.

Cybersecurity Is an Investment, Not a Cost
Effective cybersecurity is an investment in your business because it supports continuous operations and boosts customer trust.

Cybersecurity Is Affordable for SMBs
Managed security (a.k.a. security-as-a-service) enables SMBs to source cybersecurity delivered by experts as an affordable monthly subscription.

Cybersecurity Services Aren't Created Equally
Choose a managed security service provider (MSSP) with both breadth and depth in security expertise and technologies to deliver the service levels you require.

Table of Contents

PART 1:

What is Cybersecurity?

Cybersecurity is the process by which individuals and companies protect their digital assets from unauthorized access, use, disclosure, destruction, modification or disruption.

Digital assets may include:

Data
Personal identity, financial documents, trade secrets, etc.

Communications
Emails, VoIP calls, social media, websites, etc.

Applications
Productivity and line of business software, etc.

Infrastructure
Servers, computers, tablets, phones, networks, etc.

It's a Business Challenge

In today's digital world, cybersecurity helps to mitigate potential security risks, including:

- Ransomware
- Identity theft
- Corporate espionage

- Malware
- Network intrusions
- Misuse of data

- System failure
- Data corruption
- Lost or stolen equipment

Protecting your digital assets has become a necessity. For your business, cybersecurity is critical to:

- Avoid downtime
- Protect company, customer and employee data

- Keep customers' trust
- Maintain regulatory compliance

- Uphold your company's reputation

It's Not Only About Technology

There's no single cure-all solution to the ongoing threats against your company's network. There are many ways hackers can hurt your business and many ways to fight back.

Successful cybersecurity protection is a three-pronged approach that takes into consideration your people, processes and technologies. Let's look at all three:

People

Your workforce will always be your weakest link, but also can be your most potent weapon. Ongoing training with an emphasis on ways of staying safe within the network can dramatically reduce your risk.

Processes

Defining and enforcing security practices are the basis for good cyber hygiene. But it also includes a strong incident response plan, which is well-rehearsed and documented to minimize damage and downtime.

Technology

Cybersecurity tools are evolving alongside cybersecurity threats and becoming more predictive. Keeping current is critical to staying safe.

It's an Investment, Not a Cost

Whether it's training your team, establishing policies and procedures, or implementing technology, cybersecurity requires an investment in time, talent and technology. For cost-conscious small and medium businesses (SMBs), the cost may be perceived as burdensome, but it's small compared to what not having them will cost in the event of a breach.

Depending on how you define an SMB, statistics on breach costs vary greatly – from $200,000 to $4 million and everywhere in between. But the takeaway is the same – the cost of a data breach can be devastating.

It may help to think of cybersecurity like an insurance policy, which only seems like an unnecessary expenditure until you need it. And research shows that when it comes to cybersecurity, you're likely to need it. The probability that your business will experience a breach is 29.6 percent, according to Ponemon Institute, which says this figure has been trending up over the 14-year span of its research (see chart below).

Breach Probability Test
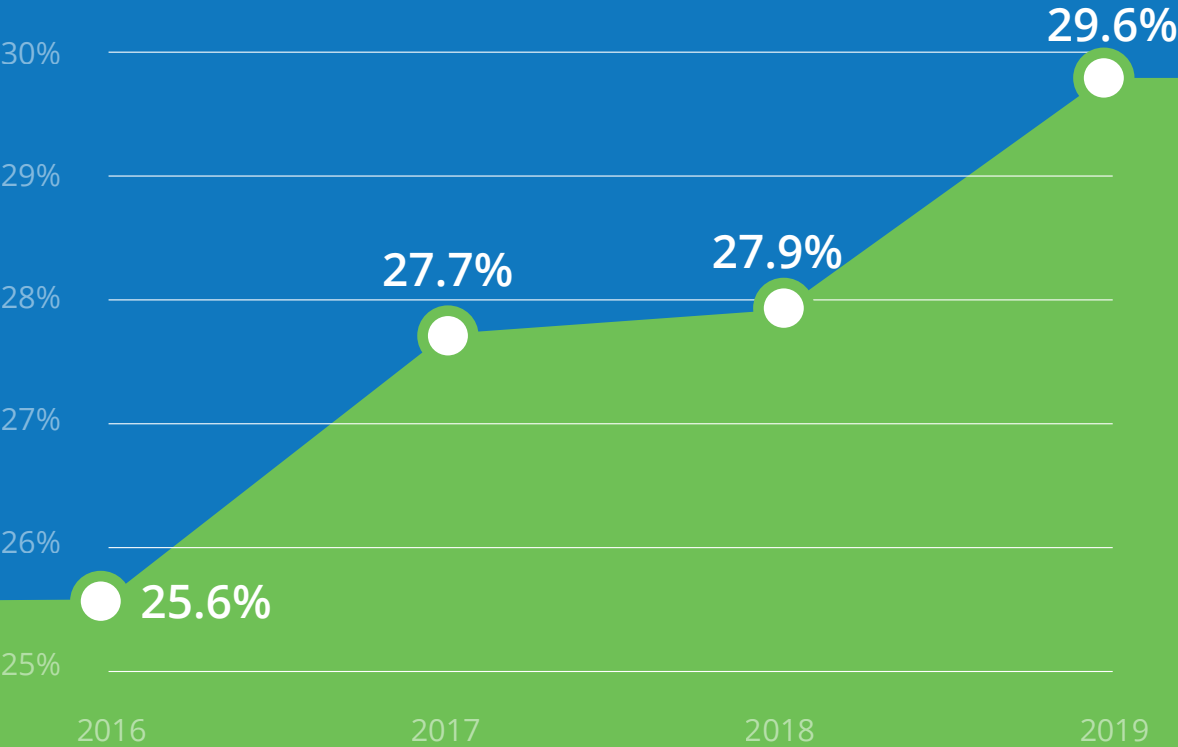
The good news is that effective cybersecurity also is available as a managed service (a.k.a. security as a service), which enables SMBs to source cybersecurity delivered by experts as an affordable monthly subscription. Managed security services mean you don't have to invest upfront in security talent and technologies to get the protection you need. Plus, managed services subscriptions are often offset by not taking your IT personnel away from other critical operational or revenue-generating functions.

PART 2:

Why Do SMBs Need Cybersecurity?

Your company is at risk, regardless of its size or industry. SMBs are especially vulnerable because cybercriminals view them as easy targets with low or no defenses in place. And they're often right.

Even organizations with their guard up can fall victim to an attack. The network of one organization recently was infected with malware and threatened to pay a ransom or else. The perpetrators warned that if cryptocurrency payment wasn't made, they would release names of anonymous informants and documents regarding criminal investigations.

You read that right—**anonymous informants and other non-public information from criminal investigations**. This 2021 ransomware victim was the Metropolitan Police Department of Washington D.C., which shows that no entity with a computer network (or computers at employee homes) storing or accessing trade secrets, customer accounts, personal identifying information (PII), financial documents or proprietary (and valuable) information is safe from cybercrime.

SMBs — perhaps your company — typically lack cybersecurity for a range of reasons like these:

- **"We're too small to be targeted."**
- **"It's on our to-do list."**
- **"We don't have IT staff."**
- **"We can't afford it."**

If any of these assertions sound familiar, you're not alone. However, most are rooted in misconceptions about the real risks and costs involved.

We know what you're thinking …

We make sure our employees don't share passwords, so we should be fine, right? After all, we've never had a problem in the past. And why would we? Our operation is too small to attract the attention of cybercriminals.

It's organizations like Twitter, Uber, Capital One, Equifax, JPMorgan Chase, Marriott International and Colonial Pipeline that make headlines for data breaches. These are all huge enterprises, especially compared to our company. Why would anyone pick us?

In 2019, three in four SMBs in the U.S. had reported a digital attack in the preceding year, according to Ponemon Institute. You just don't hear about them because attacks on smaller businesses don't make news like those involving global brands.

At TPx, many of our cybersecurity clients are SMBs. Sadly, most don't turn to us for help until they've already been attacked. One of these victims-turned-clients lost $200,000 to ransomware just weeks after leadership asserted that the company was "too small to be at risk."

Besides, there were too many other things going on. The business was growing, hiring people, launching products, etc. Who had time to shore up the company's cybersecurity risk profile?

Looking back, the executives wish they had taken the time.

Not only is financial loss a consideration for shoring up defenses, but your company's reputation is also at stake, even for smaller organizations that don't get attention from headlines. When you get hacked, you will be legally required to inform every affected customer that their data may have been stolen. According to the Federal Trade Commission (FTC), all states have enacted legislation requiring notification of security breaches involving personal information. Depending on the type of information accessed and where your business operates, there may be other laws or regulations you're required to follow.

The risk of a breach is very real, and the cost is very high – significantly higher than threat prevention, detection and remediation solutions that are affordably available to SMBs today. We'll discuss more about these later, but first, let's drill down into the evolving threats to your cybersecurity.

PART 3:

What Are Common Cyber Threats to SMBs?

So, what is your business up against when it comes to cyber threats? There are many approaches hackers can take to intercept your data or disrupt your operations. Familiarize yourself with the following common attack tools or methods, so you recognize them if/when you see them in action against your company.

Ransomware

Ransomware is a type of malware in which the data on a target device is locked via encryption and a ransom payment is demanded before the data is decrypted and access is returned to the victim. Ransomware remains the most common cyber threat to SMBs, with 60 percent of MSPs reporting that their SMB clients have been hit as of third quarter 2020, Datto reveals.

Phishing

Phishing is a data breach through social engineering. It's the bad guys fooling your employees into admitting them into your network or otherwise helping them commit cybercrimes against your business. Typically, the hacker disguises its email, phone, or other means of communication to appear as if it's coming from a legitimate source. Your staff is tricked into divulging important information such as passwords or other sensitive data. Phishing might result in identity theft or financial theft through fake invoices or payroll diversion fraud, among other crimes.

Data Collection & Exfiltration

The objective of this form of attack is to capture information that might be used by the hacker or resold to others working on the dark web. Information is obtained through hacking digital resources that are have your information on them, including accounts on e-commerce websites, online portals for insurance accounts and customer databases at commercial retail stores and restaurants to name a few. Data might include passwords, social security numbers, credit card access information, banking accounts, or other sensitive records from customers or employees. The initial attack can erode customer trust or create bad morale, but the situation can worsen if buyers on the dark web use the data to inflict further damage.

Malware

Malware, short for malicious software, is any program or file that is harmful to a device and its user. Here are a few examples:

Viruses

This method of attack has been around almost as long as the digital age. The first virus was planted on an Apple II computer in 1982. Viruses are a form of malware that self-replicates once it's in a computer or network. When activated, the bad code steals sensitive data, launches denial-of-service (DoS) attacks, or, at the very least, causes severe system slowdown.

Worms

These bad actors are another form of malware. While a virus gets into your system by the accidental actions of individuals, such as by opening a suspicious email attachment, worms are created to take advantage of vulnerabilities written into the code of legitimate software. A hacker discovers the security flaw and uses it to launch malware that "worms" its way into a computer or network.

Trojan Horses

A trojan horse is a program that appears harmless but is malicious in intent. The damage is done when the software is downloaded and introduced into your company's network.

Password Breaches

Network users aren't always careful about selecting passwords that can't be broken easily. If forced to select a more complex password, they might write it down and leave it where it can be easily accessed. Once a password has been compromised, significant system damage can occur. That's why many companies today use password managers – a technology that encrypts a user's master password in a way that makes it difficult to hack or otherwise compromise.

Insider Threats

Insider threats are risks caused by the actions of employees, former employees or third-party contractors. Through either malicious intent or ignorance, these users can wreak havoc on your business by exposing your data publicly, subjecting you to ransomware attacks, deleting and destroying critical files and systems and more. Six out of 10 data breaches in 2020 came from insiders.

Endpoint-delivered Attacks

These are attacks on any endpoint, which includes on-premises workstations, on-premises servers, virtual servers and mobile devices (laptop, tablet, smartphone, etc.).

Man-in-the-middle (MitM) Attacks

Also known as eavesdropping attacks, MitM attacks occur when bad actors insert themselves in between two-party transactions to interrupt traffic and steal data. These are commonly found on unsecured public Wi-Fi networks and are why most cybersecurity providers recommend installing virtual private networks (VPNs) on mobile devices.

Denial-of-Service (DoS) Attacks

DoS attacks oversaturate your systems, servers and networks with traffic to drain resources and bandwidth so systems can't fulfill legitimate requests from your staff.

Structured Query Language (SQL) Injections

Structured Query Language (SQL) injections happen when malicious code is inserted into a server that uses SQL. The code then forces the server to display information it would normally keep hidden. These types of attacks could be carried out by submitting the malicious code into a website's search box.

Zero-day Exploits

Zero-day exploits occur after a network vulnerability is announced but before a patch or solution is implemented. Attackers go after the vulnerability during the window of time that the network is unprotected.

DNS Tunneling

Domain Name System (DNS) tunneling uses DNS protocol to communicate non-DNS traffic over port 53. HTPP and protocol traffic will be routed over the DNS. This can be used to disguise outbound traffic as DNS, concealing data that would alert the network that an external user is connected and exfiltrating data.

Where Should SMB Cybersecurity Strategies Start?

There's no silver bullet to ensure your business will never be impacted by a security event, but there are strategies and solutions for mitigating your risk. Let's start with a five-step guide to best practices and then take a look at layering in solutions for basic and advanced cybersecurity in Parts 5 and 6, respectively.

1 Start with a security assessment.

- **Identify your critical assets.** Which data and systems need to be protected? Make sure you think through strategic information, sensitive client information (e.g., intellectual property, financial data, bank and credit card information, etc.) and sensitive information for your own company (e.g., employee personal identifying information, financial data and health information).

- **Run an external vulnerability scan.** Once you've identified the data and systems you need to protect, it's time to find your weak spots.

- **Identify and close ports and protocols that shouldn't be open.**

- **Audit web browsing and application control protocols.**

- **Review password and security policies.**

2 Develop a Bring Your Own Device (BYOD) policy.

- **Define the minimum required security** controls/software needed for safe operation.

- **Establish controls for application access and installations.**

- **Require endpoint management** agents to be installed on personal devices.

- **Develop, refine or verify your policies** for employees that leave the company and how to remove data from personal devices. Think through file storage, email, collaboration tools, etc.

3

Educate your employees and reduce exposure credentials.

- **Change passwords as is needed** to enforce strong password policies. If your systems have weak or dated password rules, beef them up. If you manage highly sensitive information that requires periodic password changes, put those rules and systems in place.

- **Use a password manager.** Implement a password manager for all members of staff so they can maintain strong password policies without needing to remember long and complicated passwords.

- **Enable two-factor authentication on as many applications and accounts as possible.** Microsoft 365 and other business accounts have the option to enable two-factor authentication, adding a second layer of security to your user accounts by sending a code to a secondary device in the users' possession to enable login.

- **Educate employees with simulated phishing emails and security awareness training.** We can't emphasize this step enough. Approximately 88 percent of all data breaches are at least partly caused by human error. If properly trained to recognize risks, employees represent your company's first line of defense against cyberattacks.

- **Put your policies in writing.** Give your employees reference materials appropriate to their job responsibilities. In other words, explain the topics in greater detail when communicating with your IT staff than when addressing marketing or accounting personnel. This documentation should clearly explain the various threats and cover risk avoidance strategies when an intrusion is suspected. State who they should contact and display that information prominently.

- **Deliver short training modules regularly to increase retention.**
Some studies suggest that humans forget approximately 50 percent of new information within an hour of learning it! Consciously reviewing new information helps fight the "forgetting curve," so opt for ongoing training modules instead of annual brushups. For instance, ransomware attacks in the news might spur a brief video explaining how that particular threat works and what they can do to dodge the risk.

Look for and defend against insider threats.

- **Restrict privileged user access** to only personnel that absolutely need it.
- **Remove user access** from employees who've changed roles or left the company.
- **Monitor logins and directory access** for atypical user behavior or document access.
- **Monitor for rogue network devices.**
- **Enact network and file segmentation** to limit file access by job, location and/or need.

## Create an incident-response plan.

- **Define responsibilities.** Identify critical network and data resources and how to recover them. Define who's responsible for neutralizing threats, implementing business continuity measures and restoring normal operations. Be sure to include audits, breach assessments, etc., in those plans, which may involve coordination with outside specialists. (Sometimes, these specialists are covered in your cyber insurance policies.) And be sure to plan for communications while you're at it (see below).

- **Develop a business continuity plan.** How will operations continue in the event of an attack? Ideally, you can tackle business continuity needs for outages caused by weather, construction and other events (like a pandemic) at the same time.

- **Establish internal and external communication plans.** Determine who will inform and update executives and internal stakeholders during a cyberattack. Plan for external communications during and after an attack just in case customers or suppliers cannot access your systems. Find out what disclosure rules you may need to adhere to if sensitive or personally identifying information data is breached.

PART 5:

What are Baseline Cybersecurity Solutions for SMBs?

There is a range of cybersecurity solutions, so which ones should you choose? As noted previously, effective cybersecurity doesn't come in one box but from layers of solutions that seek to stop attacks along their path.

The following solutions are recommended to support a basic level of cybersecurity. Some of these work at the firewall level and others at endpoints, which are individual devices connected to your network, including desktop computers, laptops and smartphones.
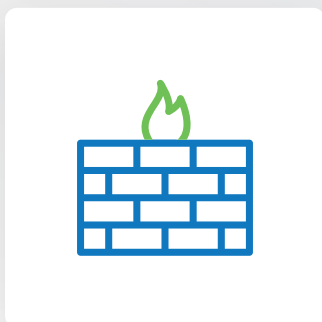
Next-generation Firewalls

A firewall creates a barrier around your network and monitors traffic in and out of that network based on security rules. A firewall alone can't protect your network, but it's one very good weapon. That's especially true if your system is protected by next-generation firewall (NGFW) technology, which does everything a traditional firewall does but boosts protection through heuristics (analysis using rules, estimates and educated guesses for prediction) or artificial intelligence (AI). Next-generation protection also delivers unified threat management (UTM), which includes:

- Antivirus software

- Intrusion Detection System and Intrusion Prevention System (IDS/IPS)

- Deep Packet Inspection (DPI) of Secure Sockets Layer (SSL) traffic

- Safelisting/blocklisting software

Backup & Data Recovery

We know a European company that did an excellent job protecting its network at both the firewall level and at its endpoints. Hackers tried to get in and failed. That was until they found a vulnerability in the company's backup system, which wasn't encrypted. From there, the hackers managed to pull down a backup of the server. That attack was like having full and uninterrupted access to the company's network.

Many businesses face this vulnerability. They know the importance of regularly backing up their data but fail to encrypt it. It's so common that it's built into some hackers' processes to leave successfully installed malware dormant for long periods, so the data backups also are infected when the target company is targeted with a ransomware attack. As a result, there's no backup rescue and the targeted company might be forced to capitulate to the ransom demands – even though they were backing up their data.

Even "clean" backup files might take several days before the recovery process can be completed, which can be devastating to your business. Instead, look for backup and disaster recovery (BDR) services that can launch a virtual copy of your files in minutes as a temporary solution that keeps your business running while your server is rebuilt.

Password Management

Long gone is the day when "password" can be your team's preferred password. Hackers buy and sell lists of the most common passwords and patiently try them on their intrusion targets. They have all the time in the world (especially when the program scripts to do the work for them). Today, most businesses are much more sophisticated when it comes to knowing how easy it is to guess short and obvious passwords. Now they're longer, alphanumeric, include at least one special character, and must be changed regularly.

But even that invites problems. One TPx client did a commendable job of mandating a safe password protocol. However, we recognized that their passwords were so long and complicated that we suspected proper steps weren't taken to safeguard those passwords. We toured the premises after-hours and found sticky notes with written passwords on or near computer terminals or under keyboards in at least 30 percent of workstations!

Password managers solve both issues by enabling users to know only one master password translated into a unique encrypted password for each place a password is used. Most password managers use military-grade AES-256 encryption and keep the encrypted passwords in a virtually impenetrable vault. No cybersecurity tool is perfect, but a password manager is as close as you'll get when it comes to keeping employee and customer passwords out of the wrong hands.
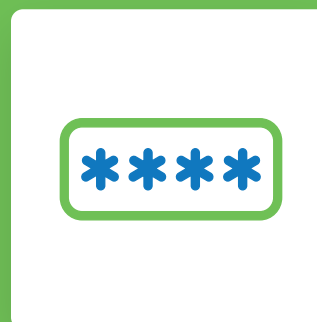
Multi-Factor Authentication

MFA is the access process by which two or more means of authentication must be provided – not just a password – to gain access. The most common method asks users to respond to security questions with previously provided answers, such as mother's maiden name, first car, favorite pet, etc. This approach isn't foolproof since many of those answers might be found within the user's social media content.

More recent and more trustworthy secondary verification methods include codes sent to external devices, such as users' cellphones or wearable devices like Bluetooth-enabled bracelets. The idea here is that, while a data thief might have stolen a password, the hacker probably isn't also in possession of secondary codes or users' phones or other devices receiving it (though code hacking has occurred). MFA methods also are being developed to use biometric verification, such as users' fingerprints or eye scans.
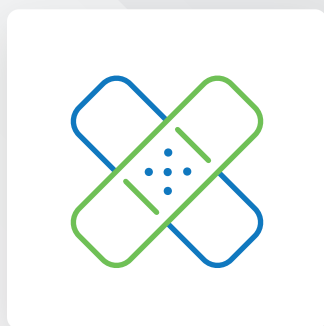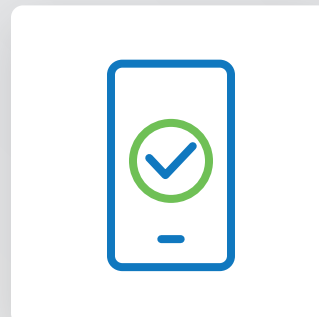
Patch Management

We all know that our Internet programs and files are under constant attack. As soon as software providers discover vulnerabilities, they issue a patch as a fix. Patches might also be released to update or improve systems. Your IT department understands the importance of applying these patches, but there are only so many hours in the day. Automated patch management is critical as an attack prevention strategy and should be part of your baseline solution.

PART 6:

What Are Advanced Cybersecurity Solutions for SMBs?

For many companies, baseline protection isn't enough—especially in the wake of the COVID-19 pandemic, which expanded network vulnerabilities to work-from-home endpoints and drove cybercrime activity through the roof. According to the FBI, cybercrime reports surged 400 percent during the pandemic, to 4,000 complaints per day. Cybercrime never stops, and neither should your protection.

Many companies, including SMBs, are deploying **endpoint detection and response (EDR)** and **managed detection and response (MDR)** solutions. To compare EDR/MDR to legacy detection solutions, imagine a couple out for the evening when they get a call from the babysitter. Junior has gotten his hands on a pair of scissors, and he's threatening the neighborhood kids. The babysitter's call is like the legacy system; its job is to alert. You've been warned. Finish dinner and get home quickly.

EDR/MDR protection, on the other hand, is like the babysitter calling to alert you to the problem but then adding that she's taken the scissors away from Junior and locked up all sharp objects. The sitter recommends a parental talk with Junior and offers a few more tips to achieve a safer household before telling you that the danger has passed and you can enjoy your night out.

That's your EDR/MDR solution. The technology monitors traffic, detects problems and remediates the issue through both a tool and a human-managed security operations center (SOC) at firewall and endpoint locations.

EDR Benefits

- Protection for endpoint devices 24/7/365
- Next-gen antivirus
- Improved system reliability and performance
- Reduced downtime
- Increased employee productivity

MDR Benefits

MDR has all the benefits of EDR, plus:

- Advanced threat hunting
- Proactive threat mitigation
- Identifies more threats (antivirus alone misses 60 percent of attacks)
- Reduced dwell time
- Fully managed
- 24/7/365 monitoring that never sleeps (just like the bad guys)

DNS Protection

In addition, you can add Domain Name System (DNS) Protection, which provides an additional layer of protection between employees and the Internet by blocklisting dangerous sites and filtering out unwanted content. A secure DNS solution can be deployed to protect both in-office and at-home networks and typically provides:

- Content filtering
- Malware and phishing blocking
- Botnet protection
- Advertisement blocking
- Typo correction to prevent entry to malicious domains
- Improved lookup speeds

Should SMBs Manage Cybersecurity In-house or Outsource?

Some SMBs manage their cybersecurity needs in-house. In these cases, they usually are among the few with cybersecurity expertise internally, have underutilized IT personnel they can train up, or don't realize that outsourced solutions are not just affordable but usually more comprehensive.

For most SMBs, managing cybersecurity in-house is a non-starter from the get-go. Obstacles include:

Lack of talent. The IT skills gap is a well-known challenge for businesses of all sizes, but especially SMBs that often lack the resources to compete for scarce talent who can command top dollar. The gap is even more pronounced in the hyper-specialized and high-value subset of cybersecurity.

Lack of bandwidth. In today's interconnected world of integrated apps, devices and other technologies, IT departments are stretched wafer-thin. Many simply don't have the bandwidth to tackle cybersecurity effectively.

Lack of awareness. As we discussed earlier, many SMB owners and managers fail to understand the risks they face, finding out all too often that they are prime cybercrime targets for this very reason.

Outsourcing solves all of these problems and delivers other benefits, which include:

Instant access to expertise. Outsourcing to a managed service provider (MSP) delivers instant access to teams of trained personnel that are experts in protecting your business from cybercrime.

Reduces overhead. You won't need to hire, retain or train cybersecurity specialists in-house since the MSP takes care of that expense for you.

Affordable, predictable and scalable plans. Outsourcing your cybersecurity can be significantly less expensive than developing and deploying cybersecurity resources (i.e., technology and talent) internally. Moreover, MSP solutions are instantly scalable and offer predictable pricing, giving you control over your IT spending.

Focus on your own business. Cybersecurity is a complex undertaking and an entire business unto itself. By outsourcing it, you can focus on managing and growing your core business.

PART 8:

What Should SMBs Look for in a Managed Security Service Provider?

As noted in Part 7, managed security services are an attractive option for SMBs, solving many challenges of securing an organization effectively and affordably. That said, not every MSP is created equally. Ensure that you're selecting the right MSP for your SMB by considering the following questions:

What is the breadth of the MSP's service?

Many MSPs offer managed firewall services, but stop short of delivering complete protection, which extends to endpoints, for example. Instead, look for an MSP that covers the entire lifecycle of an attack from user training and firewall to endpoint and backup and recovery.

What service level is being provided by the MSP?

MSPs often provide hardware or software solutions with automated alerts but no live monitoring or remediation. Make sure you're clear on the service level that you're getting from your MSP. Note: The difference in the delivery model also may explain wide swings in price quotes from one MSP to another.

How deep is the MSP's bench?

Similarly, if your MSP does have security talent, are they in sufficient number to handle vacations, illness, resignations, emergencies, other projects, etc., and still maintain the service levels you're promised and expect.

Is the MSP there when you need them?

Hackers don't work bankers' hours; they do their misdeeds from all time zones and all hours of the day and night. That means your business network is at risk of data breach 24/7. Seek assurance from your MSP that you'll be in immediate touch with a team of certified engineers – not just an answering service or non-certified support – whenever you need assistance.

Are the MSP's engineers certified in the technologies they deploy?

While all MSPs can sell and deploy hardware and software solutions, not all of them are certified by the manufacturers to do so. Certification is often arduous and expensive but ensures that the MSP's engineers set up the solutions correctly to protect your environment.

Where do the MSP's engineers go for tech support?

MSP engineers sometimes need help, so where do they turn? Certified MSPs get preferred status and go to the head of the line for support, which is critical to assuring you get both fast and expert assistance.

PART 9:

Why Should SMBs Consider TPx for Managed Security Services?

You have enough challenges in your business life. You don't also need to worry about data breaches and the potentially catastrophic impact on customer relations, business operations, workflow and your bottom line.

At TPx, we have the products, services, experience and certifications to keep your network safe and running smoothly.

Why Choose TPx?

We solve the biggest IT issues – cybersecurity, connectivity and collaboration – under one umbrella.
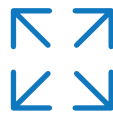
We have the IT solutions, staff and experience you need for effective results within your budget.

We have 120+ certifications across 60+ competencies, like CompTIA, Cisco, Fortinet, AWS, SMC and more.

We modernize your IT, connectivity and communications while minimizing your risk from cyberthreats.

With 23,000 clients in 50,000+ locations, we're big enough to get the job done and small enough to be agile.

We mix and match solutions and deliver a variety of service levels customized to meet your needs.

TPx is Your One-stop Shop for Managed Security Services

Managed Detection and Response (MDR)

Discover, prevent and recover from cyber threats faster. TPx's MDR helps you identify more threats, reduce attack dwell time, and proactively mitigate attacks. We offer managed detection and response for both firewalls and endpoints.

Next-generation Firewall

The firewall is the first line of defense in protecting your business from Internet-based threats. Next-generation firewalls block today's advanced threats while also providing secure access, visibility and control to help your business be more productive.

Endpoint Management and Security

TPx helps keep your servers and workstations healthy, secure and performing optimally. Our Endpoint Security service leverages remote monitoring and management (RMM), patch management and security. Together with expert support personnel and security analysts, we provide an "always-on," best-in-class, 24/7/365 service.

Backup and Disaster Recovery (BDR)

We help organizations quickly recover from system downtime and data loss caused by cyberattacks, human error, system failures and natural disasters. Using advanced hybrid local/cloud technology and skills management resources, TPx delivers a turnkey BDR solution that will meet your recovery objectives.

Unified Threat Management (UTM)

TPx ensures UTM features such as web filtering, antivirus, application control, intrusion prevention and VPNs are properly configured, monitored and maintained.

Email Security

Protecting your email communications is an important part of any security strategy. Whether it's protecting against email-based cyberattacks like phishing or ensuring that sensitive information doesn't fall into the wrong hands, we can help you navigate the email security challenge.

DNS Protection

We protect systems and users from malicious websites using leading DNS Protection software. Windows devices are protected both on the corporate network and while traveling. Network-based DNS protection covers BYOD, Guest Wireless, and Non-Windows devices to deliver comprehensive DNS security and reduce your risk of attack.

Security Awareness Training

Users are your last line of defense. The more they know, the less prone they are to be victims of phishing scams or other security incidents. Our service includes monthly phishing simulations and Security Awareness Training courses with automated reporting to track your results.