The MSP’s Guide to a Multi-Layered Security Approach

8 Steps to Ensure Your Security Practice Covers the Full Lifecycle of Cybersecurity Management
About This Guide
This guide discusses the vital importance of helping SMB clients secure their business and how to implement a layered security approach with comprehensive coverage of the cybersecurity lifecycle.

Under Siege
Why SMB Clients Must Secure Their Business .............................................. 2
Attacked From All Sides .............................................................................. 4

Fortifying SMBs’ Defenses
The Need For A Multi-layered, Proactive Defense ....................................... 6
Using Industry Standards As A Guide ......................................................... 7

8 Steps to Build a Complete Security Practice
1. Implement Identity Protection Policies & Solutions ................................... 8
2. Put Endpoint Security In Place ................................................................. 10
3. Layer On Additional Email Security ........................................................ 11
4. Enforce Data Protection & Compliance ................................................... 12
5. Implement Web & Network Security Together .......................................... 14
7. Add Mobile Security ............................................................................. 16
8. Create A Disaster Recovery, Backup & Incident Response Plan ............. 17

Your Security Experts
Putting It All Together ............................................................................. 18
UNDER SIEGE

Why SMB Clients Must Secure Their Business

The threat is real. As the startling statistics below show, businesses are under siege. Cyberattacks are possible anytime and with potential for immense damage. Small and medium-sized businesses (SMBs) are especially vulnerable due to their lack of awareness, knowledge, and resources, which can leave them feeling overwhelmed and alone against a looming threat landscape.

More Cybercrime Against SMBs

43% of cyberattacks target small businesses¹

2/3 of SMBs suffered a cyberattack in 2018²

6 out of 10 SMBs report attacks are becoming more targeted, harmful, and sophisticated²

Increasing Costs

$3 million is the average cost of a cyberattack to SMBs (with over half of that cost due to downtime)³

8 or more hours of downtime were experienced by 40% of SMBs due to a breach³

Growing Unpreparedness

Half of SMBs say they don’t know how to protect against cyberattacks²

89% of MSPs think their clients should be “highly concerned” about ransomware, but only 36% of SMBs feel the same⁴

wingman@pax8.com | +1 (855) 884-7298 | pax8.com
MSPs Need to Secure Themselves First and Foremost!

MSPs are one of the biggest threats to their downstream clients’ security.

By leveraging a remote monitoring and management (RMM) tool, an MSP has direct reach into each of their clients’ endpoints. This is the exact access a cybercriminal wants – instead of needing to break into each business individually, an attacker can target an MSP’s RMM tool to gain access to the system and push ransomware to all the MSP’s clients at once.

MSPs need to protect themselves before they can protect their clients – so always follow all the same best practices that you recommend to clients!
Cybercriminals are growing more sophisticated, making them harder to defend against.

Social engineering techniques manipulate and exploit human behavior to bait users into giving up valuable information. This is especially effective if a person’s password is compromised and the attacker can take advantage of the trust the victim’s contact list.

Phishing attempts are getting much harder to recognize – gone are rampant grammar errors, awkward phrasing, and suspicious formatting. Phishing emails and websites have become more successful at mimicking real people and legitimate brands to convince end users to give up sensitive information.

Business email compromise (BEC) attempts can trick even savvy users who see an urgent, personalized message seemingly from their boss and rush to respond.

Spoofing techniques have been greatly enhanced, using professional graphics to mimic trusted brands and trick users into downloading malware.

Zero-day attacks and fileless executable malware that can slip past attachment scanning tools are becoming more prevalent.
SMB

Trojan Horses
Imposter malware or code disguised to appear legitimate to gain backdoor system access

Spyware
Malicious software that infiltrates devices to gather information

Eavesdropping Attacks
Attempts to steal data transmitted by devices across an unsecured network

Phishing
Attempts to trick users into sharing sensitive info by posing as a trusted entity

Password Attacks
Hacking attacks (which can use scripts, algorithms, password sniffers, or keystroke loggers) that seek to obtain a system password for illegal access

DDoS Attacks
Distributed denial of service (DDoS) attacks that overwhelm the resources of a network

Malware, Worms, and Viruses
Malicious software meant to damage or steal data from a device or network

Ransomware
Malware that locks users out of a device, system, or data until a fee is paid

UNDER SIEGE
Attacked From All Sides
To defend against an increased rate and range of attacks, businesses need to take a multi-layered defensive approach that overlaps safeguards, limited access points, end user training, and perimeter defenses. Essentially, modern companies need to become digital fortresses, with multiple layers of proactive protection that serve to monitor, detect, alert, and prevent the onslaught of cyberattacks.
FORTIFYING SMBs’ DEFENSES

Using Industry Standards as a Guide

The Cybersecurity Framework developed by the National Institute of Standards and Technology (NIST) guides organizations towards better understanding, managing, and reducing cyber-risks by providing a holistic set of industry-accepted best practices, guidelines, and standards. Although voluntary, it has been widely adopted as a gold standard across organizations of all sizes and industries and continues to be updated and refined through expert input and public feedback.

Aligning your MSP security practice to the five Functions of the widely adopted NIST Framework helps ensure that your services and solutions have comprehensive, layered coverage across the full lifecycle of cyber-risk management:

- **Identify**: Gain a complete view of the risk to an organizations’ inventory of systems, assets, data, processes, and policies – prioritizing critical areas that need protection and governance.
- **Protect**: Develop and implement safeguards that will limit or contain the impact of a cybersecurity threat.
- **Detect**: Implement tools and processes to enable the timely discovery of cybersecurity events.
- **Respond**: Take rapid action to contain the impact of a detected cybersecurity event.
- **Recover**: Restore capabilities that were impaired by a cybersecurity event quickly enough to mitigate impact.

**How to Put the NIST Framework Into Action**

Use assessments to rank your organization for each of the subcategories to build your current NIST profile, then set a target profile for each subcategory. Incrementally implement solutions and processes and continually reassess your progress towards the target.
Passwords are the key to accessing business data, but passwords alone are becoming an increasingly simple lock for hackers to pick. In addition to implementing strong password policies, passwords should be reinforced with extra layers of security such as multi-factor authentication (MFA). However, it’s also important to balance security with productivity — otherwise, users can experience “password fatigue” due to the effort of maintaining unique passwords for every account or become frustrated by completing MFA every time they want to sign in.

Enforce Strong Password Policies
While passwords shouldn’t be the only line of defense to data, make them as strong as possible by enforcing password policy best practices throughout an organization:

• Require long password strings with a mix of letters, numbers, symbols, and capitalization
• Set time limits for passwords to expire and don’t allow recent passwords to be reused

Enable MFA
MFA is the best defense to reinforce passwords and strengthen access security. MFA safeguards access to apps and data by requiring a second form of authentication in addition to a password, such as time-based codes sent via text, email, or app, fingerprints, or answers to personal security questions.
Combine Single Sign-on (SSO) with MFA Where Possible

Signing into an app can slow users down by 10-30 seconds, which adds up with each app used. To help users remain productive while maintaining security, enable SSO whenever possible (example, for all Microsoft apps) to reduce the number of credentials that users have to manage and the number of sign-ins they have to complete each day. SSO also helps reduce desk tickets related to password resets.

30-50% of help desk requests are related to password reset or access issues. 7

Apply Conditional Access (CA) Rules

To further balance security and usability, set rules to limit MFA when users are in the office, but continue to enforce MFA on untrusted networks such as at home, airports, or coffee shops. This reduces user frustration at being slowed down by the extra steps of MFA when they’re at work.

1/4 of Wi-Fi hotspots in the world do not use any encryption at all. 8

Supplement SSO Gaps with a Password Management Tool

Not every app can be combined with SSO, so to further reduce the number of passwords that users have to maintain (and therefore reduce the likelihood of password reuse across apps), you should offer a password management tool that generates strong passwords, then encrypts and stores user credentials.

85 is the average number of passwords that small business employees must remember. 9
8 STEPS TO BUILD A COMPREHENSIVE SECURITY PRACTICE

2. Put Endpoint Security in Place

70% of breaches originate at the endpoint, but 42% of all endpoints are unprotected at any given time!  

The rise of wireless devices has drastically increased the number of endpoints in an organization. In addition to servers and desktops, each employee laptop, tablet, and smartphone adds another possible vulnerability that can be exploited to give incoming malware access to the corporate network. Simply installing antivirus software is no longer enough due to the proliferation of attack vectors including email attachments and hyperlinks, web browsing, social media, and apps.

While traditional antivirus solutions simply try to prevent attacks, modern Endpoint Detection and Response (EDR) solutions actively discover and remediate threats across devices, desktops, and servers. Advanced endpoint protection solutions use automation, machine learning, and behavioral monitoring to detect, respond to, and eliminate a diverse range of threat vectors, including executable or fileless malware, document and browser exploits, malicious scripts, and credential scraping. Features to look for include:

- Visibility into endpoints, apps, running processes, and encrypted traffic
- Threat forensics
- Ability to isolate and disconnect infected endpoints from the network
- File recovery and device rollback

64% of SMBs experienced one or more endpoint attacks that successfully compromised data in 2018  

55% of SMBs rank mobile devices as the most vulnerable endpoints into their network  

20% of SMBs don't have or don't know if they have endpoint security  

$763 was the average cost per compromised endpoint for SMBs in 2018
Email is the top delivery mechanism for 96% of phishing attacks and 49% of malware attacks.¹⁴

With email as the #1 vulnerability for phishing, ransomware, spam, and malware, it is critical to protect sensitive data from leaving the organization and stop threats before they can enter your network through email. The native security features of most email solutions, including Office 365, don’t offer enough built-in protection to combat today’s threats — you should layer on a third-party solution that can provide advanced security features, such as:
31% of SMBs say they do not comply with any security guidelines or standards. 12

Protecting a company’s most sensitive and proprietary information with an extra layer of protection through data loss prevention and email/file encryption helps prevent data breaches and the potential costs of litigation, penalties, fines, and settlements. This is especially essential for organizations that must comply with regulations, such as the Health Insurance Portability and Accountability Act (HIPAA), Criminal Justice Information Services (CJIS), and Payment Card Industry (PCI) standards.

Millions of healthcare records are wrongly exposed or breached each year due to failed HIPAA compliance. However, despite the massive importance of securing patient data (and the potential impact of settlements and fines due to violations), HIPAA compliance can feel overwhelmingly complex to organizations starting their compliance journey, which is where compliance software can help.

The odds of experiencing a data breach increased from a 22.6% chance in 2014 to a 29.6% chance in 2019. 21

Malicious attacks are the most common and most expensive root cause of data breaches 21

Small businesses face disproportionately larger data breach costs relative to larger organizations 21
8 STEPS TO BUILD A COMPREHENSIVE SECURITY PRACTICE

4. Enforce Data Protection and Compliance

Data Loss Prevention (DLP)
Protect confidential and critical information from being accidentally shared, lost, leaked, or stolen through rule-based monitoring and alerts (e.g., “no number formats that indicate Social Security Numbers are allowed to be sent in outbound emails”).

Email Encryption
Encrypt inbound and outbound emails based on policies to ensure that sensitive information can be safely shared inside and outside the organization.

Whole Disk Encryption
Implement whole disk encryption on every laptop to protect business data in the event of device loss or theft.

App Blacklisting and Web Security
To ensure that business data can’t be sent via unmonitored and unprotected channels, you can disallow users from using their personal email or apps such as Dropbox on work devices.

USB Device Control
In highly secure environments, lock down user USB ports to prevent employees from walking out with sensitive, proprietary, or confidential data on a thumb drive.

HIPAA Compliance Software
HIPAA compliance solutions provide structured guidance to help organizations achieve and maintain compliance with assessments, training, incident management, business associate management, and breach support staff.
8 STEPS TO BUILD A COMPREHENSIVE SECURITY PRACTICE

5. Implement Network and Web Security Together

47% of SMBs experienced web-based attacks in 2018.  

It is critical for businesses to fortify connections to protect and control access to their environment's entrance and exit. Network and web security go hand-in-hand to secure incoming and outgoing network traffic. Network security helps protect network systems and data from unauthorized or malicious access, while web security protects users from accessing malicious websites.

### Network Security

1. Install a reputable next generation firewall that can provide intrusion prevention and detection, URL filtering, and data loss protection.

2. To narrow the attack surface and provide cybercriminals with fewer vulnerabilities to exploit, disable unnecessary ports. For example, Remote Desktop Protocol (RDP) provides admins with powerful capabilities but also opens up an endpoint to attacks. Restricting access or enforcing proper authentication is critical.

3. Segment a network for guests and even employees' personal devices to keep unauthorized users from accessing resources they shouldn’t, as well as creating a defined line of work and personal web surfing habits.

### Web Security

1. Whether users are simply web surfing or are tricked into clicking a malicious link in a phishing email, protect users by blocking them from visiting malicious websites.

2. Prevent users from visiting inappropriate websites, such as pornographic, gambling, or gaming sites.

3. Preserve bandwidth consumption by blocking users from streaming services, such as Netflix, that use up precious bandwidth.

54% of SMBs don’t have a guest Wi-Fi network

24% of SMBs report malicious websites and web ads as a top ransomware delivery method

[12] [13] [15]
65% of SMBs currently don’t undergo end user training, even though end users are the number one cause of data breaches.¹³

A company’s security posture is only as strong as their least secure employee. And with phishing attempts growing ever-more-sophisticated, even savvy users can find themselves accidentally clicking malicious links, opening risky attachments, or mistaking a spoofed URL for a familiar website and offering up sensitive information. Empower end users by engaging them with ongoing security training to teach them how to spot and respond to various types of threats.

**Phishing Simulation Training**
Phishing simulation tools are a great way to teach employees to be alert for, identify, and report suspected phishing attempts in their inbox.

**78%** of end users don’t click on a single phishing email after training.¹⁴

**Ongoing Microtraining**
As cybercriminals continue to innovate, continual education is important so that users stay up to date on the latest threats. Security awareness training solutions use microcontent and quizzes to build security scores and track progress company-wide.

**Security risks are reduced by**
**70%**
when businesses invest in security awareness training.¹⁷
8 STEPS TO BUILD A COMPREHENSIVE SECURITY PRACTICE

7. Add Mobile Security

98% of employees in 2021 said they would like to work remotely, at least some of the time, for the rest of their career.¹⁸

Prior to the COVID-19 pandemic, many companies were already beginning to embrace remote work and bring-your-own-device (BYOD) policies in support of mobility. The pandemic rapidly accelerated that shift and, now, the modern workforce expects the convenience and flexibility to work where they want. However, this means that the network security perimeter is no longer enough to protect company resources. Mobile devices are now one of the most targeted entry points for incoming malware through malicious wireless networks, application vulnerabilities, and lost or stolen devices.

Mobile security solutions help businesses manage and protect mobile smartphones, tablets, laptops, and IoT devices on the corporate network, adding an extra layer of security to mobile endpoints. Features commonly include:

- **Device management** provides device administration, including enrollment, configuration, policy management, BYOD privacy setting management, and remote wipe
- **Mobile application management** provides the ability to distribute apps to devices, push notifications for needed updates, and prevent users from downloading disreputable apps
- **Content management** allows users to securely access and share company documents on mobile devices via encryption and authorization
- **Network access control** enables authorized devices to securely access the corporate network and internal resources
- **Isolation** separates a user’s work apps from their personal apps, so that business data can be wiped if needed without interfering with a user’s personal information

79% of businesses say the proliferation of mobile applications has a major or significant impact on cybersecurity strategies.¹⁴

1 in 36 devices used in organizations have high risk applications installed.¹⁰

45% of business-critical applications are accessed by mobile devices.¹²

71% of SMBs have BYOD policies in place.¹⁹

wingman@pax8.com | +1 (855) 884-7298 | pax8.com
8 STEPS TO BUILD A COMPREHENSIVE SECURITY PRACTICE

8. Create a Disaster Recovery, Backup, and Incident Response Plan

Only 28% of SMBs say their ability to mitigate threats, vulnerabilities, or attacks is highly effective.²

From malicious threats and user error to physical disasters and hardware failure, there are countless ways for a business to lose valuable data or experience downtime, which can have a huge impact on productivity, lead to mounting IT costs, and damage the company brand.

Businesses of every size need to plan ahead to know how to respond in case of a data breach, outage, or cyberattack in order to safeguard data and stay operational. This is increasingly important for businesses in compliance-regulated industries, such as healthcare and finance.

An effective backup and disaster recovery plan should:

- Identify the main threats to data and operations, as well as their likelihood
- Define the company’s tolerance for downtime and data loss
- Inventory all hardware, software, apps, and data – then prioritize what is critical
- Outline a data restoration and recovery strategy, including service/solution, storage location, and processes, and prioritize what needs to go back online first
- Build processes to re-establish access to critical IT resources, apps, and data
- Establish roles and responsibilities within the action plan
- Create a communication plan for both internal and external communications in the event of downtime
- Institute an employee training and awareness program

Microsoft + Third-Party Backup

It can be eye-opening for Microsoft clients to learn that Microsoft themselves recommend third-party backup solutions.

The Service Availability section of the Microsoft Services Agreement states:

“We strive to keep the Services up and running; however, all online services suffer occasional disruptions and outages, and Microsoft is not liable for any disruption or loss you may suffer as a result. In the event of an outage, you may not be able to retrieve Your Content or Data that you’ve stored. We recommend that you regularly backup Your Content and Data that you store on the Services or store using Third-Party Apps and Services.”
YOUR SECURITY EXPERTS

Putting It All Together

The layered security approach outlined in this guide can seem complicated and daunting to an SMB with limited IT resources — especially when the stakes are so high due to the potential cost of damage from a breach. In fact, three out of four SMBs say they don’t have sufficient personnel to address IT security!

With SMBs feeling overwhelmed and under-prepared for the increasing volume and variety of cyberattacks, MSPs like you are vitally important to guide your clients towards modern, proactive defensive practices.

And you’re not alone either – Pax8 is here to help you identify gaps in your clients’ technology stacks and easily deploy the cloud security solutions they need to combat today’s advanced cyberthreats.

WANT TO DISCUSS SECURITY SOLUTIONS YOU CAN OFFER AS ADDITIONAL LAYERS OF DEFENSE?

Your Security Experts Are Here to Help.

Schedule A Call
Sources

17. Infographic: 10 statistics that show why training is the key to good data protection and cybersecurity. Pensar, 2018, https://www.pensar.co.uk/blog/cybersecurity-infographic