WHITEPAPER

The Cybersecurity Blueprint: 2020 Edition

A Four-Pillar Model for Providing Cybersecurity

The Cybersecurity Blueprint: 2020 Edition

Over the past few years, many businesses have grown increasingly concerned about cybersecurity. Decades ago, viruses were often (although not always) mere nuisances for businesses. Now, we've seen websites taken offline by distributed-denial-of-service attacks (DDoS), companies paying exorbitant fees to unlock their data from ransomware, and both small and large companies end up in the news over data breaches.

The public has become more aware of the importance of data protection, privacy, and cyberthreats. In turn, regulators have responded by strengthening regulations related to data—both by industry and by region. For example, new data privacy laws, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), set rules for businesses to follow when handling and protecting data.

If you're an IT services provider, the general public's awareness and, by extension, the response from businesses can open some new opportunities for you. However, dealing with the sheer variety of attacks these days—ransomware, malicious insider attacks, and advanced persistent threats, among others—requires you to take a broad, layered approach to security for your clients. Beyond that, managing security for workforces has grown more complicated with the increased number of remote workers.

So where do you begin? What tools do you need? And how do you even assess what each client needs to stay protected?

This eBook presents a model for providing layered security to managed services clients. This framework is designed to help you systematically approach each client's network (or even your own) and know what elements to put in place to provide strong cybersecurity. You'll also gain a good sense of where your employees need additional training and what tools and processes they need to master.

Table of Contents

The Four Pillars of Layered Security

Your first inclination might be to think of the pillars in terms of the technological tools you should use to combat threats. However, focusing solely on individual tools to deploy can distract you from the overall goal of creating a cohesive cybersecurity strategy. While we mention some technology options in each section, the four pillars represent four main areas included in a typical cybersecurity strategy. By focusing on these broader categories and what you'd like to accomplish within them, you can systemically build defenses for almost any business.

While we'll mention technology in each section, it's worth noting individual technologies can cross multiple steps. For example, you can use endpoint detection and response (EDR) tools to detect threats and assist in recovery.

1. Prepare

The first pillar involves monitoring both electronic devices and the physical security of corporate offices. It also involves good password hygiene and remote monitoring. This layer can show early warning signs of cyberthreats, helping you stop attacks before they get off the ground. In fact, some of the defenses in the other pillars would be impossible without this foundational layer.

2. Detect

This next pillar includes many of the tools and techniques thought of as traditional security mechanisms—like antivirus (AV) to detect malware, EDR to detect endpoint threats beyond malware, patch management to detect unpatched software, and email protection to detect incoming email threats. They're not enough to cover all problems, but they can help with quite a few.

3. Recover and Encrypt

Any defense strategy requires the ability to quickly recover after a disaster. The first two pillars can prevent a fair amount of attacks, but they're not bulletproof. By implementing good backup solutions to restore systems quickly, two-factor authentication for account recovery, and strong encryption to prevent unauthorized access to intellectual property, you can help provide your clients with a kind of insurance policy against data theft and downtime.

4. Analyze and Manage

The final layer involves advanced security tactics and active management. Many businesses require a more in-depth approach than the first three pillars can provide. This step involves penetration testing, security incident and event management (SIEM) systems, and security operation centers. This pillar is often handled by specialized managed security services providers (MSSPs). Even if you don't have an interest in becoming an MSSP, it's important to be aware of these practices. In fact, you may want to partner with an MSSP to provide these advanced services for clients who need them.

But before you start utilizing the practices and technology of the four-pillars model, you'll have to assess the security situation for each client. We recommend starting with a discovery phase.

Discovery

Whether you're starting out with a new client or reviewing the security state of an existing customer, start by taking stock of existing security defenses. Whether it's out-of-date AV, infrequent scans, unpatched software, or inconsistent backups, nearly everyone can improve on something.

Start by going through this list of questions—asking these can help you formulate your plan for implementing the four pillars.

Monitoring

- What general security monitorin g do you have in place?
- Do you monitor user activity?
- Do you monitor physical security devices?
- Do you monitor access points?
- Do you monitor IP-enabled cameras?

Security Management

- What kind of endpoint protection do you have in place? Do you have an EDR solution? If not, do you use antivirus? How often do you run scans?
- Do you have a patch management solution in place? If so, how often do you update your software?
- Do you have email security in place?
- Do you have password management controls in place?
- Do you have a comprehensive employee departure process?

Risk Mitigation

- Do you have a defined data management program?
- Do you test the data management program?
- Do you track user access to sensitive data?
- Are you required to adhere to any regulatory acts?
- How often do you assess your security?

Active Management and Analysis

- Do you limit employee access to corporate data and select areas of the network?
- Do you have internet content controls in place?
- Do you train employees on security protocols?
- Do you manage the core network to avoid malicious activity?
- Do you have failover/redundancy on the full network?
- Do you have a CTO/CSO on staff or a virtual CTO/CSO?

Once you have answers to these questions, you can start implementing the model. However, please view these questions as a starting point—don't take answers at face value. For example, you may find user training on security protocols occurs only when a new employee or group of employees start. In this case, you should suggest updating employees on security protocols on a regular basis, both to remind and update them on any new processes.

Pillar One: Prepare

When it comes to the first security pillar, the basics matter. You should prepare your environment to close off as many attack vectors as possible—and you should keep up with these measures on a regular basis.

First, add safeguards for physical access to the office building and devices. For any office space, make sure only active employees have access to the building. Keep an inventory of each key card so when employees leave the company, you can recover or deactivate the keys.

This applies to physical equipment as well. Unfortunately, many employees try to keep equipment (like laptops, smartphones, or tablets) after leaving the company. Keep track of each device using a remote monitoring and management (RMM) solution with inventory tracking. Even if you can't recoup the device following an employee departure, you can use your RMM solution to lock the device or wipe the data on it to help prevent ex-employees from stealing or sharing intellectual property. Note this is equally important with remote workers. Any company-issued devices are easier to steal if they're not physically in the building. Make sure you can remotely wipe these devices as well. Writing off the loss of a remote worker's laptop is one thing—you don't want to add a data breach into the mix.

Next, double-check the webcam security. Hackers can get into webcams and spy on employees—or on important meetings in conference rooms. But the threats go beyond simple spying; criminals can also employ webcams to form a botnet used in a distributed denial-of-service (DDoS) attacks. In short, monitor your webcams—they're an easier access point than you'd expect.

Additionally, make sure to use strong passwords on Internet of Things (IoT) devices beyond just webcams. With an increased number of workers shifting to home-based networks, the attack surface has increased. Each device on a home network represents a potential access point—smart thermostats, smart TVs, and smart speakers. If it connects to the Wi-Fi, it's a potential access point for criminals. Make sure your users set strong passwords on devices and do the same for any related apps and web portals to administer those devices.

In fact, you should take the time to require all users to set strong, unique passwords on important accounts. Also, set up a schedule to have users automatically reset their passwords at least every 90 days. It's worth considering a corporate-grade password manager to help enforce password best practices.

All this speaks to an important point—monitoring. Find a strong RMM tool to help you monitor traffic in and out of your corporate network—covering all internet access points, including firewalls, routers, and switches. You should monitor any internet-connected devices, including webcams or web-connected printers, for any issues as well.

It’s also critical to set up policies to handle remote employees. Make sure they have VPN software installed to access corporate resources when they’re not in the building. This can help prevent them from exposing the main corporate network to a potential attack. Additionally, when accessing critical systems outside the office, try requiring two-factor authentication.

Finally, remember this stage is about laying the groundwork for strong security. At this stage, for any managed devices, schedule an automatic cadence for patching, running backup, and updating antivirus definitions (if using an AV solution).

Technology for Pillar One

- VPN software
- Corporate password management tool
- RMM tool for in-depth monitoring and ongoing management

Pillar Two: Detect

The next pillar of security covers your detection capabilities. Once a security attack of some kind, whether spear-phishing, malware, or ransomware, gets past your initial defenses, you need to be able to detect it fast and stop it cold.

For years, people used AV solutions as a major line of defense against cyberattacks. AV solutions still work, of course. But most rely heavily on signature-based scanning to detect, quarantine, or remove viruses. This means you must keep up with signature updates, which is why we recommended scheduling updates in the previous section.

Detecting threats today can require heavier artillery. EDR solutions detect threats against endpoints beyond malware. Instead of taking a signature-based approach, EDR solutions use artificial intelligence and machine learning to detect threats at the endpoint level. When suspicious behaviour occurs at the endpoint level, an EDR solution can flag that behavior or act automatically. This is particularly important in today’s environment as cybercriminals have shifted tactics to use malware evasion techniques and fileless attacks. If clients want to stick with AV, it may better fit their budget—but for more complete detection, an EDR solution better fits the bill.

Additionally, EDR may be particularly helpful for remote workers. As workers connect to networks at varying security levels (including their own home network), using additional endpoint protection can help protect both them and the wider corporate network.

Next, you need a strong patch management solution. While we mentioned scheduling regular patching as part of the previous step, make sure to check your RMM solution regularly to detect endpoints lacking the latest security solutions. Beyond the OS, it’s important to choose a solution that handles patch updates for third-party software, especially for commonly exploited programs like Adobe® products, Java®, and the major web browsers.

Next, you can work to reduce potential threats with email protection. Email is the top attack vector. Unfortunately, the native email security in many email solutions simply isn't enough. Add an email security solution that uses real-time pattern recognition and collective threat intelligence to detect active threats against users. Email security can act as insurance against the most common threats. A strong email security solution should include AV and aggressive spam protection to help detect potential threats. Some email security solutions also use collective intelligence from their user base to help protect users against active attacks.

The detection phase can involve a lot of active upkeep. If you're managing thousands (or tens of thousands) of endpoints, updating software with the latest patches or maintaining the latest virus definitions can quickly become unwieldy. That's why we recommend you find tools to automate as much of the process as possible.

For example, when looking at patch management solutions, you should be able to set rules, like requiring a download, update, and quick reset whenever a critical security patch becomes available for the OS. Any good RMM solution would likely involve some level of automation, but many provide additional scripting and even drag-and-drop automation capabilities.

Technology for Pillar Two

- Antivirus (good) or endpoint detection and response (better)
- Patch management for both OS and third-party software
- Email protection

Pillar Three: Recover and Encrypt

The next layer focuses on account recovery, system recovery, and data protection. Your previously implemented defense layers can prevent many issues, but they aren't bulletproof. It doesn't even take a technical hack. User errors are common and natural disasters can also cause problems (from a small electrical fire to a flood all the way to a major earthquake).

Before you start on this step, consider any regulations your clients may be required to follow. Whether industry-related like healthcare, finance, or government or based on regional requirements like the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA), many companies have to follow clear standards regarding data governance. You should familiarize yourself with these if your clients work within a regulated industry or in a regulated region.

While this should be set earlier, try to get users to employ two-factor authentication (2FA) for login accounts and devices. Employees may use the same password across accounts, despite your best efforts to train them out of this practice. If their accounts are compromised elsewhere, this opens the company up to significant risk. 2FA can alert users to someone potentially trying to compromise their account. Additionally, it can streamline the process of resetting passwords in case someone gets locked out of their account. You may want to consider looking into a self-service password reset portal for end users to take some of the burden off your staff.

Next, develop a policy on software. Employees often install their own software. That can leave you vulnerable to both security and liability issues. For that reason, you have two basic options:

1. Create a blacklist of software to prevent employees from installing them on their systems.
2. Block all software installations unless approved and installed by an administrator. This requires more management but could be worthwhile in the long run.

Next, assess the quality of your clients' backup solutions. If you're using a cloud-based solution, look for one built cloud-first. These solutions use deduplication, compression, and WAN optimization techniques to help you back up data to—and restore from—the cloud relatively simply. By allowing for faster backup windows, these techniques let you back up files more often without having to worry as much about resource usage or business disruption. You don't want out-of-date backups during a crisis.

Most also offer on-premises backups; however, don't assume you need to purchase an expensive backup appliance to cover this. Some allow you to meet the "3-2-1" backup rule by creating an on-premises version using whatever hardware you have lying around, like a USB drive or an external hard drive.

Additionally, make sure your backup solution lets you automate as much of the process as possible. You should also be able to check backup jobs from a single web-based console. When a crisis hits, you want to quickly check your system logs to make sure the data hasn't become corrupted. It helps to look for a solution that lets you easily back up servers, workstations, and critical business documents from a single dashboard. This can help you save time across your entire customer base.

Earlier, we mentioned using EDR solutions for detecting threats. Some EDR solutions can help during the recovery process as well. For example, after a ransomware attack, SolarWinds® EDR, powered by SentinelOne®, can automatically roll an endpoint back to a known safe state, minimizing disruption to the end user. This allows for rapid recovery and gives you a chance to figure out what went wrong and close the vulnerability.

You'll also need to provide a disaster recovery plan. Developing a disaster recovery plan could be the topic of an entire white paper itself, so we won't go into it here. However, remember—this recovery plan should cover both data and equipment recovery, and it should go beyond problems arising from cybercrimes, as natural disasters and human error can play a major factor as well. Whether you personally provide the recovery plan, work with your clients' internal IT team, or outsource to a third party, your clients need a playbook outlining the most likely disasters and steps to restore continuity (and sanity) to the business.

These plans take time and can be in-depth, so don't hesitate to work with a specialized firm for help on delivering this aspect of the service.

At this point, you also want to add data encryption on all devices. Some clients may view this as unnecessary, but it can protect against malicious actors pulling data from a stolen laptop, tablet, or smartphone. It may also be necessary to meet certain regulatory requirements, so again, make sure to double-check the laws for your clients' industries.

Technology for Pillar Three

- Backup solution
- Endpoint detection and response
- Two-factor authentication
- Password reset portals
- Device encryption capabilities

Pillar Four: Analyse and Manage

The final pillar consists of both day-to-day management as well as long-term analysis. This stage involves a lot of hands-on work and sophisticated tools that may be beyond the realm of many MSPs; however, familiarizing yourself with these tools and practices—and outsourcing when necessary—is important for providing complete services to your clients. As these services are often the domain of MSSPs, you may want to partner with one to provide the comprehensive value your clients are looking for.

First, look at a more robust firewall to protect your clients. A unified threat management (UTM) solution can help add a strong, enterprise-grade firewall as well as multiple other helpful technologies, like gateway AV, antispam, and network intrusion detection.

Next, start inspecting security information and event management (SIEM) solutions. An SIEM involves both a large-scale database and advanced data analysis tools to help you assess security trends. The most robust tools include forensic analysis and searching, threat intelligence that alerts you to bad hosts, monitoring for external devices being added (like USB drives), and even compliance reports.

If you have a SIEM tool and the specialized knowledge to use it, use the data from your SIEM solution to start blocking malicious domains and sites you come across. Many web content filtering solutions come with a default list of known malicious sites that will block users from visiting. However, you can also customize these rules and add more sites to the list—or select from classes of sites, like social media or gaming, to keep employees productive during the work day. Web filtering solutions help protect against several major issues, including drive-by downloads, phishing sites, and URL hijacking.

The challenge is these systems can often be difficult to maintain and adopt. In fact, we considered adding SIEM tools as part of the detection pillar, but they require active analysis and management to run and specialized knowledge to analyze and respond to threats. As a result, they're not as plug-and-play as an EDR solution would be. Additionally, data analysis and storage are specialized skills—meaning this level of service often comes attached to those with large security budgets. But as threats have grown costlier and more frequent, many midsized organizations have begun looking for SIEM providers to help them deal with threats.

To take things to a higher level, consider offering security-operations-center (SOC) services for your clients. A SOC usually requires a team of security experts to run. They offer 24/7 threat monitoring for cybersecurity incidents and remediation recommendations for incident response teams. These services may be overkill for many clients, but some regulations, like PCI DSS, require a SOC. In this instance, we highly recommend partnering with an MSSP offering SOC services—if you don't have the capabilities in house.

Finally, if you have the capabilities, periodic penetration testing can help with security readiness. Pen testing software will "war game" out different security scenarios that could arise. These tests show how hackers might attain a goal, like accessing sensitive data or taking down a network. You can use the results to address vulnerabilities and shore up your security. It's worth running these tests at least once a quarter to stay up to date.

Technology for Pillar Four

- UTM
- SIEM
- SOC
- Penetration testing software

Can IT Service Providers Afford Not to Provide Layered Security Services

Cybercriminals aren't going away. Their methods will continue to get more punishing as they evolve to meet new security protocols and standards. Any business that houses sensitive data—and that's virtually all businesses—will likely always face some level of threat.

What does that mean for the future?

With the severity of cyberthreats over the recent years, many IT service providers may be required to offer security services. When your clients have a problem with their IT—any kind of problem—they're likely to look to their MSP to fix the issue. It won't matter if your clients fall victim due to human error or if their systems get locked out due to ransomware, they will simply want their problem fixed.

For many of the services offered in this eBook—like patch management, EDR, and backup—you'll simply need to get the right tools to manage and automate. This is basic cyberhygiene, and MSPs should be comfortable offering these services. However, the current cyberthreat landscape may require you to shift into providing more advanced services, like those mentioned in pillar four. Thankfully, you don't have to go it alone—partnering with an MSSP can allow you to help deliver these services more easily.

If you're not currently a full-fledged managed security services provider, taking on more security responsibility may seem daunting. But use the model in this eBook as a guide and flesh out your layered security strategy as you go. Your clients will likely thank you—and more importantly—they'll trust you in the future.

solarwinds msp

Learn more today at
solarwindsmsp.com

SolarWinds (NYSE:SWI) is a leading provider of powerful and affordable IT management software. Our products give organizations worldwide—regardless of type, size, or complexity—the power to monitor and manage their IT services, infrastructures, and applications; whether on-premises, in the cloud, or via hybrid models. We continuously engage with technology professionals—IT service and operations professionals, DevOps professionals, and managed services providers (MSPs)—to understand the challenges they face in maintaining high-performing and highly available IT infrastructures and applications. Targeted for MSPs, the SolarWinds MSP product portfolio delivers broad, scalable IT service management solutions that integrate layered security, collective intelligence, and smart automation. Our products are designed to enable MSPs to provide highly effective outsourced IT services for their SMB end customers and more efficiently manage their own businesses.

This document is provided for informational purposes only. SolarWinds makes no warranty, express or implied, or assumes any legal liability or responsibility for the information contained herein, including for the accuracy, completeness, or usefulness of any information.