Integris.

Why Use a Managed Security Service

Integris.

CONTENTS

03 INTRODUCTION: THE GROWING CYBER SECURITY THREAT

04 WHAT IS A MANAGED SECURITY SERVICE PROVIDER?

06 WHAT SERVICES DOES AN MSSP PROVIDE?

07 END USER EMPLOYEE TRAINING

- Next-Generation Firewall Protection Network Monitoring
- 24/7 Networking Monitoring
- Offsite Backups and Recovery Plans
- Antivirus Services
- Email & Web Filtering
- Breach Prevention Services
- Automated Updates
- Password Regulations
- Encryption Services
- Security Assessments
- Dark Web Research
- Multi-Factor Authentication

18 Conclusion

INTRODUCTION: THE GROWING CYBER SECURITY THREAT

There have been a record number of cyber attacks in recent years. According to Security Magazine, there was a 1000% increase in phishing attacks in 2017 and 1.9 billion data records were lost or stolen in the first half of the year alone.[1]

In a report released by SonicWall, a network security supplier, the number of unique ransomware variants they've found had increased by 101.2% in 2017, even though there was an overall decline in ransomware attacks in 2017. SonicWall also reported that levels of malware activity in 2017 were 51.4% higher than in 2014, despite a modest decline in unique or new malware signatures.[2]

Hackers, cyber criminals, and the malware industry are constantly switching tactics to take advantage of new vulnerabilities. With the growing number of cyber attacks in the United States and around the world, businesses both large and small are coming to a harsh realization: they are not prepared.

Even enterprise companies and multinational corporations are discovering that their current IT security is not sufficient to fend off an ever-evolving list of security threats. This is perhaps most evident in the recent high-profile data breaches that have made headlines.

The breach of a company's network has the potential to result in catastrophic losses of data and exponentially high costs. A breach can tarnish a company's reputation, making it harder for them to do business in the future. It can even have deep ramifications for the wider community. In fact, security breaches at large companies have rocked our financial markets and even threatened our very infrastructure.

It's tempting for small-to-medium sized businesses to assume that they won't be a target because of their size, and that threats such as ransomware, malware, and phishing scams are far away. The reality is that the interconnectedness of the global business community has proven that a breach on almost any network can lead to a disaster. Dependence upon cloud computing and an increasingly remote, mobile workforce means threats that compromise one system can compromise a larger network relatively easily.

All it takes is a single opening. To combat these threats, businesses are naturally turning to their own IT departments to shore up their networks, implement disaster recovery plans, and coach their fellow employees on data security.

Unfortunately, skill shortages and budget constraints have made security a significant challenge even at the largest, most well-funded companies. To augment their own IT departments, manage costs, and gain access to additional IT resources, businesses of all sizes have relied on managed service providers (MSPs). Most recently, however, they've been seeking the help of outsourced IT security specialists known as managed security service providers, or MSSPs.

WHAT IS A MANAGED SECURITY SERVICE PROVIDER?

First, it's important to understand the difference between an MSP and an MSSP. A managed service provider is a third-party organization that is contracted to perform ongoing IT services. Unlike a value-added reseller (VAR), MSPs typically partner with their clients over multiple years, acting as an outsourced IT department.

A managed security service provider is similar to a managed service provider, but with more cybersecurity capabilities such as virus and spam blocking, next-generation firewalls, breach detection, and end user security training. An MSP can function as an MSSP. "MSSP" is merely the designation of a type of service offering or product, not necessarily a classification for a type of company.

Both MSPs and MSSPs can assist their clients during any stage of their IT lifecycle, whether they are just starting to create policies or they just need extra help monitoring their networks.

Some MSSPs are new entities that came into business among the growing cybersecurity threat. Others were traditional MSPs who evolved new cybersecurity capabilities because of increasing demand from their clients or because of the growing market for security within the broader business community.

Businesses and organizations may outsource some or all their IT security functions to an MSSP, depending on their needs. Either way, an MSSP's services can augment any internal IT department and align perfectly with their operations.

The following are a few reasons business rely on MSSPs:

1. THERE IS AN ONGOING IT SKILLS SHORTAGE.

There are not enough skilled IT candidates in the job market to fill every position at every company. Similarly, there are not enough cybersecurity specialists to handle the markets' needs.

Hackers and scammers may work individually or in small groups, but it takes an army of IT professionals to defend against them.

2. IT DEPARTMENTS ARE OVERSTRETCHED.

Not every business wants to outsource their IT and cybersecurity efforts completely, but their own IT department doesn't have enough bandwidth to handle all their challenges. Finding more IT staff is costly and can take months, so it makes more sense to outsource and augment their current team.

3. EVEN SMALL BUSINESSES NEED ENTERPRISE LEVEL SECURITY.

Although enterprise companies are tempting targets for hackers, small businesses are not exempt from attacks either. Small businesses that work with larger companies often store sensitive data, making them a tempting target for hackers.

Most small businesses can't afford to keep a team of IT security specialists on staff. Relying on an MSSP is an ideal way to get the capabilities they need without overburdening themselves with cost.

4. THE THREAT LANDSCAPE IS CONSTANTLY EVOLVING.

Most companies need to focus their energy on selling, growing, and providing quality products and services. They have little time to educate themselves about new cybersecurity threats, or to learn new technology and scale up their IT department. An MSSP's entire business model is built on their ability to identify threats, educate their clients, and scale with new technologies.

There are no prerequisites for partnering with an MSSP other than the need for better security or more IT resources. MSSPs can offer a broad range of IT security services to small-to-medium sized businesses, large corporations, and internal IT teams.

WHAT SERVICES DOES AN MSSP PROVIDE?

The best MSSPs have extensive expertise and more security experience than many companies can develop in-house. They work as an extension of your business through consulting, planning, and hands-on action. To obtain comprehensive security across your entire business, you need a full suite of services working in tandem.

The following are some of the essential services offered by MSSPs:

- End User Employee Training
- Next-Generation Firewall Protection
- 24/7 Network Monitoring
- Offsite Backups and Recovery Plans
- Antivirus Services
- Email & Web Filtering
- Breach Prevention Services
- Automated Updates
- Password Regulations
- Encryption Services
- Security Assessments
- Dark Web Research
- Multi-Factor Authentication

END USER EMPLOYEE TRAINING

Hackers, cyber criminals, and other bad actors have become menacingly skilled at attacking and breaching networks. But the truth is, the number one cause of security breaches at most companies is employee negligence, or a lack of employee security education.

According to a study reported by Tech Republic, 54% of the 1,000 IT professionals surveyed said poor password policies and the careless actions of employees were the root causes of cybersecurity incidents at their companies. More than 50% of the companies surveyed had experienced a ransomware attack in the past year, and 79% of those affected said the ransomware entered their system through a phishing email or some other socially engineered attack.3

Other common issues include poor password maintenance, a lack of two-factor authentication, or having no password regulations in place at all. Often, all it takes for a data breach is a lost smartphone, a weak password, or a simple mistake when opening an email.

While it's important to strengthen your network, the human factor must be addressed for your security effort to be successful. MSSPs can be contracted to create a culture of security at your company.

They'll coach your employees to recognize common security threats like phishing emails and malignant links. They can even help you establish a password policy so that passwords are regulated and changed regularly across the company.

"All it takes for a **data breach** is a lost smartphone, a weak password, or a **simple mistake** when opening an email."

NEXT-GENERATION FIREWALL PROTECTION

A Next-Generation Firewall (NGFW) combines a traditional firewall with new systems that can detect and block even the most sophisticated attacks. While traditional firewalls prevent unauthorized access to or from a private network, NGFWs provide an added layer of security by detecting and blocking attacks and unauthorized access at the application level.

Web applications are used on websites to capture, process, store, and transmit sensitive data. They enable websites to provide users with dynamic content and can facilitate familiar applications like shopping carts, checkout pages, and login screens.

These web applications are increasingly becoming a prime target for hackers because of all the sensitive information they transmit. When compromised, a web application can act like a backdoor into a system or a conduit for transferring sensitive data to attackers. According to SonicWall, nearly 5% of all file-based malware propagation attempts were hidden by encryption.[2]

Encrypted malware is more difficult to detect by standard corporate firewalls. To combat this, an NGFW maintains up-to-date information about web applications to block malware and viruses that might attempt to enter your system through them. It intercepts all incoming traffic, decrypting and inspecting every packet.

NGFW technology can also include virtual private network capabilities, rule-based intrusion prevention, and reputation-based malware protection.

24-7 NETWORK MONITORING

Most organizations can't afford to maintain an in-house IT professional to manage their network every hour of every day. Network monitoring is an important service provided by MSPs, typically to monitor for network outages, server overloads, and other errors by scanning critical network functions.

MSSPs provide 24/7 network monitoring to identify similar issues, but also manage firewalls, scan for vulnerabilities, provide intrusion protection and prevention, and provide anti-virus services.

MSSPs can monitor networks continuously via their own security operation center or through data center providers. In the event of an issue or security threat, notifications are sent to stakeholders, and engineers at the MSSP spring into action to resolve problems. The main purposes of network monitoring are maintaining network uptime and preventing intrusions.

OFFSITE BACKUPS AND RECOVERY PLANS

Data backup, in some form, is common at most companies. They may save key data to the cloud or store it on a dedicated device that they keep in-house. However, plans such as these won't always serve in the event of a disaster.

Offsite data protection ensures your data is secure and ready to be recovered in the event a system crash or internal error. It also ensures your data is protected in the event of a natural disaster, such as a fire or a flood. From a security perspective, backing up your data is a means of picking up where you left off even if your data is stolen in a ransomware attack.

An MSSP can provide you with offsite backups as well as a recovery plan. Having a recovery plan in place makes the transition from backup to full operation much easier. After doing an assessment of your data, an MSSP should be able to provide you with an estimate on how long it will take for you to recover in the event of a disaster.

ANTIVIRUS SERVICES

Many organizations still rely on basic anti-virus packages to secure their systems. Many have also been tempted to rely only on a layering of multiple free programs to secure each individual computer at their company.

While many free, and even paid, antivirus suites are well-suited for personal use, they are not ideal solutions for businesses. You should be able to manage and monitor all your devices from a single platform. Your antivirus software should receive automated updates and provide advanced protection beyond personal computing.

To combat growing security threats, businesses today need a layered approach to security. This includes enterprise-level antivirus software as well as anti-malware, Next-Generation Firewall Protection, intrusion detection and prevention, and well-trained employees. An MSSP provides all of these security layers as part of a package to your organization.

EMAIL & WEB FILTERING

Email filtering is a tool for identifying spam and phishing emails and either deleting them or relegating them to a specific folder in your inbox. Most mainstream email platforms, such as Gmail or Office 365, have a built-in spam filter. But if your email is hosted in your office, you'll need a 3rd party spam filter.

Despite these filters,some spam will always make into your employees' inboxes. Spammers and email spoofers have become sophisticated in getting past spam filters. This poses a threat to your business. An MSSP can provide you with additional email filtering services as well as employee coaching to help you identify spam and phishing emails before they're opened and clicked.

The security tools provided by an MSSP can also help you filter out malicious websites when your employees are browsing online. To increase employee productivity, you can also use web filtering to block specific types of content such as online shopping sites, social media sites, and gaming sites.

BREACH PREVENTION SERVICES

There are many different types of security breaches, but there are some misconceptions about how they typically occur.

Pop culture often depicts a hacker as someone sitting in a dark room attempting to get past a login screen while ominous code flashes across their screen. While this scenario isn't unheard of, most data breaches do not occur this way. Breaches are most often the result of employee negligence, social engineering attacks, or malignant people within an organization.

Breach prevention involves securing your data from both external and internal threats.

Breaches can happen in several ways. A breach could occur when an employee logs into your network over an unsecured wifi connection at a coffee shop, or when a disgruntled employee brings data home on a flash drive and uploads it to the dark web.

Breaches can also occur because someone at your organization clicked on a link in an email from someone that appeared to be a colleague but wasn't. As such, security must move beyond the IT department and into your organization as a whole. In addition to monitoring for attacks and unusual behavior, an MSSP can help you create a culture of security at your company through training, monitoring, and technical expertise. They'll help you get control over who is accessing your data so you can stay proactive and prevent dangerous activity before it occurs.

AUTOMATED UPDATES

Updates to your applications, software, and operating systems are typically sent to protect you against a new type of threat or to patch vulnerabilities that have been discovered within your digital tools. At the very least, they are designed to improve the functionality of your software.

These updates don't always download and apply themselves automatically. They must be authorized by a user, or by an administrator. Too often, important updates are neglected because internal IT staff are overstretched or unsure of what an update will do to the system. When updates are neglected, your system becomes vulnerable.

An MSSP identifies outdated software and provides automated updates and patching services so you'll never need to manually go through your systems and apply updates yourself. With an MSSP, you'll never have to worry about missing updates and making yourself vulnerable to avoidable threats.

WHEN **UPDATES** ARE **NEGLECTED**,
YOUR SYSTEM BECOMES **VULNERABLE**

PASSWORD REGULATIONS

Generally speaking, people are notoriously careless about password security. When you combine business data with non-existent password regulations, you create a high-risk environment for a data breach.

At many companies, employees are responsible for creating and maintaining their own passwords. To make things easier, they may use the same password for all their accounts. They may use passwords that are 5 to 10 years old, or they may use a very weak password like "123456," "password," or their name and birthdate.

According to Pew Research Center, 86% of Americans in 2016 said they memorize at least some of their passwords, which would be impossible if those passwords were as strong as they should be.[4]

Passwords like these are easy for password cracking programs to decipher. If the same password is used for multiple logins, it could give hackers access to your entire system as well as any software you use. Part of the issue is that too much of the burden is placed on individual employees, many of whom simply want to log in and get to work easily.
Without any guidance, they're likely to pick a password that's easy to remember and stick with it.

An MSSP can help your company develop a strong password strategy and implement password regulations for all your employees. Password regulations, or password policies, govern how your employees create, manage, and use passwords. You may also benefit from using a password manager, or password storage tool, to help your employees keep track of their passwords. This may be necessary if they use several accounts to do their work.

ENCRYPTION SERVICES

Data encryption is important for businesses that must meet regulatory requirements, but every business should include encryption as part of their security suite. In most cases, an "encrypt everything" approach is usually the best approach, especially when sensitive data may be passing through or coming from your business via email, your website, or the internet in general.

Encryption is about protecting data during transit so that decryption or theft is nearly impossible. There are many forms of encryption including website, email, network, and hardware encryption.

Encryption is becoming the new standard for many businesses. Most major email platforms either encrypt emails automatically or make it easy to encrypt emails yourself. At the beginning of 2017, Wired magazine reported that at least half of the web is now encrypted.[5]

Nonetheless, managing the encryption of your data can be difficult and time-consuming. An MSSP can provide your company with Encryption as a Service (EaaS) so you can focus on other tasks with the knowledge that your data is secure. They can also provide additional network layer encryption and hardware encryption.

Flip a coin once to see if your organization will be victimized by ransomware.

Flip it again to see if paying the ransom gets your data back.

SECURITY ASSESSMENTS

Assessing your IT security periodically is an integral part of preventative maintenance and an ideal way to keep yourself and your data protected. Many organizations are bound by regulations and must have certain security measures in place in case they are audited, but any organization that handles important data should check their security status regularly.

As your infrastructure changes over time, gaps can form where you least expect them. Taking a "set it and forget it" approach to security can make you vulnerable to new forms of attack.

During a security assessment, an MSSP will look for common problems, including:

- Deficiencies in network architecture
- System configuration errors
- Weak passwords and poor password regulation
- Necessary system updates
- Network vulnerabilities
- Data integrity and confidentiality

An MSSP can provide an initial security assessment of your organization followed by periodic assessments to keep you secure. While these assessments can be technical, an MSSP will present their findings in an actionable format that is easy to understand.

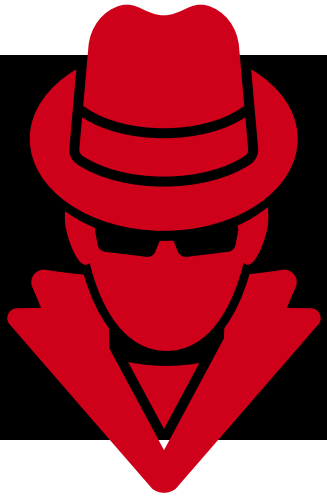
DARK WEB RESEARCH

The dark web, or deep web, is the portion of the internet that is hidden from conventional search engines like Google. It acts as a repository and marketplace for stolen data and plays host to many other illicit activities. When a system is breached, it's common for cybercriminals and other bad actors to post data on the dark web for sale.

If you're concerned that your data might make it onto the dark web, an MSSP can provide you with dark web research to help you protect yourself against the potential damage of such an event.

This service acts as an alert system for when compromised data has been detected on the dark web.

If detected, stakeholders at your company will receive notifications and your MSSP will do everything it can to mitigate the damage. However, the best line of defense against your data landing in the dark web is by preventing a breach in the first place.



IT'S **COMMON** FOR CYBER CRIMINALS TO POST DATA ON THE **DARK WEB**

MULTI-FACTOR AUTHENTICATION

Strong passwords were once seen as the best method for defending against intrusions and protecting data, but it has become increasingly evident that passwords alone are not enough. While you should still focus on creating strong passwords and enforcing password regulations at your company, you should also recognize the multiple ways that passwords can be compromised.

Hackers can decipher passwords using password cracking programs, but passwords can also be compromised by other types of breaches. For example, if your company uses a third-party application that requires a login, your passwords could be compromised if the company that makes that application suffers a security breach.

Once your passwords are revealed, it won't matter how strong they are. If one of your employees' emails is compromised, hackers can reset passwords on all their applications to gain access. At this point, the strength of their passwords becomes irrelevant.

Multi-factor authentication (MFS) is a simple way to create an additional level of security. In a two-factor authentication (2FA) system, an account holder must provide two separate pieces of information to access an account. This often takes the form of a primary password (something the user knows) and a temporary, randomly generated PIN that can be sent to the account holder's smartphone (something the user has) via SMS or email.

This can also be accomplished through a specific device that generates a random PIN, token, or password which the account holder possesses. The second piece of information, or token, is secure because only the account holder has access to it.

Additional layers of security can be put in place for extremely sensitive information. For example, you can add biometrics, such as a thumbprint, as a requirement for access. This will now offer three layers of protection: "something the user knows," "something the user has," and "something the user is."

An MSSP can help your company set up multifactor authentication for all your important accounts and provide guidance on how to use it. It will also educate employees about keeping their devices secure so they aren't lost or stolen.

CONCLUSION

When it comes to security, you can't pick and choose which areas to focus on and which to ignore. Combined, all the services an MSSP offers will provide you with a comprehensive security package that safeguards your entire company, within your budget.

If IT and security issues are draining your resources, or if your team is overwhelmed by fixing gaps in your system, consider starting with a network audit and security assessment from Integris. Simply call us to get started. You'll receive an unbiased evaluation that's easy to understand and can point you toward your next steps.

Integris.

WHO IS INTEGRIS?

We're a one-stop shop for all your managed IT services needs. We look out for you so you don't waste time trying to figure out why your technology isn't working, or spend money to recover from an avoidable breach. When you partner with Integris, you can get back to running your business and leave the rest to us.

We believe that every business has the right to technology that works for them when they need it. We're here to remove the hurdles, keep your equipment proactively updated, and offer your network top-notch protection so you can sleep easy knowing that you, your employees, and your clients are taken care of.

WHY CHOOSE INTEGRIS as your Partner?

When it comes to security, you can't pick and choose which areas to focus on and which to ignore. Combined, all the services an MSSP offers provide you with a comprehensive security package that safeguards your entire company, within your budget.

If IT and security issues are draining your resources, or if your team is overwhelmed by fixing gaps in your system, consider starting with a network audit and security assessment from Integris or email us at sales@integrisit.com. You'll receive an unbiased evaluation that's easy to understand and can point you toward your next steps.

CONTACT US TO SEE IF YOU QUALIFY

SOURCES

1. https://www.securitymagazine.com/articles/88778-2017-was-a-record-year-for-cybersecuritybreaches

2. 2018 SonicWall Cyber Threat Report, 2018 SonicWall, Inc.
https://www.sonicwall.com/en-us/resources/white-papers/2018-sonicwall-cyber-threat-report

3. https://www.techrepublic.com/article/report-negligent-employees-are-no-1-cause-ofcybersecurity-breaches-at-smbs/

4. http://www.pewinternet.org/2017/01/26/2-password-management-and-mobile-security/

5. https://www.wired.com/2017/01/half-web-now-encrypted-makes-everyone-safer/