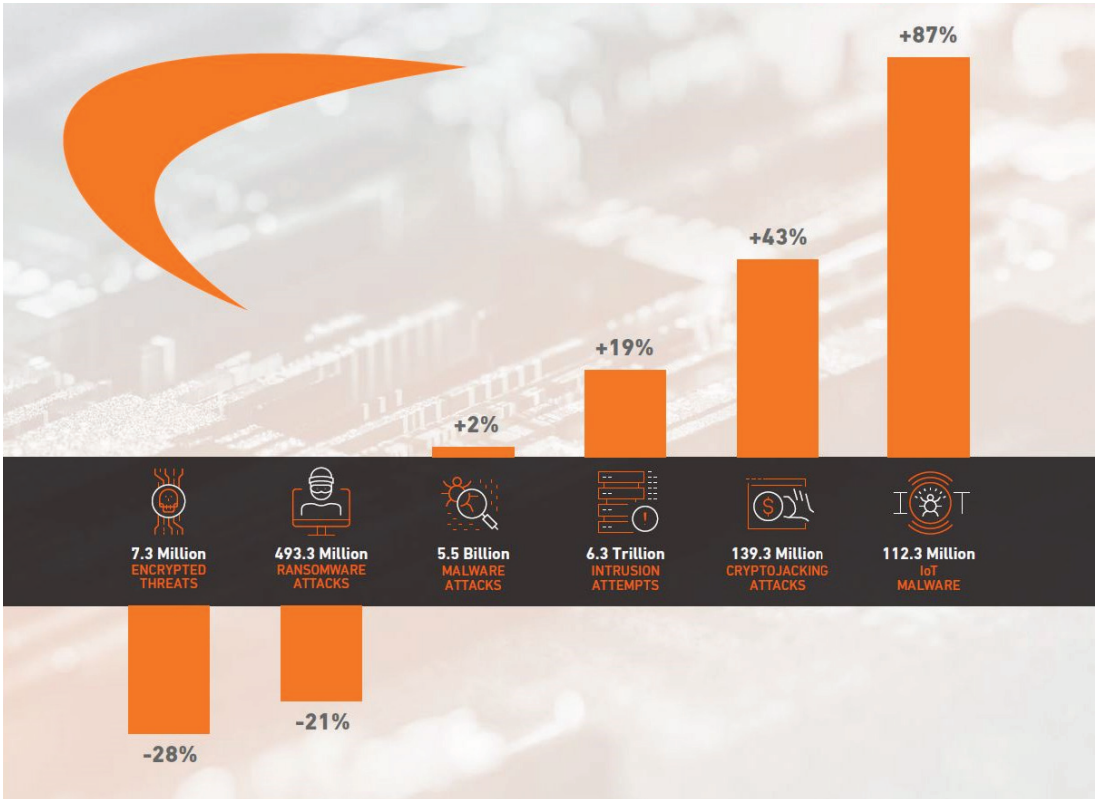
TOTAL SECURE
TECHNOLOGY

MSP vs. MSSP:
Knowing the Difference

How to Secure Data and Technology for a Small to Medium Size Business

A Total Secure Technology Thought Leadership White Paper



SonicWall Cyber Threat Report 2023

Introduction

Based on the news, it might be tempting to conclude that only big businesses are of interest to cyber criminals. Unfortunately, nothing could be further from the truth.

Small to medium size businesses (SMBs) are increasingly seen as ideal targets due to their relatively high degree of vulnerability and their vast numbers compared to larger targets. Yet unlike larger companies, just one damaging hit can wipe out a smaller business.

With the average cost of remediation at $1.4 million, it's no wonder that 60% of breached businesses fold within six months, according to one U.S. Small Business Administration official.

And the number of assaults against SMBs is rising. In a recent 12-month period, 66 percent had experienced a data breach—up from 61 percent in 2021. And that may be understating the case. Most businesses are understandably reluctant to have reports of a breach shared publicly.

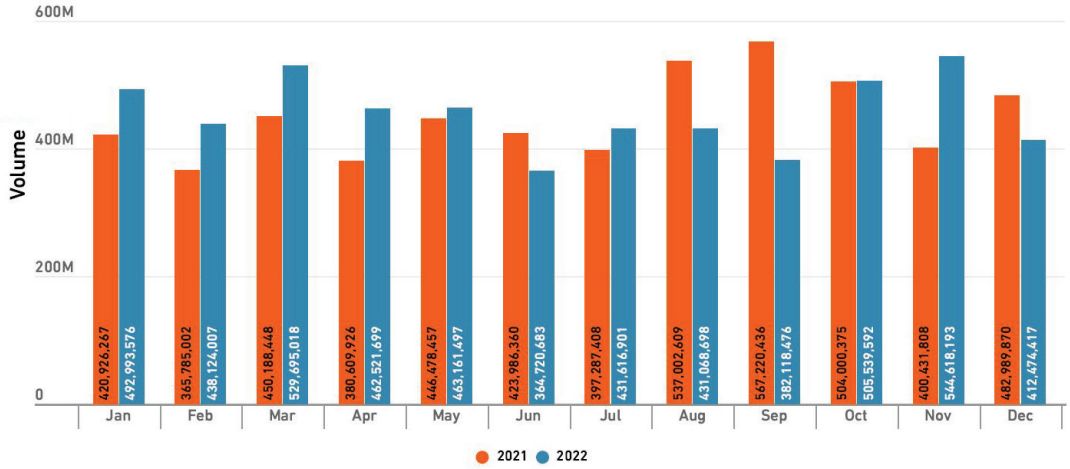
Yet there is good news! With the advent of MSSPs, comprehensive data security has become a more practical and affordable solution for many small to medium size businesses.

The purpose of this white paper is to help you, the SMB owner or executive, to acquire the most cost-effective defense system for your company's critical data. In order to do this, you'll need to clearly discern the differences between an MSP and an MSSP.

Armed with this insight, you'll be better able to find and select the best security partner for your organization. And by doing so, you'll help your organization not only survive in today's cyber battlefield, but also thrive.

GLOBAL MALWARE ATTACK VOLUME

SonicWall Cyber Threat Report 2023



Viability of the Business

With an ever-increasing reliance on electronic information and communication systems, SMBs are more vulnerable to cyber attack than ever before. Consider the case of Brookside ENT and Hearing Center of Battle Creek, Michigan. They were forced to shutter their practice following a ransomware attack in which all their patient records, including surgery notes, contact information and other non-encrypted data were entirely wiped out.

And they are far from alone. In a recent study, the Ponemon Institute found that 66% of small businesses had experienced a cyber attack in a recent 12-month period.

Unfortunately, the risks associated with a data breach don't always stop at the business: owners and key executives of an organization can be held personally liable, especially in certain types of cybercrimes targeting high level officials in a company.

In a 2023 Press Release on their website, the FBI's Internet Crime Complaint Center reported a 127% increase in identified exposed losses due to Business Email Compromise (BEC) scams. Total dollar losses were estimated at $2.4 billion, impacting nearly 20,000 organizations and businesses. And yet, many SMB owners and executives remain unaware of the increasing likelihood of such attacks against them.

Regulatory Risk

Growing a profitable business in today's volatile economy can be challenging enough. Yet, financial success could matter little when all it takes is one government agency to force company dissolution due to regulatory noncompliance.

With data breaches on the rise, especially among SMBs, government bodies are stepping up demands requiring businesses to protect sensitive customer data. Typically, smaller businesses simply don't have the in-house expertise to navigate what seems like an increasingly complex minefield of federal, state and local regulations. This can be especially true if in trying to catch up with new regulations, your business falls behind in maintaining a stable, long-term solution.

Yet in this environment of ever-spiraling regulatory complexity and stringency, you simply cannot afford to get caught with a violation. Staying ahead of the curve on compliance and regulatory issues today demands a higher priority than ever before.

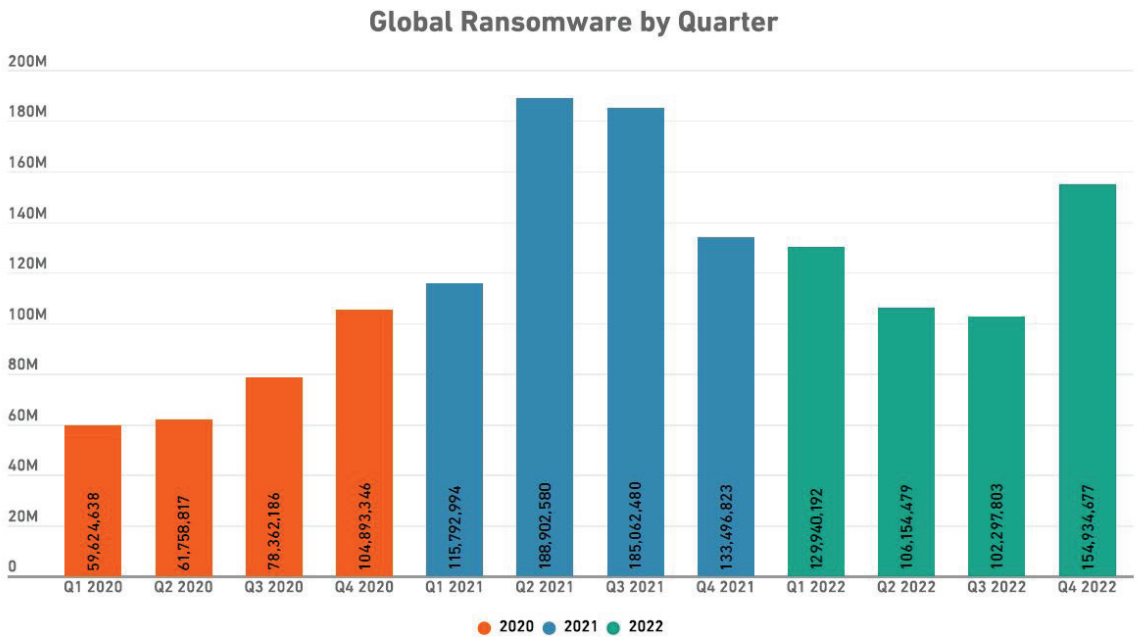
"These type of attacks have ruined the careers of many executives and loyal employees. Successful CEOs have been fired because of it. Stock prices have collapsed. IPOs and mergers have been taken off the table."

- KnowBe4

Cyber Criminals Are Getting Smarter Every Day...

Small and medium size businesses are besieged with an ever-increasing variety and volume of cyber attacks. These attacks occur when least expected and may include phishing, spear-phishing, ransomware, spyware, malware, zero-day, DDOS, social engineering, business email compromise (BEC), and other forms of attack yet unseen.

And, according to a survey by Kaspersky Labs, attackers are presenting SMB owners and executives with an ever-increasing variety of concerns.



SonicWall Cyber Threat Report 2023

The Limits of Cyber Security Insurance

While insuring against cyber risk is prudent in today's world of online communications and technology, it may not fully protect your business. No matter how high your premiums, you may not qualify for claims if you don't take adequate or proper measures.

Consider what happened to Cottage Health System following a system breach. They were held financially responsible—even though they had cyber insurance. Their insurer cited failures to "deploy a system to detect unauthorized access or attempts to access sensitive information stored on its servers."

And what about reputation, and all the intangibles your insurance policy may not cover, such as reputability and customer trust?

According to a recent study by ISACA, nearly 1 in 3 consumers are unlikely to do business with a company that suffered a breach in which financial information was stolen. Sixty-five percent of consumers, however, would be more confident doing business with companies that hired certified cyber security professionals.

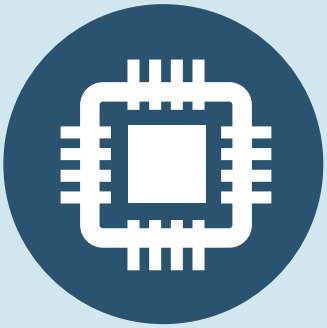
Without a dedicated focus on security, there is little chance you can keep up with all the latest threats that put your business or organization at risk. Managed Threat Security is now a full-time endeavor requiring a properly armed and up-to-date cyber defense arsenal.

We do recommend that you insure properly as well as adequately. However, partnering with a dedicated security professional you can count on is essential to your firm's security today.

TOTAL SECURE TECHNOLOGY

Is Your Company at Risk?

For a quick self-assessment, consider the following questions.



Does your business rely too much on technology alone for data protection?

It's natural to think that an app or a suite of data security tools is enough to keep your data safe. While it may be a good first step, don't forget that in a BYOD world, your defensive perimeter walks out the door in the pockets and handbags of your employees every day. All too often, employee error or a simple lack of awareness can let the bad guys in.

Have your key employees been trained to recognize personally targeted attacks, such as social engineering, spear-phishing and BEC scams?

If Security Awareness Training (SAT) isn't part of your company's onboarding and ongoing training, you could be leaving the proverbial barn door wide open for infiltration and attack. The difficulty is typically not in the training. After all, the training itself is fairly easy. The challenge is enlisting commitment from everyone who touches your data to take the training, and then diligently apply what they've learned to their daily practices.

How much real-time visibility do you have into ongoing threats to your company's data?

A good Security Information and Event Management (SIEM) system provides real-time analysis of security threats generated by your system's apps and network hardware. It's a holistic approach that allows your team to detect, diagnose and take swift action to stay one step ahead of attackers. However, if your current system is narrowly focused on just one or two attack vectors, your data may be susceptible to a runaround in the very areas being monitored.

Have you accurately assessed your MSPs ability to provide comprehensive security for your data?

A common and potentially disastrous misconception is to assume that when it comes to data protection, your "IT guy" has it covered. In the past, that may have been true. However, as the severity and likelihood of cyber attacks against SMBs have escalated, the old MSP model, where an IT service provider was assumed to also be your security analyst, has gone by the wayside. Today, in order to provide the best protection for your organization's most sensitive data, you need the services of a qualified MSSP. It's truly become a matter of survival against increasingly overwhelming and legitimately hostile odds.

Partnering With an MSSP: Today's Critical Edge

MSP vs. MSSP: What's the Difference?

Managed Service Providers (MSPs) typically offer server/desktop monitoring and management, data backup and local network and endpoint support for client organizations. At one time, this model was a good alternative to break-fix or on-demand outsourcing, where these services are provided on a more sporadic, as-needed basis.

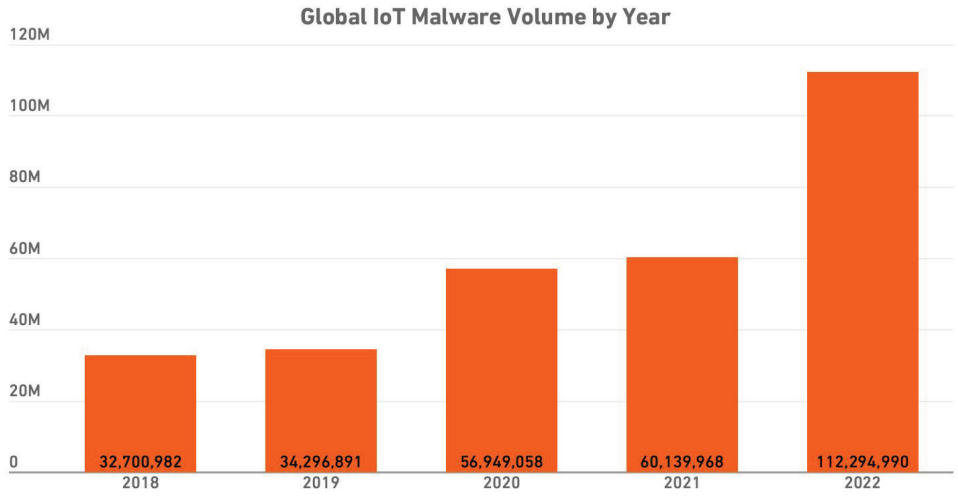
An MSSP, or Managed Security Services Provider on the other hand offers cybersecurity monitoring and management services in addition to everything a traditional MSP offers.

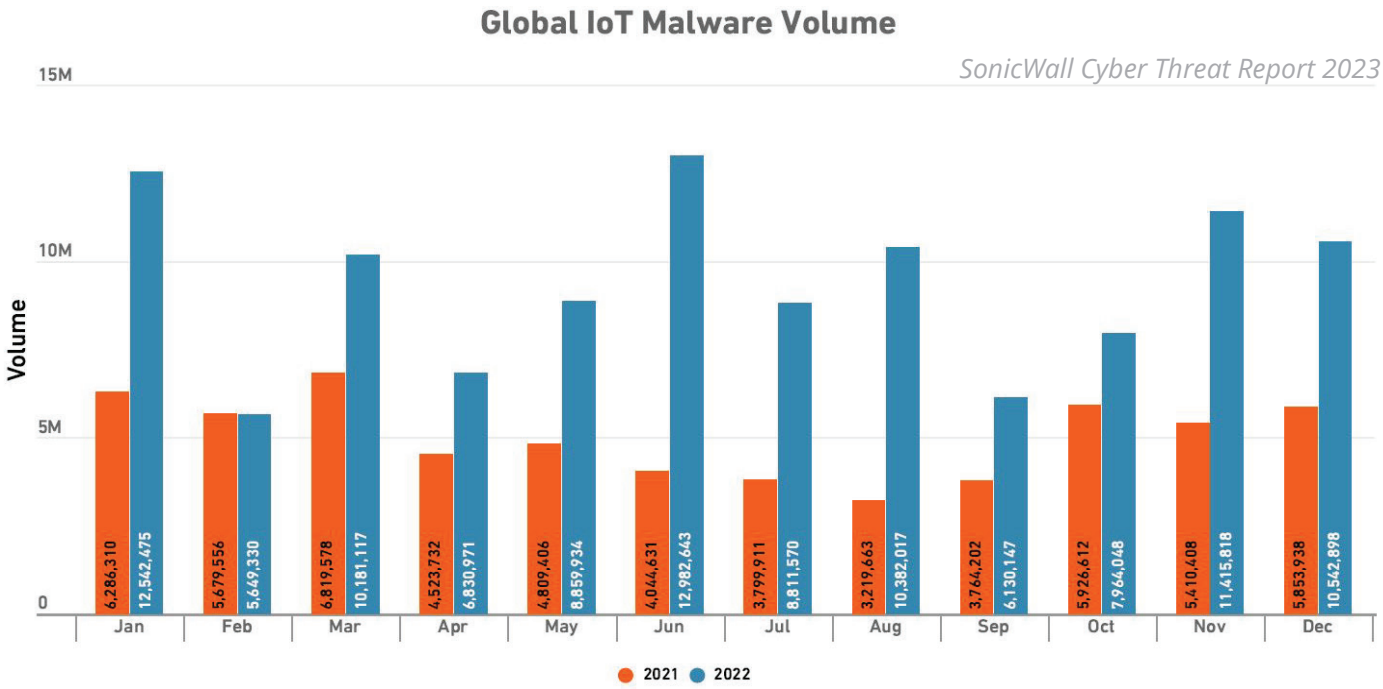
These services may include virus and spam blocking, intrusion detection, firewalls and virtual private network (VPN) management, and more. An MSSP may also handle system changes, modifications and upgrades. However, the key strategic benefit a reliable MSSP can offer is a comprehensive, holistic coverage of all your data security needs.

The chart to the right illustrates the key differences in services you can typically obtain from each type of provider.

Service	MSP	MSSP
Remote Management and Monitoring (RMM)	✓	✓
Onsite Services	✓	✓
Help Desk Support	✓	✓
Network Security	✓	✓
Network Operations Center (NOC)	✓	✓
Security Operations Center (SOC)		✓
Security Information and Event Management (SIEM)		✓
Security Analysts		✓
Cyber Remediation Services		✓
Constant Process Evolution		✓
Advanced Endpoint Protection		✓
Security Awareness Training		✓

SonicWall Cyber Threat Report 2023





As you can see from the chart on the previous page, MSSPs differ from traditional MSPs in at least seven critical areas:

1) Security Operations Center (SOC)

A SOC monitors gateway devices and is responsible for protecting networks as well as websites, applications, databases, servers, data centers, and other technologies. It works in tandem with and complements an organization's NOC (Network Operations Center), whose primary function is to ensure uninterrupted network service.

2) Security Information and Event Management (SIEM)

Security Information and Event Management (SIEM) is a term for software products and services that combine security information management (SIM) and security event management (SEM) in the form of real-time analysis of security alerts generated by network hardware and applications. SIEM is delivered as software, appliances and/or managed services, and can also be used to log security data and generate reports for compliance purposes.

3) Security Analysts

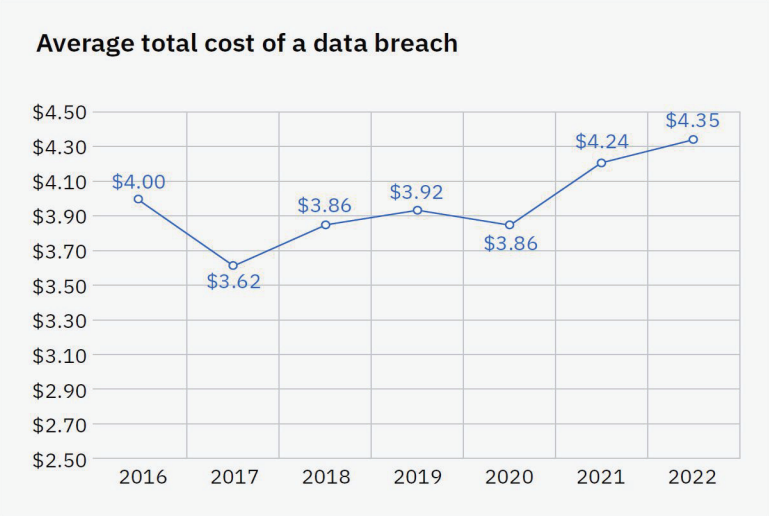
Security analysts are responsible for maintaining the security and integrity of an organization's data. Their main role is to analyze security measures and determine how effective each process is on an ongoing basis. Most SOCs are staffed with multiple CISSPs (Certified Information Security Systems Professionals) working around the clock, 24/7/365.

4) Remediation Services

Once you have comprehensive monitoring and detection, the next step is to address issues as they arise. Not only will a good MSSP alert you of security concerns, they'll take responsibility for remediation to mitigate risk and provide the appropriate due diligence to reduce risk.

5) Constant Process Evolution

A key aspect to success in data security is keeping your systems and processes current, facilitating your ability to remain as proactive as possible. Bear in mind that today's malware is always one step ahead of any prevention system. You've got to remain constantly vigilant to know when your system has been compromised in any way.



IBM Cost of a Data Breach 2022

6) Advanced Endpoint Protection

Antivirus software has been around now since 1987. But it still remains unable to protect against attacks that use unknown threat techniques. It continues to look for a known hash, and small changes to the hash can bypass the system. Antivirus systems also overlook "file-less" attacks that can infect your system's memory, and write directly to RAM.

In 2013, a new type of technology emerged, designed to detect and prevent threats at the endpoint using a unique behavior-based approach. Instead of looking for something known or its variant, like signature-based detection, this next-generation endpoint security analyzes file characteristics (to uncover known and unknown file-based malware) as well as the entire endpoint system behavior to identify suspicious activity on execution.

Known as Endpoint Detection and Response (EDR), it monitors for activity and enables administrators to prevent incidents from spreading throughout the organization. Next-Generation Endpoint Protection (NGEP) then goes a step further and takes automated actions to prevent and remediate attacks.

7) Security Awareness Training (SAT)

Even a single misstep by an employee can open the door to a potentially devastating breach. Security Awareness Training (SAT) helps your team be more informed about security threats and more skeptical about what they receive via email or other channels. SAT helps prevent damaging behaviors, such as clicking on malicious links in email, oversharing on social media, or believing requests delivered through electronic channels without first verifying them.

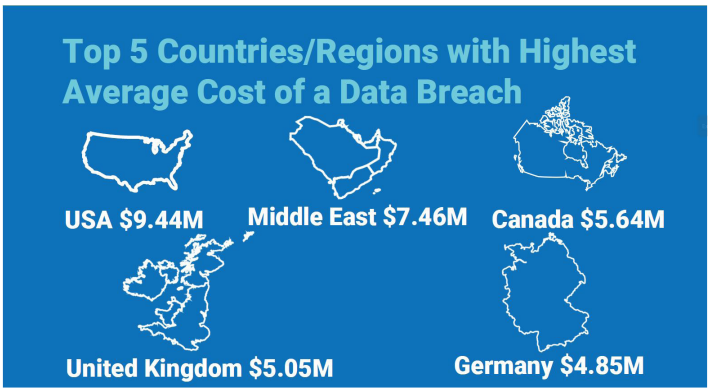
As these points illustrate, when it comes to providing comprehensive data security, there are a number of areas where the MSP model falls short. In a recent occurrence, for example, a local MSP was hacked, resulting in over 80 of their client accounts being subject to a crypto locker ransomware attack. This simply points up the need to work with an IT partner possessing depth of expertise in cybersecurity: that means working with an MSSP.

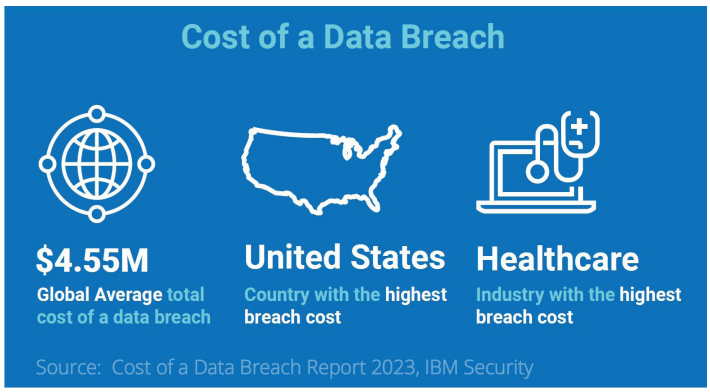
The global **average cost** of a data breach increased 2.6% from **$4.24 million** in 2021 to **$4.35 million** in 2022.

IBM Cost of a Data Breach 2022

Since COVID-19, **47% of remote workers** have fallen for **phishing scams** and the average cost of a data breach for organizations with remote workers was **$1.07 million higher.**

ISACA Journal April 2022





Benefits of Partnering with a Reliable Managed Security Services Provider

Small and medium size businesses today face a never-ending barrage of data security probing and attack. With state-sponsored and non-state actors honing cyber weapons into cheap but effective means of theft and extortion, vigilance in the arena of cyber security is fast becoming a critical factor in setting your organization apart.

The benefits of partnering with a reliable MSSP include:

Efficiency: Instead of separate and competing budgets for detection, prevention and response, you get all three within one holistic service and technology suite.

Compliance: CPRA is just a recent addition to an already crowded alphabet soup of data security regulations. An experienced MSSP can proactively help you navigate the regulations minefield, ensuring that your organization remains free from unnecessary fines, penalties and sanctions.

Enhanced Customer Experience: By allowing customers to do business with you digitally, you can provide them with an exceptional experience. And obviously, safety and security lay the foundation for that experience.

Reduced Cost: Often, the total cost of security services can be hidden upfront until the need arises, at which point they can balloon exponentially. A knowledgeable MSSP can help you avoid these hidden costs.

Disruption Avoidance: By providing a comprehensive suite of services and taking a holistic approach to data security, an MSSP helps reduce your organization's exposure to potentially debilitating attacks.

Insurability: By demonstrating comprehensive data security coverage such as can be provided by an MSSP, your organization is assured of insurability and overall insurance costs may even be reduced.

Peer-to-Peer Relationship: Because most MSSPs are also SMBs, you'll typically enjoy the benefits of working with a partner who understands the challenges of running a business similar in size to yours.

How to Evaluate an MSSP

Before you begin interviewing a potential partner MSSP, it's a good idea to take stock of your data security needs. That said, in order to determine if an MSSP will be a good fit for your business, start with the following key questions:

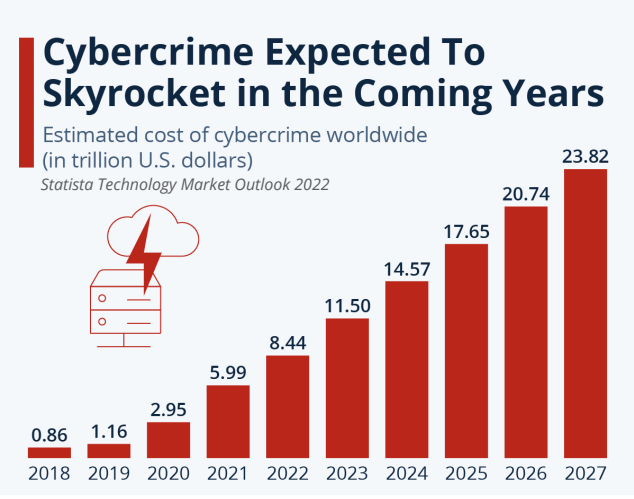
Threat Intelligence Lifecycle: How does their company arrive at its threat intelligence, and how will it be incorporated into your company's response strategy?

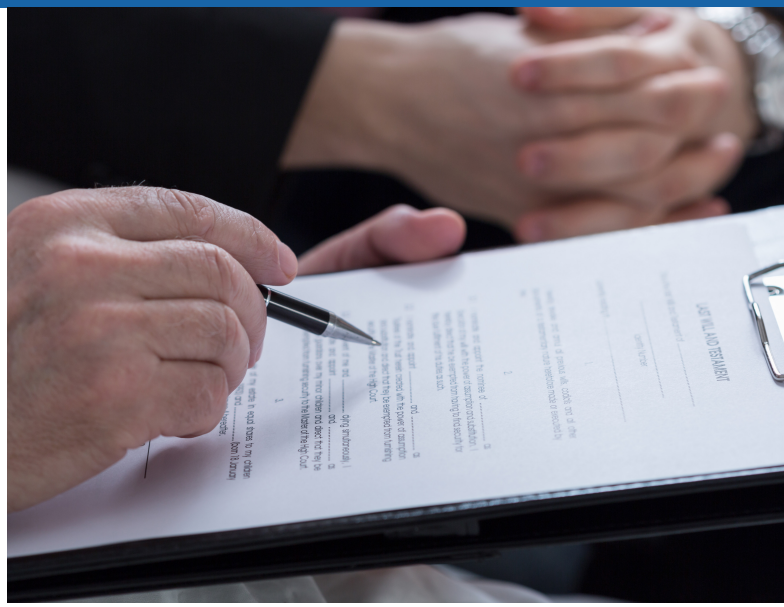
Experience in Execution: Can their service offer best practices in response plans, and do they have mature processes backed by service level agreements?

Commitment to the Mission of Security Service: Do they create a culture of service in delivering support your organization? Are they primarily (or originally) a hardware and software company, or a services company?

Holistic PDR: What is their PDR (Prevention, Detection and Response) system and how well have they executed on it in past situations?

Overarching Approach to Data Preservation: Is their approach tactical, or strategic? Holistic or focused on micromanagement? (Ideally, they employ a multi-layered strategic approach with a single point of command and control.)





How They Handle Their Own Security: How do they monitor and manage their employees that are responsible for managing and monitoring your data? What are their Access Control measures to gain entry into their offices and systems? What are their onboarding practices for vetting and training the people who ultimately manage and monitor your security posture? What kind of background checks do they run on their employees? Do they require multifactor authentication to gain access to your environment?

Current Clients: Who are some of their current clients? Their existing client base reveals much about the type of practices they engage in on a day-to-day basis. Ideally, they include credit unions, banks, hospitals and any other entities that require third-party due diligence.

Visibility into Threat Intelligence: What kind of visibility, reporting and actionable insights do you provide?

You'll also want to know the basics, such as how long have they've been in business, etc. The questions above should help you zero in on the right MSSP for your particular organization.

Where to Begin

If you are at all concerned about your data's security today (and you probably should be), a good first step is to obtain a risk assessment from an experienced data security professional. A risk assessment performed on your company's security infrastructure can reveal threats to key corporate assets and vulnerabilities in your current security controls of which you may not be aware.

About Total Secure Technology

Total Secure Technology (TST) provides tailor-made data security built around your unique business needs. Our holistic approach means you can truly secure your business to the greatest extent possible.

Our 7-Level Protective System helps make sure our clients never suffer a damaging breach. It includes:

1. Network Monitoring and Patch Management
2. Proactive AV (Anti-Virus) and Malware Management
3. Managed Business Continuity
4. Managed Firewall with Content Filtering
5. Managed Gateway DNS Protection
6. Advanced Endpoint Protection (beyond AV and anti-malware)
7. SIEM Monitoring (Systems Incident and Event Management)

TOTAL SECURE
TECHNOLOGY

There are no magic "silver bullets." And none of these systems are a "set it and forget it" tool. They all need to be managed, monitored and reported on regularly. That's why we report monthly, and insist on meeting with clients quarterly, in order to make doubly certain all bases are being covered.

Our experience as an MSP since 1999 and MSSP since 2017 gives us an uncommon advantage in providing you with seamless and comprehensive data management and security. And that advantage enables you to focus on achieving more for your business.

For a Complementary Consultation
to Determine if Your Organization is a Candidate
and for Our 27-Point Security and Network Audit,
Contact Us Today

916-696-7200
sales@totalsecuretech.com

Sources

ISACA Journal — Cybersecurity in a COVID-19 World: Insights on How Decisions Are Made
https://www.isaca.org/resources/isaca-journal/issues/2022/volume-2/cybersecurity-in-a-covid-19-world

Loki Labs — Guide for SMBs: Choosing the Best Managed Security Service Provider
https://lokilabs.io/choosing-mssp/

Reddit — Local MSP got hacked and all clients cryptolocked
https://www.reddit.com/r/msp/comments/ani14t/local_msp_got_hacked_and_all_clients_cryptolocked/

FBI Internet Crime Complaint Center — Pres Release 22 March 2023
https://www.fbi.gov/contact-us/field-offices/springfield/news/internet-crime-complaint-center-releases-2022-statistics

TheNextWeb.com Problem Solvers — Why you should(n't) get cyber insurance
https://thenextweb.com/problem-solvers/2018/09/24/why-you-shouldnt-get-cyber-insurance/

Channele2e.com — Managed Security: 3 Reasons to Make Your MSSP Move Now
https://www.channele2e.com/influencers/3-mssp-business-drivers/

Forbes — Cybersecurity in 2022 - A Fresh Look at Some Very Alarming Stats
https://www.forbes.com/sites/chuckbrooks/2022/01/21/cybersecurity-in-2022--a-fresh-look-at-some-very-alarming-stats/?sh=36ed09da6b61

IBM — IBM Security X-Force Threat Intelligence Index 2023
https://www.ibm.com/reports/threat-intelligence

SonicWall — 2023 SonicWall Cyber Threat Report
https://www.sonicwall.com/2023-cyber-threat-report/

WWMT TV — West Michigan doctor's office hacked, doctors held for ransom
https://wwmt.com/news/local/west-michigan-doctors-office-hacked-doctors-held-for-ransom

PR Newswire — Nearly 70 Percent of SMBs Experience Cyber Attacks, Half Do Not Know How to Protect Their Companies
https://www.prnewswire.com/news-releases/nearly-70-percent-of-smbs-experience-cyber-attacks-half-do-not-know-how-to-protect-their-companies-300749965.html

ISACA Journal — Consumers Stopped Doing Business W/a Company Known to Have Compromised Cybersecurity
https://www.isaca.org/about-us/newsroom/press-releases/2022/1-in-3-consumers-stopped-doing-business-with-a-company-known-to-have-compromised-cybersecurity

SOPHOS — Sophos 2023 Threat Report
https://www.sophos.com/en-us/report/threat-report