SolCyber

20 years of MSSPs, what's broken and what SMEs need today.

SolCyber

It's been 20 years since Symantec acquired the startup MSSP Riptech, hailing the start of MSSPs everywhere. Have they been able to keep up with the rapid changes in threats and business needs for SMEs?

It should come as no surprise that cyberattacks and internet crime are on the rise. In March of this year, the FBI released its Internet Crime Complaint Center (IC3) report on cybercrime in 2020, which stated that there were almost 800,000 complaints of suspected internet crime in 2020, roughly 300,000 more than in 2019. These attacks resulted in a loss of more than $4 billion.

2020 800,000 ATTACKS $4 BILLION IN LOSSES

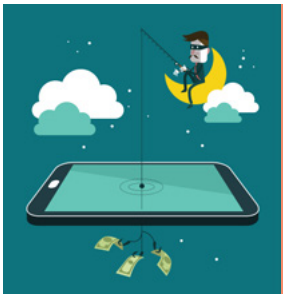
While cyberattacks, and ransomware attacks specifically, were once primarily aimed at large corporations and government agencies, attackers are now using the same advanced techniques on businesses large and small. What's more, they can attack at anytime, so not only are small businesses at risk, but they're at risk every hour of every day.

Unfortunately, these attacks are becoming increasingly profitable for attackers—and equally devastating for businesses. A 2021 report from the Identity Theft Resource Center reported that the recovery times for small businesses hit with cyber-attacks was significantly slow. Roughly 42% of businesses claimed recovery took 1 to 2 years, 28 percent said it took 3 to 5 years, and 7 percent weren't able to fully recover.

Evolved hackers and the changing threat landscape

As cybercrime becomes more profitable, it's attracting more talent, including state-sponsored and well-funded criminal enterprises. These new players are advancing the hacker industry's capabilities. Ransomware, for instance, isn't only being used to lock up a company's data but to exploit it in what's known as double-extortion ransomware attacks. This attack holds data hostage, whether it's intellectual property, sensitive employee or customer data, or data that could lead to reputational consequences if leaked.

Malicious actors are also opportunists — they have automated scripts that launch thousands of attacks on an ongoing basis. With spam lists and info from data breaches, these attacks hit all kinds of organizations 24/7, including nights, weekends, and holidays.



In fact, there's evidence showing that attacks launched over holiday weekends are more lucrative, because they tend to go undetected for several days.

Finally, the attack landscape is more expansive than ever. Most companies have invested in digitization heavily, especially since COVID — making their data more accessible and employees more susceptible to bad actors. Attackers can use third-party tools or purchase existing hacker tools to enter an environment, move through it, and find a company's most valuable data.

The pandemic has only exacerbated this risk as company computers are being used on home networks and personal devices are used to log into a company's network. IT and security teams can't monitor devices and patch software as easily as before, when everyone was working on-site and they may not have invested in the tools or technology that provide an inventory of all the devices connecting to the organization. If security and anti-virus software, as well as common apps and tools on many devices, haven't been updated, they're leaving computers vulnerable and dangerous as they re-enter company networks.

The challenge for small and mid-sized enterprises (SMEs)

While this threat landscape poses a challenge for all businesses, SMEs are particularly vulnerable because they face the same risks and attacks as massive corporations but lack the in-house security expertise and budgets. Without the resources needed to take on automated attacks as well as targeted attacks levied by professional hackers and nation-states, they become sitting ducks.

SMEs are also likely to suffer the most if compromised by a cyber attack. Nearly 60% of small businesses who are hit with a cyberattack actually shut down after six months. The cost and impact is too burdensome on an SME.

Despite the lack of resources to properly secure their organization, SMEs are still beholden to compliance regulations and need to establish trust with customers in order to continue to win business and scale up. And nothing kills trust faster than a data breach.

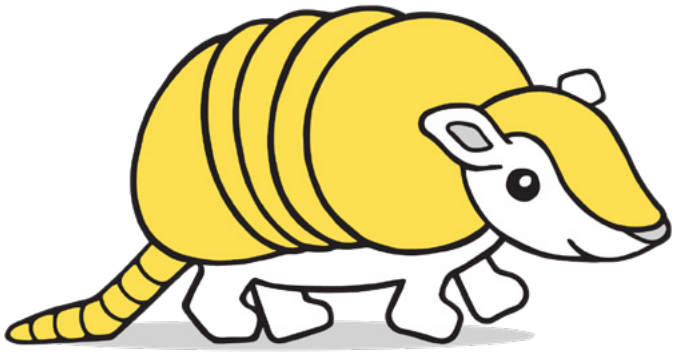
It is a necessity for many SMEs to turn to a managed security service provider (MSSP) to outsource their security efforts. Unfortunately, many MSSPs are ill-equipped to help SMEs because they haven't adapted to the aforementioned changes to the threat landscape and fail to offer a modern approach to security.

Others are accustomed to working with large organizations with robust in-house security teams that take over where the MSSP leaves off. And others have pricing and licensing structures so complicated and expensive that SMEs can't afford the service tiers that will truly keep them protected.

SMEs need an MSSP that can handle the entirety of their security efforts, reduce the operational burden and ensure the whole journey towards cyber resilience is fast, effective and uncomplicated.

In order to better serve today's SMEs, modern MSSPs should provide the following.

- **True cyber resiliency:** Protection shouldn't be partial or piecemeal. MSSPs should provide the tools, expertise, and 24/7 coverage that significantly reduces risk and improves your security posture.
- **A bundled and effective tech stack:** Customers should receive security tool recommendations from their MSSP rather than needing to weed through the noise themselves.
- **Simple, easy-to-understand pricing:** Having a clear, easy-to-understand pricing model can help make the case for working with an MSSP and ease the burden of forecasting budgets for quarters and years to come.
- **Fast implementations for an immediate impact:** Attacks are happening every day, so if a company is exposed, they need protection that kicks in immediately, not in several years.



01.

BASIC COVERAGE OFTEN DOESN'T COVER YOUR BASES

Anytime you purchase a service, you have expectations that it'll deliver your desired outcome. When you take your dirty clothes to the dry cleaner, you expect your clothes to come back clean. If the dry cleaners ask you, "How clean do you want your clothes? We have basic cleaning which makes your clothes 60% clean or advanced which gives you 80%." You'd think the place is crazy and go find a real dry cleaner.

The same goes for MSSPs. In today's world where the same advanced attacks are hitting businesses large and small, there is only one desired outcome.

An MSSP should provide you with true cyber resiliency — the ability for your business to continue if even one or some of your systems are compromised.

The modern MSSP needs to shift from offering piecemeal or tiered monitoring services to full security coverage. This should include:

24x7 coverage: Hackers aren't taking nights, weekends and holidays off, so security coverage shouldn't either. Attacks happen 24/7 meaning MSSPs should be monitoring and actively responding to threats 24/7. Otherwise, businesses are left vulnerable at key moments, allowing malicious actors to enter and move through the environment undetected.

A proactive and dedicated team: SMBs need more than automated services. They need a proactive response team who will work and respond in time as an extension of the company, actively hunting known malware and malicious behaviors, shutting down systems at the sign of an attack, and pushing perpetrators out as soon as they're detected. These experts should also be true partners from the onset, assessing the SMB's security posture and offering guidance and solutions on any gaps that may exist.

Modern cybersecurity across the kill chain: A modern MSSP should provide cybersecurity support and services that go beyond just prevention: providing tools, systems, controls, and processes that impact an attack through the entire kill chain — the steps that make up an attack from attempt to compromise to exfiltration.

A variety of controls and response capabilities: Too many MSSPs focus solely on detection, alerting you when a potential issue is found and leaving you to take care of the rest. But the modern MSSP will go beyond detection, hardening your systems and configurations, implementing prevention and response capabilities, and training your employees to better detect and respond to threats and attacks.

A full tech stack: The modern MSSP should come to SMEs with a full tech stack that includes tools that provide coverage across the threat vectors you're likely to face in the wild. This includes email, endpoint and active directory and decreases the likelihood that an attack goes undetected. The team should also have deep experience using these tools and possess capabilities in prevention, detection and response.

A flexible approach to technology: Though modern MSSPs should come to the table with tech stack recommendations, it's also important to allow SMEs to finish any existing contracts or sub out tools in the tech stack with what's in place — unless the tools will hinder the outcome, at which point, the MSSP should call it out and explain why.

Don't rely on AI

AI and automation are hot new buzzwords in security, but AI alone won't keep a business safe. Threats are driven by humans and the security response should be too. Many AI tools cannot yet be proactive or react to new threats, so relying too heavily on these tools can be detrimental.

The modern MSSP needs to ensure the customer becomes cyber resilient and provide all the necessary components to do so from expertise to the security tools themselves.

02.

TECH STACK CONFUSION LEADS TO RISK

If you provide detergent to your dry cleaners and the clothes don't come out clean, who's fault is it? You expect the dry cleaner to choose the best cleaning products for the job. The same is true for an MSSP.

There are more than 3,500 cybersecurity vendors to choose from when it comes to the tools an SME may be in the market for.

However, many MSSPs today put the onus on small businesses to determine which tools—and how many—they need. They will then take over the tech stack and monitor the chosen tools. This is extremely problematic for SMEs for a number of reasons.

Choosing tools requires in-depth cybersecurity knowledge

Selecting the appropriate tools for a tech stack requires an incredible familiarity with the kill chain. It's vital to understand where a company is most vulnerable and where protection is needed. But those who haven't been living and breathing cybersecurity for the last decade probably aren't confident in making those calls.

The right MSSPs employ security experts who are equipped to make recommendations on the types of tools needed to keep a business protected and should be able to pass off that expertise to you in the form of recommendations and guidance.

Building a tech stack is time-consuming

Even if you've identified the types of tools you need, such as endpoint detection and email protection, you'll still need to find vendors who offer those tools. The entire process of weeding through them and finding the right fit can take years, especially if you're not familiar with said tools or are responsible for more than just security.

Business owners and executives don't have the time and you want to minimize how much time your organization is exposed to risk.

Find an MSSP who can bring their own set of tools in order to speed up time to implementation and protection.

Many SMEs can't build a comprehensive security platform

When MSSPs ask their customers to build their own tech stacks, companies run the risk of building a bloated and expensive tech stack and may have gaps in coverage due to a lack of understanding or ability to navigate the FUD within the cybersecurity market.

Beyond knowing where a business needs protection, it's also important to know how many tools are needed, where they overlap, how they work together, and how they integrate within your environment.

But without an in-depth knowledge of how security tools work together, making these calls can be a challenge for business owners — the expertise needs to be found elsewhere.

An MSSP may lack experience in the chosen tools

If there's a disconnect between an MSSP and the SMEs existing tools, SMEs are forced to go back to the drawing board to either find new tools or find a new MSSP partner. Whatever the outcome, the organization is left unsecured until the issue is resolved. This is extremely important and needs to be part of the conversation as you conduct your due diligence with any MSSP.

MSSPs should come to the table with a tech stack not only because they are more familiar with the best tools, but because they can maximize the capabilities of said tools.

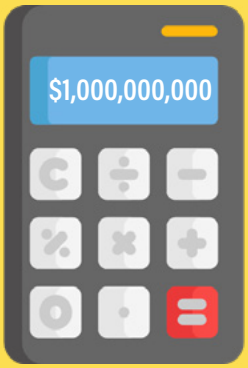
Building a tech stack is a huge responsibility and burden. For SMEs, building an in-house cybersecurity team is a non-starter and experience in the field is needed to know what kinds or tools are needed.

Unlike today's MSSPs that require customers to come to the table with a tech stack, MSSPs of the future should come to customers with a prescribed tech stack that works together to ensure the business is fully protected. It should be up to the MSSP to integrate the technologies based on industry best practices and a business's specific risks.

Only when your MSSP is responsible for delivering cyber resiliency and not just alerting you, are you truly managing your cyber risk.

03.

MORE DOLLARS MEANS MORE PROTECTION?



There are a number of Fortune 100 companies spending $1B each year on cybersecurity. Needless to say, SMEs don't have those kinds of budgets. But that doesn't mean they don't deserve or can't have similar coverage. Cybersecurity is no longer a "nice-to-have" — it's a necessity.

But too many MSSPs are still treating it as a service reserved for those who can pay.

Tiered pricing leaves SMEs vulnerable

Most MSSPs offer tiered pricing with higher price tags for more protection. Protection today shouldn't be dependent on what a business is willing to pay. Pricing should scale with the number of users — not the level of protection. Otherwise, how certain are you that your MSSP is really looking out for your protection or your wallet?

What exactly are you paying for?

When looking for a security partner, executives and business owners need to decide if they want to partner with an MSP, MSSP or EDR, XDR or MDR solution provider. What are their differences? What outcomes do they provide? You then need to choose a package level, which may or may not specify what tools are included and how those tools translate to overall protection.

This is just one more decision business owners need to make in a field where they don't have a deep background.

Customers shouldn't be tasked with choosing their level of coverage. An MSSP should provide enough coverage to keep a customer safe at any service level.

Complex billing structures can overwhelm customers

When businesses set up individual contracts with each security vendor then negotiate a separate contract with an MSSP, managing security costs and contracts becomes incredibly complex. Even if an MSSP handles all vendor contracts and pricing, their own pricing may not be straightforward.

For example, an MSSP might charge log collection fees based on storage volume,

endpoint detection management based on the number of devices, and email protection management based on the number of users. When your responsibility is to clearly communicate expectations, costs, and benefits of an MSSP, this unnecessarily complicated pricing structure only makes things more difficult.

Calculating security costs is complex

With so many contracts and different pricing structures, it can be difficult for businesses to calculate the total cost of their security services. This makes budgeting difficult and further complicates the decision on how much coverage a business should and will pay for. MSSPs can run into the same issue — with a complicated pricing structure, SMEs will find it more difficult to set expectations for pricing 1, 3, and 5 years down the line, especially as they expect to grow and scale.

But with a simplified pricing structure that includes services and the technology stack, businesses can get a clear picture of what their security efforts cost and then make more informed decisions about coverage in the future.

SMEs need to streamline their security efforts by outsourcing everything to a single partner.

Modern MSSPs need to meet that need by handling vendor management (and contracts), modernizing their pricing structure to a simple per-user fee.

This simplifies things for customers on the administrative side and allows them to better understand their coverage.

04.

TWO YEARS IS TOO LONG WHEN IT COMES TO CYBER RESILIENCE

Depending on where an SME stands today, becoming cyber resilient could take years. The process of conducting an internal audit, implementing new technologies, improving existing controls, and training or hiring staff could easily take two years or more regardless of whether the efforts are handled in-house or through an MSSP. During that time, your company is vulnerable to attack and likely to be hit. Modern MSSPs need to drastically shorten the time to resiliency in order to be an effective partner.

Leap forward with foundational coverage

It's true that audits are valuable and that a company's security strategy should be specific to their industry and the risks they're facing. However, there are a few tools and techniques, like endpoint detection and response and phishing training, that every company needs. These basic technologies can be implemented by an MSSP with confidence on day one to significantly improve your security posture. This means that rather than waiting two years to realize cyber resiliency, an SME is immediately protected from a majority of threats.

From there, an MSSP can conduct a more thorough audit, add-on defenses that are unique to your business and further educate staff on security best practices. But you'll already have the foundational coverage you need to be resilient against an attack.

A prepared MSSP means a prepared SME

While security solutions should be customized to the SME, an MSSP's approach to working with SMEs should be standardized. By building a standardized process for working with SMEs that includes a well-defined onboarding schedule, a foundational coverage tech stack and a consistent approach to audits and training, MSSPs can make faster work of constructing reliable defenses.

By building a standardized process for working with SMEs, MSSPs can make faster work of constructing reliable defenses.

The modern MSSP

As the world evolves and vendors become more customer-centric, customer expectations change and SMEs should be asking for more from their MSSPs. Today's SMEs need streamlined and comprehensive services from their security partner and many MSSPs are failing to provide that.

The modern MSSP should provide a foundational capability that enables a customer to be cyber resilient, including a minimum effective dose tech stack that can be implemented in weeks and not months. All this should come in a package that's easy to understand and maintain as your company grows.

Why SolCyber?

SolCyber is a modern MSSP. We offer amazing security, managed by approachable humans at an incredible value. When you hand off your security efforts to SolCyber, you can rest assured you're protected. Our security is comprehensive, proactive and built to allow SMEs to gain the same coverage as Fortune 100 companies.

Learn more about the SolCyber difference and drop us a note to learn more about how we can help you protect your environment fast.