DivergeIT
IT's in our nature

The Business Leader's Guide to IT Security:

How to Choose the Right MSSP to Protect Your Growing Business

By DivergeIT

Key Takeaways

The threat landscape has fundamentally changed – and mid-sized companies are in the crosshairs. Cybercrime is now a $10.5 trillion global industry. Attackers no longer target companies because of who they are, they target them because of what they can get access to. If you hold customer data, process transactions, or do business with larger organizations, you are a target.

Business email compromise has overtaken ransomware as the leading threat. AI-powered phishing attacks generated $2.77 billion in U.S. losses in 2024 alone, and the attacks behind those numbers don't require breaking through your firewall. They require one person to trust one email. With AI, phishing emails are nearly indistinguishable from legitimate communication, making employee education around spotting phishing emails an insufficient prevention approach.

A cyberattack costs far more than most business leaders expect. The cost of a cybersecurity breach for a small to mid-sized company – including investigation, legal fees, and recovery – can easily exceed $100,000. Add compliance penalties, customer attrition, and the operational disruption of being down for days or weeks, and the true cost compounds quickly. 60% of small businesses that suffer an attack close within six months.

AI has introduced a new category of internal risk that most companies haven't begun to govern. Employees using AI tools inside your organization, often without your knowledge or a formal policy, represent a meaningful data exposure risk. Unsanctioned AI use can put your intellectual property, client data, and financial records into environments you don't control. Governance doesn't have to be complex, but it does have to exist.

Building comprehensive security internally is harder and more expensive than most companies realize. There are more than 4 million unfilled cybersecurity positions globally. A single senior security analyst commands $150,000–$250,000 in annual compensation. Running a true 24/7 Security Operations Center in-house costs a minimum of $2–3 million annually. For most SMBs, this is not financially viable or operationally practical.

When evaluating an MSSP, three filters eliminate most of the market quickly. Industry experience in your vertical, active security certifications (e.g., SOC 2), and current Microsoft or Google partner credentials will narrow a crowded field down to a small number of genuinely qualified candidates.

The right MSSP is a business partner, not a vendor. The relationship works when the provider understands your industry, communicates clearly during incidents, reports transparently on your security posture, and treats your risk as a mutual responsibility. Use the Evaluation Scorecard in Section 7 to compare providers systematically and always check references.

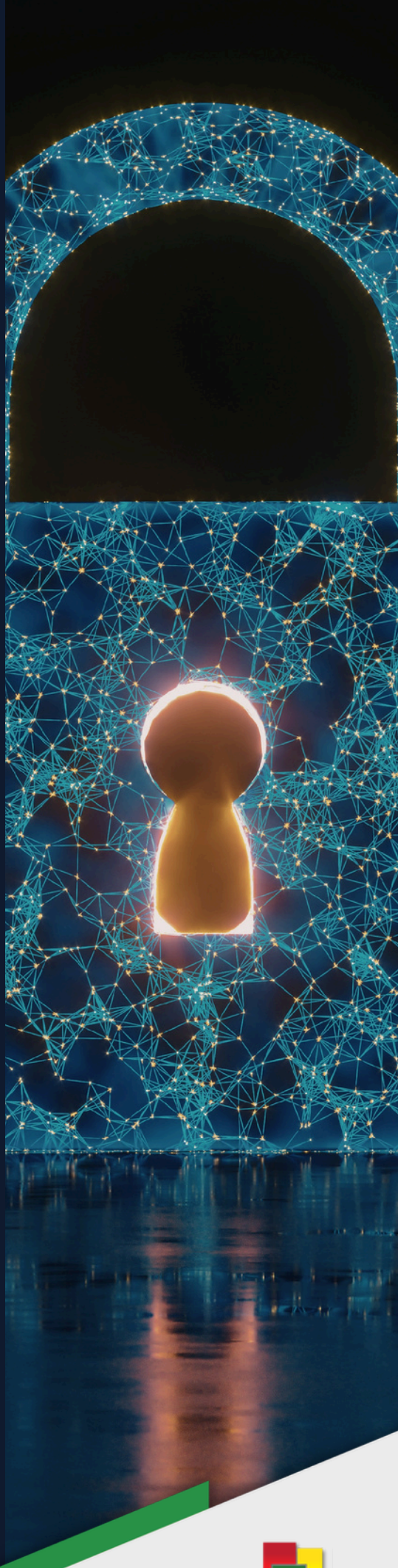


Table of Contents

Executive Summary

IT security used to be largely an IT problem. **Today, it's a business problem** – and for mid-sized companies between 50 and 500 employees, it may be the most consequential operational risk you face.

The threat landscape has shifted dramatically. **Attackers are no longer targeting only large enterprises** with the most data**.** They're systematically going after small and mid-sized companies because they're faster to breach, harder to defend, and less likely to detect an intrusion until after the damage is done.

Then there's AI. The same technology driving productivity gains inside your organization is being weaponized against it. AI is enabling attackers to craft more convincing phishing emails, automate large-scale intrusions, and identify vulnerabilities faster than most security teams can patch them. And while you may be focused on whether your employees are using AI responsibly, the greater immediate risk may be the threat actors using AI against them.

This guide is built for business leaders, not IT security specialists. It will help you understand the real nature and cost of today's cyber risk, assess whether your current approach is adequate, and make a smart, informed decision about whether to bring in outside help – and how to pick the right partner if you do.

2980 Columbia St, Torrance, CA 90503 USA

(866)216-3778

sales@divergeit.com

www.DivergeIT.com

The Threat Landscape Has Changed – **And So Has Your Risk**

WWW.DIVERGEIT.COM

DivergeIT
IT Solution Partner

The Threat Landscape Has Changed – **And So Has Your Risk**

Cybercrime has become a massive, well-organized, global industry. Projected to have cost businesses up to $10.5 trillion annually in 2025, it ranks as the third-largest economy in the world behind the U.S. and China.[1] And, the nature of the threat has evolved in ways that directly affect companies of your size.

Why would sophisticated hackers bother with you if you are a smaller company? Because attackers don't typically target you, they target opportunity. You're a pathway to larger companies you do business with. You process financial transactions. You hold employee and customer data with real market value. And with today's automation tools, attackers can run campaigns against thousands of companies simultaneously at almost no cost.

Phishing and Business Email Compromise (BEC) are now the leading attack vectors, and they're getting harder to spot.

While ransomware still makes headlines, business email compromise has surpassed it as a primary driver of financial loss, generating **$2.77 billion in reported U.S. losses in 2024 alone**, according to the FBI's Internet Crime Complaint Center (IC3).[2] These attacks don't rely on technical exploits. They rely on getting someone inside your company to click a link, approve a wire transfer, or share credentials. The entry point is human, and that's by design.

What a Modern Attack Sequence Can Look Like:

A phishing email lands in your controller's inbox. It appears to come from your CEO. Same name and domain. The email asks for an urgent wire transfer to a new vendor. The email is grammatically perfect, references a real project, and even includes your CEO's typical sign-off language. Your controller approves it. The funds are gone. None of this required a hacker to break through your firewall. They never touched your network. They just needed one person to trust one email.

DivergeIT
IT Solution Partner

The Threat Landscape Has Changed – **And So Has Your Risk**

Ransomware Hasn't Gone Away; It Has Just Evolved.

Ransomware attacks remain a serious threat, but the playbook has changed. Attackers now routinely exfiltrate your data before encrypting it, giving them double leverage: pay the ransom, or they'll publish your sensitive customer and employee data publicly. If you're in any regulated industry — healthcare, financial services, legal — that threat carries compliance consequences on top of operational ones.

Healthcare

HIPAA breach notification required within 60 days — plus potential fines up to $1.9M per violation category annually.

HIPAA

Financial Services

SEC and FINRA mandate incident reporting and customer notification — non-compliance compounds the financial damage.

SEC **FINRA**

Legal

Client privilege exposure and potential bar liability — data exfiltration may constitute an ethical violation requiring disclosure.

ABA Rules

Sources:
[1] Cybersecurity Ventures / VikingCloud, Cybersecurity Statistics 2025
[2] FBI IC3 2024 Annual Report

What a Cyberattack **Costs Your Business**

WWW.DIVERGEIT.COM

DivergeIT
IT Solution Partner

What a Cyberattack **Costs Your Business**

Most business leaders significantly underestimate the full cost of a cybersecurity incident. A ransom demand, if one is made, is often the smallest line item. Here's what the full picture can look like for a mid-sized company:

Incident Response

Engaging a professional incidence response (IR) firm often runs $40,000–$50,000 just for the investigation, not including recovery costs.

Recovery Costs

Restoring systems, data, and operations adds another $20,000 or more depending on scope.

Legal Fees

Required from the moment an incident is declared to preserve privilege during the investigation.

Notification and Monitoring

Restoring systems, data, and operations adds another $20,000 or more depending on scope.

Total Incident cost

Research estimates the average SMB cybersecurity breach cost is between $120,000 and $1.24 million, depending on the nature of the incident.[3]

> ***"For businesses under 500 employees, the average breach cost reached $3.31 million in 2025."***
>
> Digacore / MSSP Market Analysis, 2026

DivergeIT
IT Solution Partner

What a Cyberattack **Costs Your Business**

Operational Disruption

This is often one of the most devastating and least-discussed costs. Consider:

- Your operations may be fully halted during the investigation period, sometimes for weeks.
- 60% of small businesses that suffer a significant cyberattack close within six months.[4]
- Recovery timelines of 2+ weeks dramatically increase the risk of permanent closure, particularly for businesses with tight margins or customer dependencies.

Compliance and Regulatory Consequences

California's consumer data laws, HIPAA in healthcare, PCI standards for payment processing, and SEC requirements for financial services all carry tangible financial penalties for data breaches, and some will actively pursue enforcement. Equally important is that if a breach reveals that your environment didn't meet the security standards your cyber insurance policy required when you filed your application, your claim may be denied entirely, leaving you to absorb all costs out of pocket.

Reputational and Customer Impact

- 43% of businesses lose existing customers following a cyberattack.[5]
- The trust implications extend to prospective clients as well, particularly in industries like professional services, healthcare, and financial services, where handling sensitive data is a core part of the relationship.

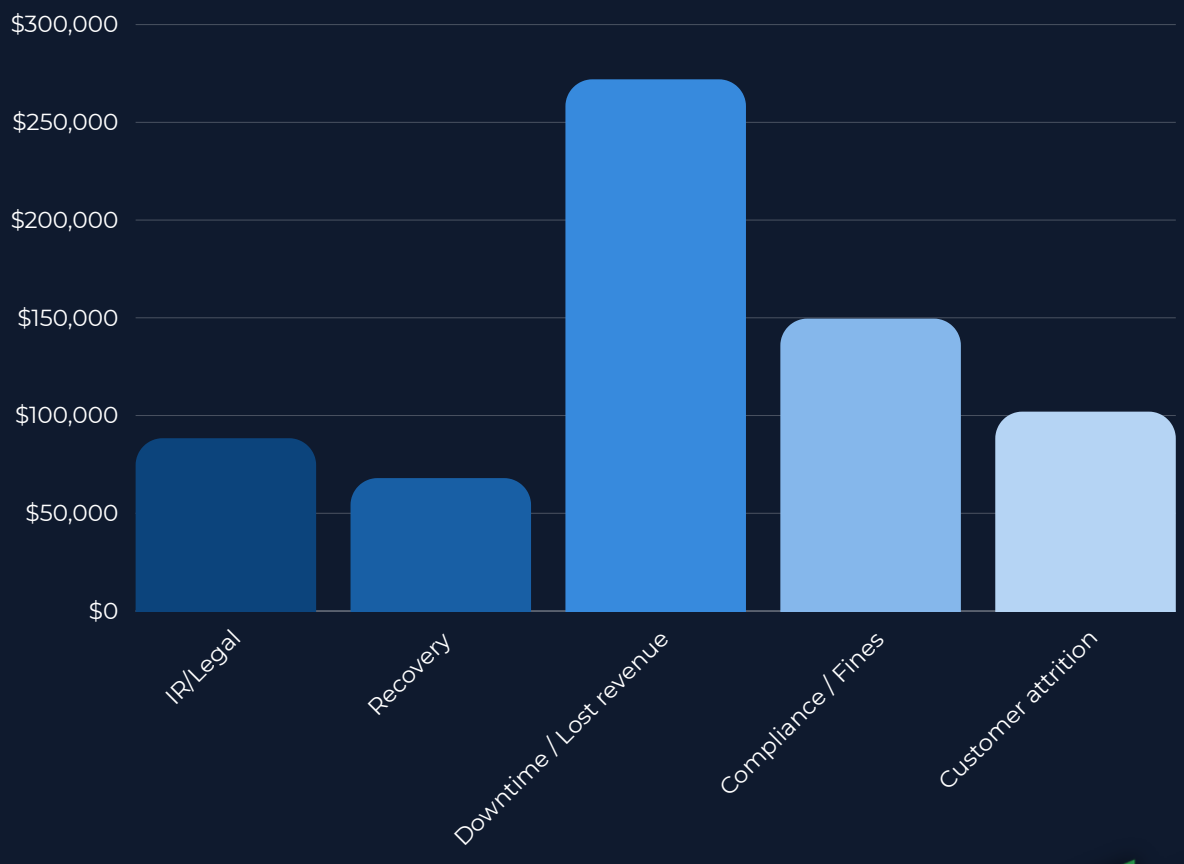
Sources:
[3] BD Emerson, Small Business Cybersecurity Statistics, 2025; DivergeIT client experience
[4]Qualysec / Total Assure, Small Business Cyber Attack Statistics, 2025
[5]Hiscox Cyber Readiness Report, 2024

DivergeIT
IT Solution Partner

What a Cyberattack **Costs Your Business**

Avg. SMB Breach Cost	Large Cost Driver	Cost Components
$680K	**Downtime**	5

IR / Legal (13%)
Recovery (10%)
Downtime / lost revenue (40%)
Compliance / fines (22%)
Customer attrition (15%)



Industry research. Actual costs vary by incident type, scope, and industry.

www.DivergeIT.com

3

Why SMBs Are at Greater Risk **Than They Realize**

WWW.DIVERGEIT.COM

DivergeIT
IT Solution Partner

Why SMBs Are at Greater Risk **Than They Realize**

Large enterprises have dedicated security teams, significant budgets, and mature programs. SMBs have simpler systems, fewer people, and fewer entry points, but they've grown complex enough that the attack surface is real. And they haven't yet built the infrastructure to defend it.

The Internal IT Team is Stretched Thin

At most companies in the 50–500 employee range, a single IT generalist, or a small team, is typically managing help desk support, infrastructure, software deployments, and security simultaneously. These are four distinct disciplines. Security alone is a full-time specialty that requires continuous training, 24/7 monitoring capability, and deep familiarity with an ever-changing threat landscape. Asking a generalist to cover all of this creates gaps.

54% of businesses admit their IT department lacks the experience to manage complex cyberattacks, and that was before AI-enabled attacks became mainstream.[6] Many mid-sized businesses are operating today without multi-factor authentication (MFA) fully deployed, without formal IT security policies documented and enforced, and without a tested incident response plan. MFA alone blocks an estimated 99% of account compromise attacks, yet implementation rates remain surprisingly low.[7] These aren't expensive capabilities. They're foundational ones. And their absence leaves the door open to threats.

No One Clearly Owns the Problem

In a 200-person company, who is responsible for IT security? It's a question that often yields a vague answer. The IT person manages the tools. The CFO controls the budget. The CEO may not realize the exposure. Without a clear owner and governance structure, security programs stagnate – not because no one cares, but because no one has been explicitly assigned accountability.

Sources:
[6]Sophos, cited in GetAstra Small Business Cyber Attack Statistics
[7]Keepnet Labs, Phishing Statistics 2025–2026

DivergeIT
IT Solution Partner

Why SMBs Are at Greater Risk **Than They Realize**

Cyber Insurance is Not a Safety Net

Many business leaders assume their cyber insurance policy will cover a breach. But insurers are increasingly denying claims when they can show the business was negligent in its security practices; practices the insurer likely required on the application. Insurance companies have begun suing claimants for fraudulent claims in cases of clear negligence. Coverage is valuable, but it is not a substitute for a sound security program.

What Insurers Actually Look For

Coverage can be denied — or clawed back — when these three realities collide.

What You Claimed on the Application

Insurers require you to certify security controls — MFA, patching, backups — at time of application. If those weren't in place at the time of breach, your claim is at risk.

What Negligence Looks like Post-Breach

Unpatched systems, no incident response plan, no security awareness training — insurers are increasingly using these gaps to deny claims or reduce payouts after an incident.

What Actually Protects You

A documented, enforced security program — not just a policy. Insurance is a backstop, not a strategy. The controls that satisfy your insurer are the same ones that prevent the breach.

The AI Factor: A New Layer of Risk Most Companies **Aren't Ready For**

WWW.DIVERGEIT.COM

DivergeIT
IT Solution Partner

The AI Factor: A New Layer of Risk Most Companies **Aren't Ready For**

AI has changed the cyber threat landscape in two distinct and compounding ways.

1. It has given attackers dramatically more powerful tools.
2. It has introduced a new category of internal risk most companies haven't begun to govern.

The external threat: AI-powered attacks are faster, cheaper, and harder to detect.

- AI-generated phishing emails now account for roughly 40–50% of all phishing activity, a figure that has surged from under 5% just months ago.[8]
- AI-powered phishing achieves a 54% click-through rate, compared to 12% for traditional phishing campaigns.[9] The gap in effectiveness is enormous.
- The FBI's 2025 IC3 report logged a 37% rise in AI-assisted Business Email Compromise incidents.[10] Attackers are using AI to clone executive voices, impersonate known contacts, and craft emails that reference real internal projects and relationships.
- Attack timelines are compressing. Security professionals have demonstrated full network compromise achieved in under 30 minutes using only AI-assisted tools.

The reason AI phishing is so much more effective is that it eliminates the issues that used to give the scams away: poor grammar, odd phrasing, and generic or poorly written content. AI-generated attacks are grammatically perfect, contextually relevant, and stylistically indistinguishable from legitimate email. Traditional filters aren't built to catch them.

DivergeIT
IT Solution Partner

The AI Factor: A New Layer of Risk Most Companies **Aren't Ready For**

The internal risk: Your own employees are using AI unsafely.

This may be the more immediate risk for manySMBs, and the one least on leaders' radar.

Employees are adopting AI tools rapidly, often without their employers' knowledge or guidance. When they do, they frequently input sensitive business data, such as contracts, financial records, HR information, and customer data, into AI platforms that may retain, use, or expose that data in ways your organization has not authorized or even considered.

Consider what happens when an employee pastes your company's confidential client agreements into a consumer AI tool to summarize them. Or when your finance team uses an AI assistant that has been granted broad access to your Microsoft 365 environment, giving it visibility into every file across the organization. Or when a single compromised account – obtained through a phishing attack – can now query your AI-connected systems to map your entire company structure, identify key personnel, locate financial data, and even draft follow-on attacks.

> ***"If you haven't set up your AI tools properly to isolate different kinds of data, you've essentially built a searchable guide for attackers to find exactly what they need."***
>
> — Robert Praul, Security Director, DivergeIT

DivergeIT
IT Solution Partner

The AI Factor: A New Layer of Risk Most Companies **Aren't Ready For**

AI governance is not optional, it's urgent

According to the World Economic Forum's Global Cybersecurity Outlook 2025, 66% of organizations expect AI to significantly impact cybersecurity, but only 37% have processes to assess AI tool security before deployment.[11] That gap is where the risk lives.

Getting ahead of this requires three things:

- Clear policies about which AI tools employees are permitted to use and how
- Technical controls that enforce those policies (such as Microsoft Purview for data loss prevention)
- Governance processes that require new AI tools to be reviewed before adoption.

None of this needs to be complex, but it needs to exist within your company.

AI-powered attacks by the numbers

40-50%

of all phishing emails are now AI-generated

Up from under 5% just months ago

54%

click-through rate on AI phishing vs. 12% traditional

4.5x more effective

37%

of orgs assess AI tool security before deployment

vs. 66% expecting AI to impact security

Sources:
[8]Hoxhunt Phishing Trends Report, 2025–2026
[9]The Network Installers, AI Cyber Threat Statistics, 2025
[10]FBI IC3 Annual Report, 2025; DeepStrike AI Cyber Attack Statistics
[11]World Economic Forum, Global Cybersecurity Outlook 2025

5 Can You Handle This on Your Own? **What It Really Takes**

WWW.DIVERGEIT.COM

DivergeIT
IT Solution Partner

Can You Handle This on Your Own? **What It Really Takes**

This is an honest question worth answering directly. Some companies can manage meaningful security improvements internally, particularly those with a dedicated IT resource or team that has the bandwidth and charter to prioritize it. But the bar is higher than most leaders realize, and the cost and complexity of doing it well is often underestimated.

The Talent Problem is Real

There are currently more than 4 million unfilled cybersecurity positions globally.[12] SMBs struggle to compete for specialized security talent against large enterprises and government contractors offering higher compensation and more defined career paths. A senior security analyst commands $150,000–$250,000+ in annual compensation, and that's one person covering one shift.[13] Running a 24/7 security operation internally requires multiple headcounts across shifts, plus management and tooling overhead.

The Tooling Cost is Significant

Building and operating a basic Security Operations Center (SOC) in-house, to cover endpoints, identity, network, email, and cloud, can carry an annual investment of $2–3 million when you factor in personnel, technology, and operations.[14] Achieving a formal security compliance framework (SOC 2, HIPAA, CMMC) typically requires an additional $60,000–$100,000 in consulting and platform costs, with no guarantee of outcomes until all the underlying controls are in place.

DivergeIT
IT Solution Partner

Can You Handle This on Your Own? **What It Really Takes**

The knowledge gap is accelerating

Even well-resourced IT teams are struggling to keep pace with AI-era security requirements. The discipline required to govern AI tools, monitor for novel attack patterns, and respond to fast-moving incidents requires continuous specialization. Security knowledge that was current 12 months ago may be materially incomplete today.

The practical reality for most mid-sized companies is that fully self-managed security is either financially out of reach, technically beyond current internal capability, or both. The question isn't whether you can do it yourself in theory, it's whether you can do it well enough, consistently enough, and at a cost that makes business sense compared to alternatives.

A useful framing is to think of it the way you'd think about building a specialized function like legal or financial audit. Most companies don't run their own law firm or internal auditing. They engage outside counsel when the expertise is needed and the stakes are real. Cybersecurity, at this level of complexity, warrants the same logic.

How Most Companies Handle It

- Legal risk? Engage outside counsel.
- Financial audit? Bring in a specialist firm.
- Cybersecurity? Still trying to figure it out internally.

The Question to Ask

Can you do it well enough, consistently enough, and at a cost that makes business sense — compared to the alternative?

Most mid-sized companies find the honest answer is no — not because they lack effort, but because the bar has moved.

Sources:
[1,2]ISC2 Cybersecurity Workforce Study, 2025
[13, 14]Vectra AI / Managed IT Security Services Market Analysis, 2025

6

When and Why to **Consider an MSSP**

WWW.DIVERGEIT.COM

DivergeIT
IT Solution Partner

When and Why to **Consider an MSSP**

A Managed Security Service Provider (MSSP) is a specialized third party that takes responsibility for monitoring, managing, and responding to cybersecurity threats across your environment. Unlike a general IT managed services provider (MSP) that focuses on keeping your IT systems running, an MSSP is specifically focused on keeping your systems secure, operating a dedicated Security Operations Center (SOC) staffed by security professionals, 24 hours a day, 7 days a week.

Signs it may be time to bring in outside help

- You don't have confidence in the completeness or currency of your security posture
- Your IT team manages security as just one of many responsibilities, not as a dedicated focus
- You've recently experienced a breach, phishing incident, or near-miss
- You're facing compliance requirements (HIPAA, PCI, SOC 2) without a clear roadmap
- Your employees are using AI tools and you don't have policies or controls governing how
- You're in a high-value industry, such as healthcare, financial services, or professional services
- You're growing through acquisition or expansion and inheriting new systems and risks
- You've had difficulty getting cyber insurance or have concerns about your ability to make a claim

DivergeIT
IT Solution Partner

When and Why to **Consider an MSSP**

What an MSSP should provide

A credible MSSP manages the full security stack, not just one piece of it.

- **Endpoint protection** — securing all devices connected to your network
- **Identity and access management** — controlling who has access to what, and monitoring for anomalies
- **Email security** — filtering, threat detection, and business email compromise protection
- **Network monitoring** — detecting unusual traffic patterns that signal intrusion
- **Cloud and application security** — protecting your Google, Microsoft 365, cloud storage, and connected SaaS tools
- **AI governance support** — policies, controls, and monitoring for how AI tools are used in your environment
- **24/7 SOC monitoring** — continuous watch, not just business-hours coverage
- **Incident response** — clear and coordinated ownership and fast action when something goes wrong
- **Compliance support** — helping you meet and document adherence to relevant regulatory frameworks

What an MSSP cannot replace

Working with an MSSP does not eliminate the need for you to implement and maintain the security controls they recommend. An MSSP is a powerful force multiplier, but they need a reasonably secure foundation to work from. Companies that resist implementing MFA, don't enforce policies, or continuously defer security decisions will see limited results regardless of the provider they choose.

DivergeIT
IT Solution Partner

When and Why to **Consider an MSSP**

Security Model Comparison

	Managing Internally **In-House IT Team**	Partnering with an MSSP **DivergeIT**
Cost	$2–3M+ annually for a functional SOC, plus tooling and overhead	Predictable monthly fee — fraction of the cost of internal build-out
Coverage	Business hours only — gaps on nights, weekends, and holidays	24/7/365 monitoring — attacks don't keep business hours
Expertise	One or two generalists covering security alongside other IT duties	Dedicated security specialists — threat hunters, analysts, engineers
Response	Reactive — incidents often discovered hours or days after the fact	Proactive detection and containment — mean time to respond in minutes
Compliance	Ad hoc — frameworks like SOC 2 or HIPAA require costly outside consulting	Built-in compliance support — SOC 2, HIPAA, CMMC mapped to your program

How to Evaluate and Choose the **Right MSSP**

WWW.DIVERGEIT.COM

DivergeIT
IT Solution Partner

How to Evaluate and **Choose the Right MSSP**

The MSSP market is crowded, and partner quality and capabilities vary significantly. Here is a practical framework for narrowing the options and making a sound decision. These three filters will narrow a large field down to a very small number of credible candidates.

1. Do they serve companies like yours?

Look for an MSSP with documented experience in your industry. Security requirements and threat profiles differ meaningfully across government, healthcare, financial services, legal, manufacturing, and professional services. A provider who doesn't understand your regulatory environment or how your business operates will miss context that matters.

2. Are they security-certified themselves?

This is a critical and often-overlooked filter. Ask whether the MSSP holds an active SOC 2 certification or equivalent security compliance framework. It's remarkable how few do. A provider who can't certify the security of their own environment is not positioned to secure yours.

3. Do they hold certifications with the major platforms in your environment?

If you operate in a Microsoft environment (as most SMBs do), the MSSP should hold active Microsoft partnership credentials. This ensures their team is trained and recognized on the platforms managing your data, identity, and communications.

DivergeIT
IT Solution Partner

How to Evaluate and **Choose the Right MSSP**

Once you get down to a smaller, high quality starting point, continue to evaluate on:

- **Scope of coverage:** Do they monitor across all five threat vectors (endpoints, identity, network, email, and cloud/AI)? A provider strong in one area but absent in others leaves gaps that attackers will find.
- **24/7 monitoring:** Threats don't operate on business hours. Confirm that SOC coverage is continuous, not "follow-the-sun" with handoffs, not on-call only, but actively staffed around the clock.
- **Response time SLAs:** Monitoring without fast response is inadequate. Ask specifically how long from detection to alert? How long from alert to active response? What is the escalation process? Get this information in writing.
- **Onshore vs. offshore teams:** Consider where the provider's security analysts are located. For regulated industries, there may be compliance implications. For all companies, availability and cultural/linguistic fluency in how they communicate during an incident matters.
- **Transparency and reporting:** You should receive regular reporting on what's being monitored, what's been detected, and how your security posture is trending. Ask to see a sample report. If they can't show you clear, readable reporting, that's a red flag.
- **Incident response ownership:** Ask directly about if a breach occurs, who owns the response process? What is the communication protocol? Will they engage on your behalf with your insurance carrier? Know this before you need it.
- **Referenceable clients:** Ask for references from companies similar to yours in size and industry. A strong MSSP will have them readily available.

DivergeIT
IT Solution Partner

How to Evaluate and **Choose the Right MSSP**

Red Flags to watch For

Some common issues to look out for include:

- No SOC 2 or equivalent compliance certification
- Vague or evasive answers about response time SLAs
- No demonstrated experience in your specific industry
- A "one-size-fits-all" service offering with no customization
- Offshore-only delivery without clear escalation to U.S.-based staff
- Lack of a certified Microsoft or Google partner credential (aligned to your environment)
- Unable to provide client references

Regarding Cost

Managed security services for SMBs typically range from $50 to $250 per user per month, depending on the scope of coverage and services included.[15] On a per-user basis, this is a fraction of what in-house coverage would cost, and it comes with 24/7 coverage, specialized expertise, and tooling your internal team wouldn't be able to replicate cost-effectively on its own. Compare this against the $120,000+ minimum cost estimate of a single incident, and the business case becomes clear.

Sources:
[15] Digacore, Managed Cybersecurity Services for SMBs, 2026

DivergeIT
IT Solution Partner

MSSP Evaluation **Scorecard**

You can use this scorecard to help you evaluate MSSP candidates. Rate each provider on a scale of 1–5 for each criterion. The providers with the highest total score across the categories that matter most to your business are likely your best candidates to engage with further. Beyond scoring well on this scorecard, you also want to assess for overall fit with the culture of your organization and teams.

SECTION A: Qualifications & Credentials

Evaluation Criterion	Notes	Score (1–5)
Active SOC 2 or equivalent certification	Ask to see the current certificate	_____
Microsoft / Google / other relevant platform partnership credentials	Verify at partner level, not just a reseller	_____
Industry-specific experience (your vertical)	Ask for specific client examples early	_____
Years in business (5+ preferred)	Longevity indicates stability and maturity	_____
Dedicated MSSP practice (vs. general MSP that "does security")	SOC-based model, own NOC / SOC	_____

SECTION B: Scope of Security Coverage

Evaluation Criterion	Notes	Score (1–5)
Endpoint detection and response (EDR)	All company devices covered	_____
Identity and access management (MFA, PAM)	Includes admin / privileged access controls	_____
Email security and BEC protection	AI-aware filtering, not legacy signature-only	_____
Network monitoring and threat detection	Active, not just logging	_____
Cloud and Microsoft 365 / Google Workspace security	Covers your primary productivity environment	_____
AI tool governance and data loss prevention (DLP)	Critical given current threat landscape	_____
Vulnerability management and patching	Proactive, not just reactive	_____

DivergeIT
IT Solution Partner

MSSP Evaluation **Scorecard**

SECTION C: Operations & Response

Evaluation Criterion	Notes	Score (1–5)
24/7/365 SOC monitoring	Staffed, not just automated alerting	_____
Documented response time SLAs	Get specific timeframes in writing	_____
U.S.-based security analysts available	Especially important for regulated industries	_____
Clear incident response ownership and process	Know exactly who does what when	_____
Business communication protocols during an incident	Do they communicate with leadership directly?	_____
Coordination with your cyber insurance carrier	Do they support the claims process?	_____

SECTION D: Compliance & Governance

Evaluation Criterion	Notes	Score (1–5)
Support for your specific compliance frameworks (HIPAA, PCI, SOC 2, CMMC)	Relevant to your industry requirements	_____
Documentation and audit trail support	Can they generate reports for auditors?	_____
AI governance framework and policy support	Increasingly essential	_____
Security awareness training for your employees	Should be included or available	_____

DivergeIT
IT Solution Partner

MSSP Evaluation **Scorecard**

SECTION E: Transparency & Partnership

Evaluation Criterion	Notes	Score (1–5)
Quality and clarity of regular reporting	Review a sample report	_____
Client portal or real-time visibility into security activity	You should be able to see what's happening	_____
Referenceable clients in similar industries	Ask for 2–3 and call them	_____
Responsiveness during the sales process	How they sell is how they serve	_____
Clarity on pricing and what's included vs. extra	No surprise fees for incident response	_____

Scoring Summary

Section	Max Score	Provider A	Provider B	Provider C
A: Qualifications & Credentials	25			
B: Scope of Coverage	35			
C: Operations & Response	30			
D: Compliance & Governance	20			
E: Transparency & Partnership	25			
TOTAL	**135**			

About **DivergeIT**

DivergeIT is a high-performance managed IT and security services provider with more than 20 years of experience supporting mid-sized companies across the United States. We partner with businesses in a range of industries including healthcare, entertainment, financial services, manufacturing, and professional services.

DivergeIT operates with a security-first posture across every client engagement. We are ranked in the top 1% of Microsoft® Partners in the United States and are SOC 2® certified by AICPA. Our five-layer, proactive security framework enables us to protect client environments against today's most prevalent threats, including business email compromise, ransomware, and emerging AI-driven attacks.

Ready to assess your current security posture?

Contact DivergeIT for a no-obligation security assessment.

Sales@divergeit.com | www.DivergeIT.com | 866-216-3778