The Cyber Provocateur
Exploring controversial themes in cybersecurity

The Cyber Shift in Finance: From Point Solutions to Unified Platforms.

How the right MSSP could elevate your security strategy.

Joseph E. Krull, Cybersecurity Industry Analyst, CISSP, IAM, CIPP

SEPTEMBER 2024

Sponsored by sel®

CONTENTS

3 Executive summary

3 MSSPs: Where did they come from?

4 MSSPs today: M&A activity and platform convergence

4 Risks and opportunities for financial services organizations

5 Leveraging MSSPs for optimal cybersecurity in finance

6 MSSP relationships: How to select the right partner

7 The MSSP relationship is a two-way street

8 Client case study

9 Conclusion

Executive summary

Managed security service providers (MSSPs)—some people love them, and others hate them. In this edition of *The Cyber Provocateur*, we look at current trends in the MSSP market and opportunities for initiating and improving relationships with MSSPs. We also dive into ways to de-risk critical components of managed security operations—including network and cloud—and offer key questions to determine whether an MSSP can provide the right services to meet the requirements of a financial services organization. And we present a case study of an organization that broke the code on how to effectively make an MSSP a core component of their cybersecurity strategy.

MSSPs: Where did they come from?

The concept of managed security did not evolve overnight. From the first basic offering in 1997, it's taken more than a quarter of a century to progress into today's current iteration. There were several initial challenges to overcome, most notably resistance by heavily regulated financial services organizations to offload any security services to a third party. MSSPs also needed to work hard to gain the trust of their clients, prove the value of their services, and define their pricing models.

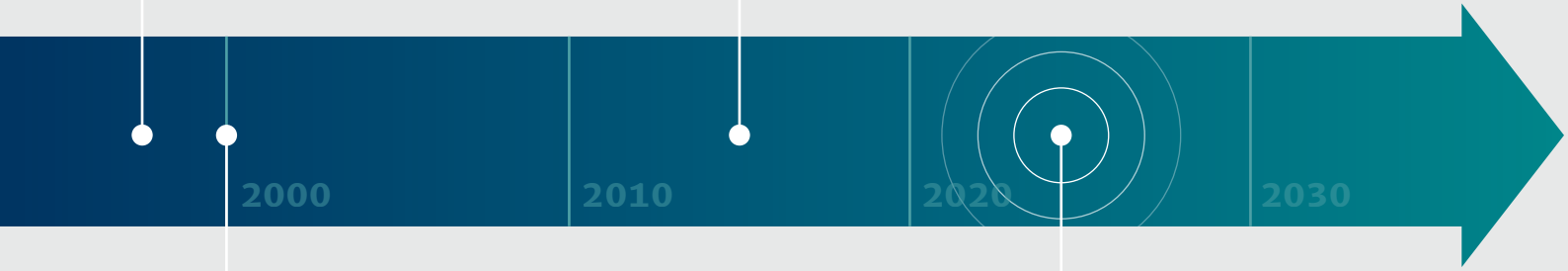
MSSP evolution

First generation (1997)

US West, a Regional Bell Operating Company, begins offering customers leased managed firewalls and, later, virtual private network services. Soon after, internet service providers offer various forms of supplemental security products and services.

Maturing market (2015–20)

By 2020, many enterprises and midsized companies begin to see the value in engaging MSSPs for some cybersecurity functions. Hundreds of independent MSSP companies are created. MSSPs offer the option to manage client security tools or provide their own.



Market adoption (2000)

Counterpane Internet Security Inc. is founded by renowned cryptographer Bruce Schneier. The company sells an Enterprise Protection Suite service, including security device management, network scanning, and consulting. They use the term "managed security monitoring service," and based on the Counterpane model, other companies enter the market.

Proven solution (now)

The annual global MSSP market now exceeds $80 billion, and the environment is robust with mergers and acquisitions. MSSPs go beyond managed security technologies to offer value-added services, including incident response, remediation, virtual chief information security officer, penetration testing, and threat hunting.

Source: Canalys: Cybersecurity Ecosystems Report, January 2024

MSSPs today: M&A activity and platform convergence

The MSSP market is closely mirroring elements of the broader cybersecurity market. The key theme is consolidation. Frenetic mergers and acquisitions continue in 2024 after a robust wave of both cyber services and product amalgamation in 2023. This consolidation stems from two primary motivators:

- **Market share:** MSSPs are rapidly growing their market share and client base through acquisition of competitors rather than slow and costly organic growth. Cybersecurity vendors, MSSPs, and private equity firms continue to look for distressed but valuable companies. Vendors look to add new features, capabilities, or customers.
- **Platform convergence:** MSSPs and cybersecurity vendors are quickly moving toward unified platforms as opposed to point solutions, whereby different cybersecurity tools and products can be managed from a single interface to counter tool sprawl and eliminate security and network management tools that no longer provide value.

As of May, more than 140 M&A deals related to the managed services/managed security services market have occurred in 2024. There were more than 330 M&A deals in 2023.

Source: CyberRisk Alliance and ChannelE2E

The 2024 MSSP market is growing even faster than predicted in 2023 as more organizations of all sizes resort to outsourcing key cybersecurity functions fueled by a shortage of cyber talent and cost-cutting measures. Managed detection and response (MDR) has proven to be extremely enticing for the SMB market, and services such as managed remediation and managed cyber technology are now considered to be credible outsourced services, even for larger enterprises.

Risks and opportunities for financial services organizations

Risks abound in financial services, and the increased sophistication and frequency of cyberattacks have elevated cybersecurity at all levels of the financial services industry. In fact, the International Monetary Fund's 2024 Global Financial Stability Report cited that extreme losses from cyber incidents are increasing, and such losses could potentially cause funding problems for targeted companies and even jeopardize their solvency. Engaging a security services partner can be part of a cybersecurity strategy to address cyberthreats.

65%

of financial services organizations were hit by ransomware in 2024[1]

$12B

in direct losses to financial firms in the past 2 decades from cyber incidents that affected the global financial sector[2]

$2.58M

in average costs for financial services organizations to recover from a ransomware attack in 2024[3]

[1] Puja Mahendru, "The State of Ransomware in Finance Services 2024," *Sophos News*, June 24, 2024.

[2] Spencer Feingold, Johnny Wood, "Global financial stability at risk due to cyberthreats, IMF warns. Here's what to know," World Economic Forum, May 15, 2024.

[3] Mahendru, "State of Ransomware 2024," *Sophos News*.

The current state of the MSSP market offers both risks and opportunities. The high rate of M&A activity could be viewed as a risk or an opportunity. If an existing MSSP is acquired, the served client could either see enhanced services from the larger organization (albeit at a potentially higher price) or a significant negative impact on the relationship if the acquiring company poorly integrates the acquired MSSP. In some recent instances, MSSPs involved in mergers have elected to stop serving some existing clients that are not in line with the acquirer's business strategy. This could negatively impact ongoing security operations and cause a mad scramble to find a new MSSP.

The move by MSSPs toward unified cybersecurity platforms is also a significant opportunity for financial services organizations. Platforms offer the ability to manage multiple security tools and feeds from a "single pane of glass." More advanced platforms add features such as process automation; event correlation; incident management; and increasingly, machine learning and artificial intelligence. Extended detection and response (XDR) is increasingly the underlying basis for these platforms, which receive feeds from beyond endpoints to include network devices, security information and event management (SIEM) components, cloud telemetry, and email security tools. XDR-based platforms can offer the ability to provide a more comprehensive picture of the technical state of cybersecurity, reduced need for human analysis, and rapid alerting of anomalies.

Leveraging MSSPs for optimal cybersecurity in finance

An MSSP relationship, if properly sourced and selected, can offer financial organizations of all sizes an alternative to managing an internal cybersecurity team or department. An MSSP can assume certain cyber functions, freeing up the internal team for more complex projects. There is inherent risk in maintaining an internal security team or department. The departure of one or a few key team members can negatively affect the overall cyber program, and the shortage of experienced cyber personnel in the marketplace can make backfill a lengthy (and expensive) proposition. An MSSP relationship can de-risk the potential for personnel gaps since an effective MSSP will maintain a bench of trained specialists supporting multiple clients.

From a pure dollars-and-cents perspective, engaging a good MSSP can reduce or eliminate tool licensing and annual maintenance fees. The MSSP will generally absorb or replace the licenses and most likely obtain significant discounts through volume licensing across their installed client base. Consolidated single invoicing from MSSPs for their clients can easily translate to predictable budgeting and reduced procurement workload via vendor consolidation.

In 2024, the average cybersecurity salary in the U.S. is $122,079 per year. Entry-level positions start at $95,290 per year, while most experienced workers make up to $169,576.

Source: Talent.com based on data collected from 10,000 non-executive cyber employees

There are also some implied benefits that stem from an MSSP relationship. An MSSP will have visibility into threats and effective cyber strategies across a range of clients and industries. They can advise organizations on methods to protect sensitive client data, considering a constantly changing threat landscape. Avoiding fines and sanctions stemming from a data breach, thanks to enhanced cyber intelligence and early detection from an MSSP, can ostensibly be the biggest potential return on investment for a financial services organization. Additionally, with today's proliferation of ransomware attacks that can render infrastructure and data unavailable, an MSSP can quickly surge resources for an "all hands on deck" response when warranted.

A back-of-the-napkin analysis based on the potential benefits detailed above will almost always favor a buy-versus-build strategy, but before rushing out to engage an MSSP, let's look at the other side of the coin.

MSSP relationships: How to select the right partner

Some people just hate MSSPs and are not shy about expressing their opinions. They may have had a bad experience or heard from their industry contacts of instances when a managed security provider dropped the ball or could not meet their expectations. However, in most cases, it's likely that the wrong questions were raised during the MSSP selection process. To properly assess an MSSP and de-risk a potential relationship, the following questions should be asked at the earliest opportunity and prior to a contract:

Topic	Questions
Relevant experience	• Does your company have direct experience working with heavily regulated financial services organizations? How many? • Provide specific examples of successes delivering cybersecurity value to these clients.
Business outcomes	• Can you attribute your services to positive business outcomes for your clients? Examples include direct cost savings, increased efficiencies in your clients' operations, detection and blocking of attacks that the client would not have likely identified, and demonstrable improvement in your clients' findings from auditors and regulators.
Financial considerations	• How is your company funded, and is your strategy based on growth, acquisition, or being acquired? • What is the current financial strength of your company?
People	• How many cyber specialists in your company are directly devoted to cyber operations as opposed to administrative of internal management functions? • How do you recruit new talent and provide ongoing training for cyber operations specialists? • How often do you perform background checks on your employees and contractors?
Service delivery	• Do you assign a dedicated point of contact and backup contact for operational communications with your individual clients, or is this a pooled function? • Can your company provide a true 24/7 service? • Do you operate an automated ticketing handling system that allows your clients to raise issues and risks until full resolution?
Technologies	• Have you developed or intend to soon develop a service platform that consolidates feeds and telemetry from a wide range of cybersecurity products and tools into a single portal available to your clients? • Is your focus primarily on managed endpoints or a broader range of feeds and sensors? • What is your approach to network monitoring and your capabilities to detect anomalies or threats to cloud environments?
Costs	• What services are included in your basic pricing scheme and what are supplemental based on additional charges? • What is your process for obtaining client approval for supplemental charges? • How does a client receive an invoice and report potential discrepancies?

The MSSP relationship is a two-way street

All too often, organizations pigeonhole MSSPs into traditional vendor relationship programs. This can dangerously result in the MSSP being viewed as just another vendor as opposed to an organization that can be entrusted to provide a viable line of defense against cyber-born threats. An MSSP should be selected and constantly evaluated as a partner as opposed to a vendor. At the same time, organizations considering an MSSP relationship must understand that responsibility for cyber success can't be completely turned over to an MSSP—the organization needs to be actively and constantly engaged and appoint an executive to oversee the relationship and be a point of contact for day-to-day operations.

Financial services organizations should embrace the concept of a security management partner and select an MSSP that can go well beyond generic cybersecurity services provided by the majority of MSSPs. The partner model treats the cybersecurity services provider as a logical extension to the organization's IT and cybersecurity teams and encourages a complete and transparent two-way communications channel.

Financial services organizations should select an MSSP that can go well beyond generic cybersecurity services provided by the majority of MSSPs.

CLIENT CASE STUDY

Shielding a regional bank from a cyberattack.

SEI Sphere® dives deep to investigate and defend against the 3CX third-party compromise.

CLIENT PROFILE

- Award-winning, locally owned bank with six locations
- Over $800 million in assets
- More than 130 employees; a small IT staff
- Partners with SEI Sphere for cybersecurity and cloud services

A THOROUGH APPROACH

SEI Sphere's security team confirmed malicious activity from the 3CXDesktopApp using shared intelligence from their endpoint security tool and other open-source intelligence. Their unified platform allowed them to:

- Immediately run command and control (C2) indicators and hash values (numerical values that uniquely identify data) through their custom-built security information and event management (SIEM) tool to determine if any were observed in their clients' environments.
- Run recommended threat-hunting queries in event search to validate the full extent of this application in client environments.
- Discover additional C2 indicators not originally reported by their endpoint security tool from their community of open-source intelligence channels and add these to their SIEM and proxy blocks.

A STRONG POSITION

By adding these indicators to their SIEM, SEI Sphere could see and block any future hits to the associated C2 domains via endpoint detection and observation of all proxy logs. As businesses grow, so does reliance on outside providers, and so too does vulnerability to third-party attacks like this one. In a time when crafted attacks toward handpicked organizations are becoming the norm, it's important to have a cybersecurity provider who performs comprehensive, timely work with every inquiry.

"When we looked to expand our regional footprint, we found that our existing IT infrastructure was an impediment. In partnership with our team, (our MSSP) SEI (Sphere) re-architected our network and security designs with new technology solutions, allowing us to pursue our growth strategy with confidence."

— Senior Vice President, regional bank

Conclusion

- It's taken more than 25 years and a lot of lessons learned, but managed security service providers are now a proven solution for financial organizations.
- The MSSP market is flavored by a high number of mergers and acquisitions as MSSPs rapidly increase their market share via rivals as opposed to slow organic growth. Financial organizations should consider the potential impact of an acquisition on their MSSP relationship.
- The move by MSSPs toward unified platforms as opposed to a collection of point solutions offers enhanced monitoring, greater visibility, rapid correlation, and incident identification via a "single pane of glass" approach. Coupled with XDR architecture, machine learning, and AI, platforms can reduce the need for expensive human analysis.
- There is a clear value proposition for engaging an MSSP, but organizations need to ask critical qualification questions during the selection process so that expectations are clearly defined.
- All too often, organizations approach an MSSP as a vendor as opposed to a trusted security partner. To get the best results from an MSSP relationship, financial organizations must treat the cybersecurity services provider as a logical extension to the organization's IT and cybersecurity teams and encourage a complete and transparent two-way communications channel.

About the author

Joseph Krull, Cybersecurity Industry Analyst (CISSP, IAM, CIPP), has nearly 50 years of experience in information and cybersecurity, serving both government and commercial organizations. He has worked in 115 countries and has provided cyber consulting to large enterprises on four continents. Most recently, he was a senior cyber industry analyst for Aite-Novarica Group. Previously, he was Principal Director at Accenture Security, where he focused on helping large companies formulate their cybersecurity strategies. Prior to Accenture, Mr. Krull held leadership roles with a Big Four, a senior role at an application security vendor, and led his own company focused on reducing security risk to telecommunications companies. Prior to consulting, Mr. Krull was the chief information security officer at three Global 1000 companies, and he served as a technical officer and military attaché at seven U.S. Embassies.

About SEI®

SEI delivers technology and investment solutions that connect the financial services industry. With capabilities across investment processing, operations, and asset management, SEI works with corporations, financial institutions and professionals, and ultra-high-net-worth families to help drive growth, make confident decisions, and protect futures. As of June 30, 2024, SEI manages, advises, or administers approximately $1.5 trillion in assets.

About SEI Sphere®

As an MSSP, SEI Sphere provides comprehensive business solutions that deliver cybersecurity, network operations, and cloud services. Supporting and securing the evolving IT needs of today's regulated and fast-growing businesses, SEI Sphere helps them build and maintain a secure technology foundation. For more than 55 years, SEI has provided technology platforms and solutions that enable clients to focus on strategic initiatives and drive future growth.