Aite PARTNER. ADVISOR. CATALYST.

IMPACT BRIEF

MAY 2021

Joseph Krull, CISSP, IAM, CISA, CRISC, CIPP
+1.210.421.8233
jkrull@aitegroup.com

Introducing the Security Management Partner: A Specialist for Financial Services Security

General practitioners can provide a basic level of care for the human body, but specialists are normally called in to diagnose and treat more complex issues based on their advanced training, unique talent, and expertise. Managed security services providers (MSSPs) frequently operate like general practitioners and provide a range of generic cyber services to multiple industries. But this one-size-fits-all approach to cybersecurity often misdiagnoses issues and risks specific to the financial services industry. Enter the security management partner—a new approach to cybersecurity based on deep expertise in the types of threats facing financial services organizations. The security management partner is ideally suited to financial services organizations that may not have sufficient cyber expertise on staff, but it can also be enticing for firms that want to augment existing cyber capabilities. This report provides a high-level overview of the managed service provider (MSP) and MSSP market and provides two case studies to show how a specialized approach for financial services clients offers unique advantages for managing cyber risk.

INTRODUCTION

Financial services organizations have a lot of options to outsource cybersecurity services. There are hundreds of MSPs, MSSPs, and technology solution providers that provide a range of services, from basic network monitoring and firewall management to a full set of capabilities, including sophisticated threat hunting and incident management. Although there are many options when selecting a cybersecurity service provider, financial services organizations have specific needs that cannot be readily met by service providers that do not have specific knowledge and experience with financial services operational and regulatory requirements. This report details the cybersecurity market and introduces the concept of a security partner approach for financial services.

METHODOLOGY

This Impact Brief is based on briefings, discussions, and participation in virtual events with service providers, technologists, cybersecurity practitioners, and IT professionals utilizing outsourced security services. Activities took place from July 2020 through March 2021.

THE MARKET

The market for cybersecurity services has become particularly crowded over the last four years as more and more MSPs and MSSPs seek to offload cybersecurity functions from organizations that cannot build and operate these services themselves. Today, there are more than 500 MSPs and MSSPs vying for cybersecurity business with a dizzying array of service offerings and technologies. This makes evaluation and comparison of the various services and the resultant pricing particularly challenging for buyers of cybersecurity services. It is very uncommon for MSPs or MSSPs to provide cybersecurity services specifically tailored to the needs of financial services organizations.

During our discussions with service providers and IT professionals from July 2020 through March 2021, Aite Group examined the current state of the cybersecurity services market and identified several trends that are impacting the market and reflect the needs of small and midsize financial services organizations (Table A).

Table A: The Market

Market trends	Implications
The MSP/MSSP market is highly fragmented, with hundreds of MSPs and MSSPs offering a wide range of cybersecurity capabilities.	Buyers of cybersecurity services can be challenged to properly evaluate and compare the services of multiple providers due to the sheer volume and similar service descriptions of providers.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Market trends	Implications
The MSP/MSSP and related technology solution provider markets are a hotbed of mergers and acquisitions activity, with more than 530 publicly reported deals in 2020 and more than 150 in the first quarter of 2021 according to industry group ChannelE2E.	Significant risk exists for the supported organization should an incumbent MSP, MSSP, or technology solution provider be acquired during the period of a service contract. An acquisition can result in changes in technologies, pricing, and service coverage at the point of contract renewal.
MSPs/MSSPs are trying hard to differentiate their services to move beyond monitoring and alerting, but have limited capabilities to provide customized services for specific clients.	Customization for individual industries, including financial services, is rare. Not all organizations have the same cybersecurity needs.
MSSPs are quite adept at learning and deploying cyber products and technologies but are less adept at tying their services to clear business outcomes.	MSP/MSSP success is rarely tied to specific business objectives. Organizations may quickly change their risk appetites based on new business opportunities or perceived threats. The MSSP will likely have limited resources or expertise to have detailed insight into the commercial considerations of their clients.
MSPs and MSSPs reach economic scale by offering standardized services to their clients regardless of business needs or industry. In the case of MSPs, security is not a primary focus.	MSPs and MSSPs build a standard set of capabilities that can be offered across multiple industries to be profitable and provide consistent performance. This equates to a generalist approach to cybersecurity that may not be sufficient for financial services organizations.
The majority of MSPs and MSSPs experience high staff turnover due to the nature of the work, compensation models, and the chronic shortage of cybersecurity talent in the marketplace.	As is the case for all organizations, MSPs and MSSPs compete for in-demand cybersecurity talent. A stable and capable team of cyber specialists can be a significant differentiator when considering cybersecurity services providers.

Source: Aite Group

FINANCIAL SERVICES ORGANIZATIONS HAVE SPECIFIC NEEDS

Brand reputation and customer trust are critical to the financial services industry. Even a small cybersecurity issue (let alone a breach) can negatively impact the success of the business. Financial services organizations have specific cybersecurity criteria, as shown in Figure 1 and further defined herein:

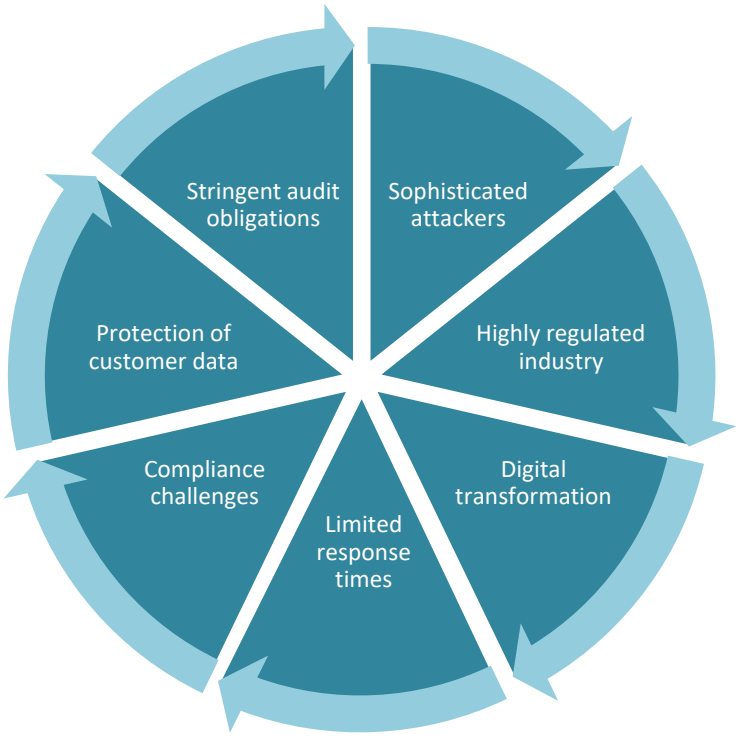
- **Sophisticated attackers:** Financial services organizations are routinely in the crosshairs of the most sophisticated and motivated cyber attackers, including cybercrime gangs and nation state hackers. Attackers are targeting both monetary assets and sensitive customer data.
- **Highly regulated industry:** The financial services industry is under intense scrutiny and regulation by governments, including regulators, examiners, and auditors.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Multiple and overlapping regulations define business conduct, data protection, privacy, and reporting requirements.

- **Digital transformation initiatives:** Banks of all sizes have embarked on digital transformation innovation programs to include new web and mobile banking products. These programs come with new risks and the need to perform constant monitoring for anomalies and attack indicators.
- **Limited response times:** Organizations no longer have the luxury to investigate and respond to cyber anomalies and suspected attacks when resources become available; cyberattacks propagate quickly and can inflict significant brand damage.
- **Compliance challenges:** Financial services organizations have specific data archiving, records management, communications backup, and data management requirements related to compliance.
- **Protection of customer data:** Financial services organizations collect, process, and store highly sensitive customer information.
- **Stringent audit obligations:** Financial services organizations are rapidly adopting data aggregation and data warehousing strategies, often using business intelligence and artificial intelligence capabilities to drive new business opportunities. These types of initiatives can add to audit complexity and the need to demonstrate how data is being protected.

Figure 1: Specific Cybersecurity Concerns for Financial Services Organizations



Source: Aite Group

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

REASONS THAT OUTSOURCED CYBERSECURITY CAN FAIL

Many organizations have used outsourced cybersecurity services, often with mixed results. Several factors can lead to a failed relationship:

- The cybersecurity services provider staff do not have specific financial services industry knowledge, particularly in audit and compliance requirements.
- The supported organization treats the service provider as a vendor rather than a business success partner.
- The organization has unrealistic expectations for the service provider.
- The organization requires the service provider to manage outdated cyber tools and products.
- There may be limited or infrequent coordination with the service provider after the initial "honeymoon" period.
- In smaller organizations, the person responsible for security does not devote sufficient time to nurture the relationship or fully understand the provider's capabilities.
- The cybersecurity services provider offers complex pricing models that complicate the organization's cost control measures.

For these reasons and many others, some financial services organizations had less than favorable outcomes with their first forays into managed security services. However, recent innovations in the managed security services market, particularly the concept of a security management partner, may warrant another look at a service provider relationship.

THE SECURITY MANAGEMENT PARTNER CONCEPT

The concept focuses on several service differentiators specifically tailored to financial services organizations and goes well beyond generic cybersecurity services provided across multiple industries. A security management partner for financial services includes the following characteristics:

- Expert-level financial services cybersecurity knowledge and experience
- Highly trained and motivated management and staff
- Daily exposure to the full range of attacks and tactics directed at financial services organizations
- Available and responsive on a 24/7 basis
- Well-versed in financial services compliance and audit requirements
- Tested and tuned tools and platforms for cyber defense
- A simplified or all-inclusive pricing model

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

- A true extension to the business and committed to successful joint business outcomes

The partner model treats the cybersecurity services provider as a logical extension to the organization's IT staff and encourages a complete and transparent two-way communications channel.

EXAMPLE OF THE SECURITY MANAGEMENT PARTNER CONCEPT

In July 2020, Aite Group met with members of SEI Investments Company (Nasdaq: SEIC), a publicly owned asset management holding company founded in 1968. SEI is a leading provider of technology-driven wealth and investment management solutions with 3,800 employees and 11,300 clients. SEI administers approximately US$1 trillion in hedge funds, private equities, mutual funds, and pooled or separately managed assets.

SEI's cybersecurity team has been defending SEI assets for more than 20 years, including the SEI headquarters, branch offices, and data centers. Based on this pedigree and specific experience applying IT support and cyber defenses to a large financial services organization, SEI has begun to offer IT and cybersecurity services to financial services companies of all sizes. SEI has built robust cyber defense monitoring tools, partners with security solution providers, and goes well beyond monitoring to include remediation and advisory services.

Aite Group had several meetings with SEI's cybersecurity team from July 2020 to March 2021 to assess the company's cybersecurity services capabilities and to observe SEI's approach to serving as a security management partner for its financial services clients. Aite Group was particularly intrigued by SEI's deployment model, which essentially extends the full range of cybersecurity services to customers by adding the client's infrastructure as an extension of the SEI platform as if SEI was adding a new branch office or data center. This approach allows SEI to provide clients with the same level of cyber support provided to its own entities and a consistent coverage across all entities.

Aite Group's take is that SEI's cybersecurity services are an excellent example of the security management partner concept. SEI's cybersecurity services are ideally suited to smaller financial services organizations that may not have sufficient cybersecurity expertise on staff. The services would also be enticing for larger firms seeking to expand existing in-house cybersecurity capabilities.

CASE STUDY #1

Aite Group spoke with the information technology officer of a rapidly growing U.S. state-chartered community bank with US$1.5 billion in assets and an asset management division with an additional US$1 billion under management. The bank has 12 physical branches, a small IT staff, and limited in-house cybersecurity expertise.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

The bank had previously used an MSSP, but the bank's information technology officer noted shortcomings with the services—particularly, the MSSP's responsiveness to cyber anomalies, slow responses to bank inquiries, and the poor quality of data contained in MSSP reports.

The bank partnered with SEI for cybersecurity services and completed a successful proof of concept in April 2019, with a move to full production in February 2020. The bank has full access to the SEI platform's capabilities and receives extensive details on alerts, cyber health, and other valuable information not available from the previous MSSP.

The information technology officer noted that he and the IT team have direct access to SEI's engineers on a 24/7 basis and can log into the portal to obtain the information they need to respond to leadership inquiries and prepare reports for auditors and examiners. The information technology officer told Aite Group that with SEI's services, the bank gets expert cybersecurity services rarely seen at organizations of this size.

The information technology officer stated that he now feels that he has engaged a partner that truly cares about the bank's security with a refreshing approach to cybersecurity. He particularly stressed the full visibility and transparency of SEI's cybersecurity services.

CASE STUDY #2

Aite Group spoke with the chief technology officer (CTO) of a full-service community bank for consumers and businesses. The bank has more than US$1 billion in assets and is rapidly growing into new markets and geographies. The CTO has engaged service providers for cybersecurity services in the past, but he indicated that he was not impressed with their lack of financial services experience. He told Aite Group that he needed reliable and capable cybersecurity services, as the bank was crossing the US$1 billion threshold and was subjected to additional regulatory oversight.

The bank partnered with SEI in September 2020 and completed a rapid integration of SEI services. More than 90% of the bank's endpoints were added to SEI's coverage within two months, and this included a complete replacement of the bank's aging endpoint security product. The CTO reported that the IT team encountered no issues during the rollout, primarily due to SEI's detailed processes for service implementation.

The CTO indicated that he frequently accesses the SEI portal and can obtain the information he needs to brief the bank's leadership. He was particularly impressed with the SEI team's ability to provide the bank with audit support based on SEI's own experience with similar audits. The CTO said that this is something that previous service providers could not provide, and the assistance from SEI contributed to a successful audit.

The CTO said that he is seeing great value from SEI's cybersecurity services, as SEI is covering a lot of cybersecurity tasks that the bank's IT team had to perform themselves because the previous service providers would not or could not do so. He indicated that working with SEI was the difference between real security and checking boxes.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

RECOMMENDATIONS

Aite Group makes the following recommendations for representatives of financial services organizations looking to outsource cybersecurity services or replace an existing service provider:

- Reevaluate your organization's overall requirements for cybersecurity, particularly when outsourcing key services. Consider whether the needs include remediation support.
- Consider the unique needs of financial services organizations when seeking or replacing service providers. Does the service provider understand the types and severities of the threats?
- Take into consideration the fragmented nature of the market. Will the service provider be acquired or exit the market?
- Examine the provider's service offerings. Do negotiated costs cover the organization's full requirements or will there be supplemental service charges for "extras"?
- Scrutinize the provider's portal and graphical user interface. Can it be successfully interpreted by noncyber staff?
- If cyber compliance and audit support are a value proposition, look for providers that understand the landscape and can help.

CONCLUSION

- The cybersecurity marketplace has become particularly crowded during the last four years as hundreds of MSPs and MSSPs have offered their services to offload cyber tasks from organizations.
- Financial services organizations have specific cybersecurity needs that cannot usually be met by cybersecurity services providers that do not have specialist expertise in financial services requirements.
- A new concept—the security management partner—is ideally suited to financial services organizations and provides tailored cybersecurity capabilities, including remediation and advisory services.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

ABOUT AITE GROUP

Aite Group is a global research and advisory firm delivering comprehensive, actionable advice on business, technology, and regulatory issues and their impact on the financial services industry. With expertise in banking, payments, insurance, wealth management, and the capital markets, we guide financial institutions, technology providers, and consulting firms worldwide. We partner with our clients, revealing their blind spots and delivering insights to make their businesses smarter and stronger. Visit us on the web and connect with us on Twitter and LinkedIn.

CONTACT

For more information on research and consulting services, please contact:

Aite Group Sales
+1.617.338.6050
sales@aitegroup.com

For all press and conference inquiries, please contact:

Aite Group PR
+1.617.398.5048
pr@aitegroup.com

For all other inquiries, please contact:

info@aitegroup.com

RELATED AITE GROUP RESEARCH

Better, Stronger, Cheaper Cybersecurity: Doing More With Less in a Crisis Economy, June 2020.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com