GreatAmerica® FINANCIAL SERVICES

HARD WORK • INTEGRITY • EXCELLENCE

COLLABRANCE®

A GREATAMERICA COMPANY

Survey Report:

MANAGED SECURITY SERVICES IN THE IT CHANNEL

STUDY SHOWS MSPS LOSE MORE END-USER CUSTOMERS THAN MSSPs

TABLE OF CONTENTS

In this report, you will find answers to questions such as:

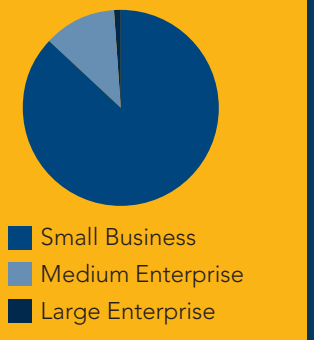
- How many service providers consider themselves MSSPs?
- What security components MSPs are looking to add to their offering?
- How many MSPs currently outsource components their security offering?
- How many MSPs have looked into partnering with a MSSP?
- How many MSPs feel that becoming or partnering with a MSSP is critical to sustaining the future success of their business?

MSSP SURVEY

- July 2018
- 237 MSPs
- C-Level Participants
- Located in the U.S.A.

TechValidate by SurveyMonkey

BUSINESS SIZE OF PARTICPANTS



GreatAmerica Financial Services surveyed nearly 250 executive MSP contacts in the U.S. through a third party research firm, TechValidate to confirm the results. The survey helped explain the security evolution in the SMB Market. This report shares what MSPs reported when it comes to security and becoming an MSSP.

EXECUTIVE SUMMARY

MSPs today are faced with whether or not to pursue becoming a Managed Security Service Provider (MSSP). While MSPs weigh the pros and cons, the shift towards more cybersecurity continues to evolve.

One of the largest drivers of this shift are clients requesting more and more security offerings. A key finding from the survey found that 87% of MSPs reported they have lost end-user customers because they needed more security services the MSP wasn't currently providing. On the flip side, of those who consider themselves an MSSP today, only 5% report they have lost end-user customers because of the same reasons.

These statistics support why many MSPs are reviewing their current managed services offering and including more security components in their technology roadmap. MSPs appear to have an opportunity to both deepen their relationship with current customers and expand their customer base with security enhancements to their offering and becoming an MSSP.

MSPs LOSE CUSTOMERS DUE TO LACK OF SECURITY OFFERINGS

More than 8 out of every 10 surveyed MSPs have lost customers because of a lack in their security offering.

Source: TechValidate survey of 133 users of GreatAmerica Financial Services

Only 5% of MSSPs report they lost customers because they needed more security services they aren't yet providing.

Source: TechValidate survey of 20 users of GreatAmerica Financial Services

Number illustrates an opportunity for MSPs to transition to become an MSSP and avoid losing more customers.

Image: The GreatAmerica and Collabrance team prepare for the MSSP security webinar.

WHAT IS A MSSP?

There is a lot of confusion and no clear answer on defining what an MSSP is by today's standards.

An MSP has to take security into account for just about everything they do. For example, if they are managing an endpoint, they need to do it securely. If an MSP is even installing a printer, they have to think about the most secure way to do it.

DIFFERENCE BETWEEN MSP & MSSP

"An MSSP is actually offering security solutions. They aren't simply offering a solution and doing it securely; the focus of their offering is security."

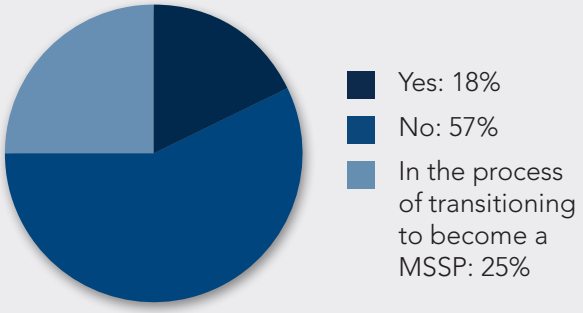
An MSP typically focuses on managing the network, and always keeps security in mind.

Not just doing things securely, MSSPs have security-focused solutions. Those solutions are focused on protecting and preventing their clients from cybersecurity attacks using both technology, process and policy.

OFFERING MANAGED SECURITY SERVICES

While there are no benchmarks on what makes an MSSP, in our survey we asked customers to identify whether they considered themselves a Managed Security Services Provider.

Do you consider yourself a "Master Security Service Provider (MSSP)" today?



Source: TechValidate survey of 226 users of GreatAmerica Financial Services

Out of the 226 Managed Service Providers we surveyed, most do not consider themselves MSSPs. Only 18% (or around 40) currently consider themselves MSSPs and a quarter of those we surveyed are transitioning to becoming a security services provider.

THE SECURITY INDUSTRY IMPACT ON MSPS

The IT threat landscape is constantly evolving. As security demands increase over time, MSPs have the opportunity to thrive in this area and expand their business since they already serve customers who see value in outsourcing their IT needs. SMB customers in particular need to partner with an MSP or MSSP to protect their business from external threats. Today, to prevent and protect clients from those threats, outsourced security providers need a multi-layered approach with various security components. MSPs will need to evolve with the demand to remain relevant and to maintain and grow their customer base.

"If MSPs don't work to evolve their security offering, they will continue to lose customers and be left behind."

The security landscape can be seen as a game of leapfrog. The bad guys think of new clever ways to get into networks and steal data. The MSPs on defense have to come up with new solutions, new ways to stop cybercriminals, and then the bad guys will constantly continue to think of new ways to go around the new measures. As we play a game of leap-frog in the IT industry, MSPs who don't proactively work to innovate and evolve their IT solution will be left behind.

THE SPECTRUM OF SECURITY SERVICES

There is no single solution or silver bullet that will cover every client's needs for security. No one can ever be 100% secure, so the question becomes "How secure does a customer want to be?" coupled with what the SMB client can afford. The results of asking MSPs which security elements they are currently offering demonstrates there are no standards. Even solutions that are widely-adopted are not being offered by all Solution Providers. MSPs interested in creating security offerings need to determine what security components they include in their offering.

(The more you include, the more it would cost. The fewer items, the more risk exposure.)

Even if you aren't promoting your business as a security provider, you may find your customers will begin relying more on you to help them assess and mitigate their security risks and to help them implement the appropriate security solutions.

33 SECURITY SERVICES BEING OFFERED BY MSPs

What's included in your CURRENT security offering?

Source: TechValidate survey of 185 users of GreatAmerica Financial Services, comprised of Small Business and Medium Enterprise IT organizations.

Image: We asked MSPs what security solutions they are currently offering clients.

What do MSPs believe should be included at a minimum for security?

In our TechValidate survey, we wanted to understand where MSPs are at today and where their opportunities are to expand their security offering in the future.

So what are the minimum requirements for a security offering? As we stated earlier, there are no industry standards, so MSPs must both look at their customers' needs while creating their own benchmarks. Each customer will be different, but you may find commonalities among industries. For example, healthcare organizations will have similar requirements, banks and financial institutions are also abiding by the same regulations. You will find some "like to have" security components may be a "requirement" for other customers based on their needs.

Image: The top five security components MSPs provide to end-user customers at minimum include: UTM/Firewalls, Computer Updates/ Patch Management, Backup & BDR, RMM and Email SPAM Filtering.

Our survey findings revealed the following security components MSPs require their customers to adopt before taking them on as clients. Those include a firewall or unified threat manager, updated computer or patch management, backup disaster recovery, remote monitor, and email filtering.

This indicates that while there isn't a baseline for security offerings, most MSPs are taking their clients' security into consideration before taking them on.

What are MSPs currently offering for security?

Image: A majority of MSPs include these 12 security components in their current offering.

Only 18% of MSPs we surveyed consider themselves a security services provider, yet most are offering services in the security spectrum. Here are the top twelve security services offered by MSPs.

These top offerings include an additional seven components above and beyond the minimums outlined above. The number of security components MSPs offer have continued to increase and are expected to expand in the future. This reflects the evolving security industry and the growing needs of SMB customers.

As an enterprise business, GreatAmerica applies all of these security elements with the addition of two other major components: Security Information Event Management (SIEM) and Vulnerability / Penetration (VUL/PEN) Testing.

What security components MSPs are looking to add to their offering?

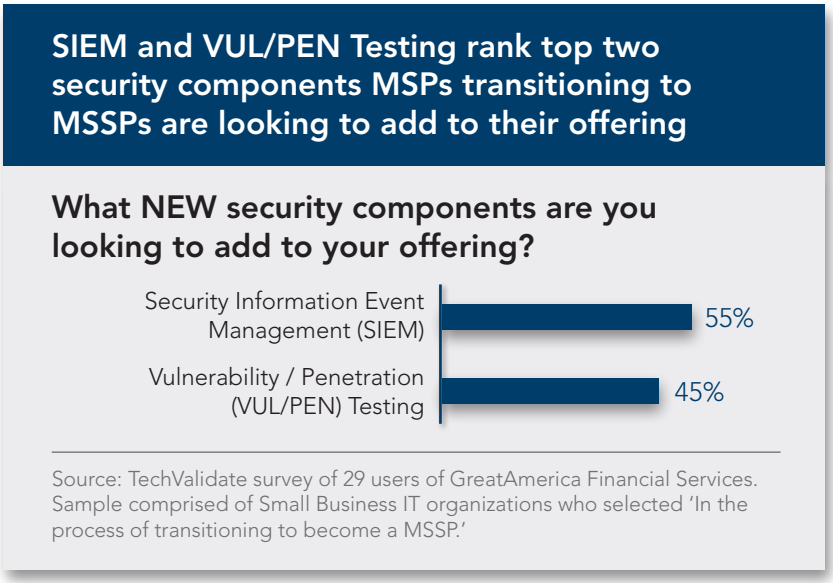


Image: A majority of MSPs share the top two components they want to add to their security offering includes (1) SIEM) and (2) Vulnerability and Penetration Testing.

Incidentally, SIEM and VUL/PEN Testing are also the next wave of services being adopted and deployed in the MSP community.

Both SIEM and VUL/PEN Testing are two solutions many enterprise-level companies have been using to improve their IT security. As more small and medium sized business become more aware of security threats, MSPs are expected to provide these types of security elements.

Image: Collabrance discusses security enhancements for MSPs.

55% of MSPs look to add Security Information and Event Management (SIEM) to Security Offering

Today, most MSPs have a Remote Monitoring and Management (RMM) solution to proactively monitor endpoints and receive alerts based on triggers. It would be impossible for an organization only using RMM to monitor the thousands or even millions of events generated on a daily basis. If you're going to evolve your security offering, a SIEM solution should be implemented to thoroughly monitor your customers' critical devices.

A SIEM solution aggregates all the logs and events from the various servers, switches and unified threat management devices and identifies the ones which could pose a security threat.

45% of MSPs look to add Vulnerability and Penetration Testing to Security Offering

Enterprise customers have been using VUL and PEN testing for a while, but it is an emerging need for the SMB market. Do your customers know how secure their technology environments are from outside threats? Do you know if line of business applications have been maliciously patched? Vulnerability management is a process that scans the network and looks for gaps or potential entry points for cyber threats. Penetration testing is typically done by a third party to see if they can enter the network through any of the gaps.

SIEM & VUL/PEN Testing in Collabrance Master MSSP Offering. Collabrance, a GreatAmerica company, provides Service Providers with a standardized technology stack and Master MSSP offering. The all-in offering currently includes over 20 different security components, with a roadmap of others to be added in both the short and long term. Their latest enhancements included both SIEM and VUL/PEN Testing to help MSPs differentiate and meet the needs of end-user customers.

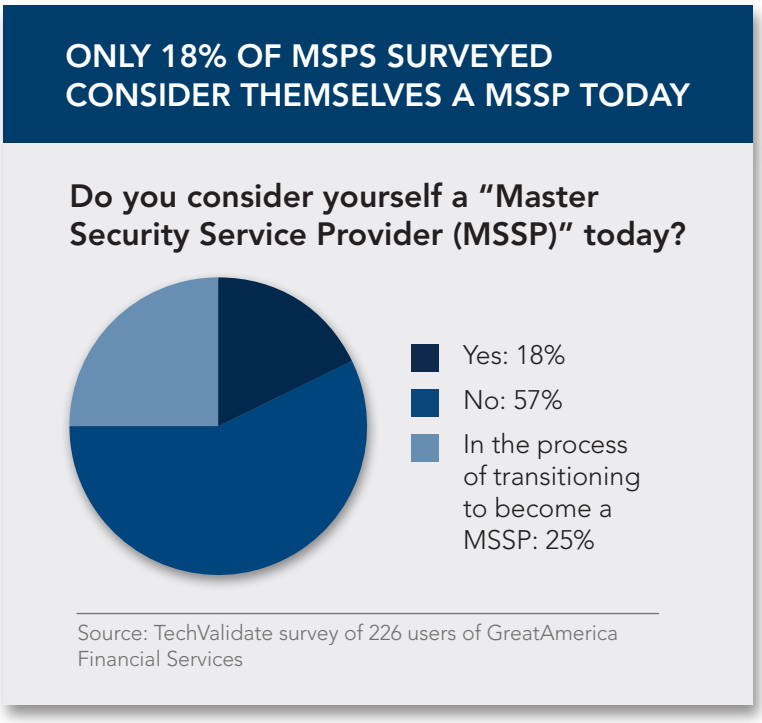


Image: As security becomes more of a request from end-user customers, we expect more MSPs to make the move towards becoming a MSSP.

MSSP TODAY AND TOMORROW

According to the data, MSSPs on average offer 12 more security components than their MSP counterparts. Security is a central topic in the managed services industry and we assume it will remain top of mind for both MSPs and end-user customers. Out of the pool who don't consider themselves an MSSP today, 44% are in the transition of becoming one (25/57).

If we combine those who are currently in transition to become an MSSP and those who already consider themselves an MSSP, then MSSPs in the future would make up nearly half of the market.

TOP CHALLENGES TO MAKE THE MSSP TRANSITION

The transition to become an MSSP comes with significant challenges, which could contribute to the small number of MSPs who consider themselves an MSSP today.

Through our research, we identified two main challenges for making the transition: people and technology.

#1 People - IT is one of the fastest growing industries, and IT security is the fastest of them all which makes it hard to find good, qualified people to add to the team. An MSSP recruiting those qualified IT candidates is difficult, and it's even harder to convince them to work all the hours needed.

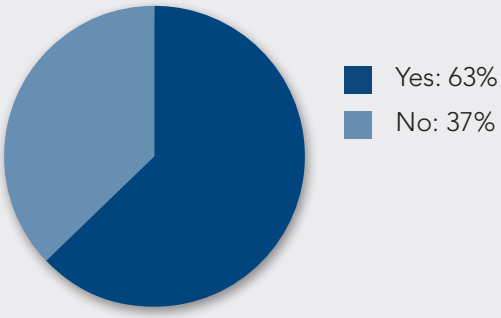
#2 Technology - Technology is hard to because it is not a set-it-and-forget-it mentality. Training someone to set up everything needed for a security offering, tune it, monitor it, as well as continuing maintenance and administration is not easy. This all leads to a significant barrier in MSPs trying to transition to become an MSSP.

IN TRANSITION OF BECOMING AN MSSP

A quarter of Service Providers indicated they are currently in transition to becoming an MSSP. This could be a result of a majority of MSPs reporting that making the transition will be critical to the future success of their business and to not lose customers.

MAJORITY OF MSPs FEEL MSSPs ARE CRITICAL TO SUCCESS

Do you feel that becoming or partnering with an MSSP is critical to sustaining the future success of your business?



Source: TechValidate survey of 152 users of GreatAmerica Financial Services

Image: Majority of MSPs feel that becoming a MSSP is critical to the success of their future business.

OUTSOURCING WITH A PARTNER TO BECOME AN MSSP

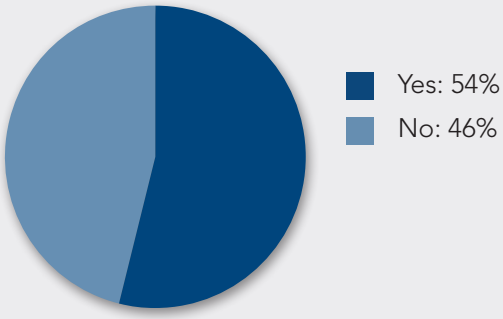
Similar to becoming an MSP, you have three options on your journey to transition to become an MSSP:

- Build your own MSSP offering
- Buy and acquire an MSSP
- Partner and outsource with a current MSSP

As MSPs expand their offering and technology stack, vendor management and product development can consume a significant amount of time, effort, resources and money. There are a lot of different options when it comes to security in the IT channel. As enhancements are made, it may become more difficult for MSPs to manage all of the vendors and services effectively.

MAJORITY OF MSPs OUTSOURCE SECURITY COMPONENTS

Do you outsource any components of your security offering to a 3rd-party?



Source: TechValidate survey of 152 users of GreatAmerica Financial Services

Image: 54% of Service Providers already outsource components of their security offering today.

More and more MSPs, especially high performing MSPs, have found value in outsourcing. Partnering with and MSSP can remove the barriers of technology and people as well as decrease a Service Providers risk.

Image: Collabrance discusses strategies for MSPs to grow faster.

"Outsourcing allows MSPs to focus on scaling the business efficiently, quickly as well as being able to find ways to differentiate from their competition. It's seen as one of the best ways to get into the market faster."

No one company can be best-in-class at everything and this is familiar to MSPs who have to wear a lot of hats in the business. As your customer's trusted technology advisor, your SMB customer wants to be able to call you for everything, and you need to be able to offer solutions with vendors who are the best of breed if you want to keep the competition out. Partnering can also reduce your time and cost of implementation. Outsourcing is a reality of the industry today.

Image: 58% of Service Providers in transition to becoming an MSSP report they are looking at partnering.

CONCLUSION

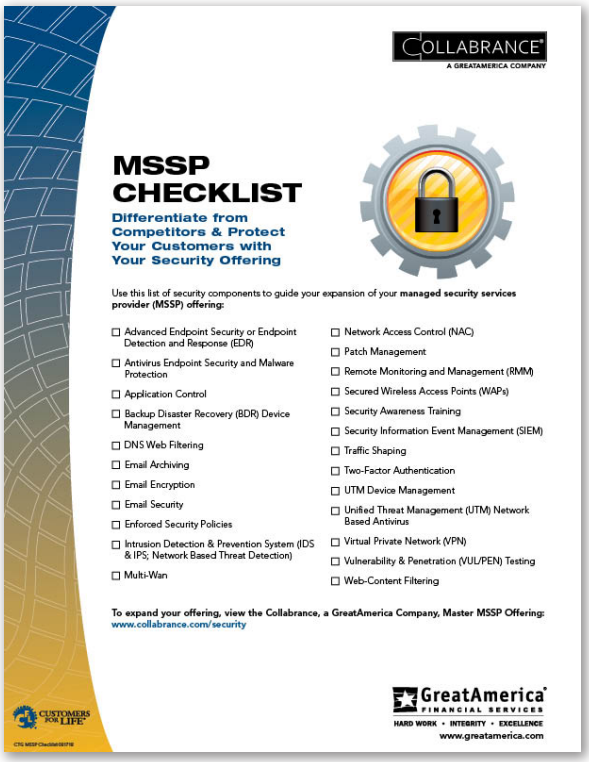
As we reported, one of our major key findings from the survey was that 87% of Service Providers reported they have lost customers because they needed more security services they aren't yet offering. When we asked MSSPs the same question, only 5% reported they have lost customers because of a lack of security offering. This significant difference may represent the large opportunity Service Providers may have if they decide to evolve to being an MSP to an MSSP.

Since a good portion of the market has not made the transition to be an MSSP yet, there are differentiation opportunities for MSPs and MSSPs. Other opportunities include more customers, deeper relationships, and increase monthly recurring revenue which results in a higher business valuation.

The risk of not transitioning includes the continual loss of more customers and competition with MSSPs who have evolved to offer more security services customers seek.

"Security will continue to increase in the news and in your SMB customers everyday needs. It is critical that you consider the opportunity and potential impact of transitioning your business to become an MSSP in order to not be left behind."

Based on our findings, we anticipate the number of MSSPs to notably increase over the next several months. Of those who are looking to transition, a majority have indicated that outsourcing and looking for an MSSP partner is the fastest way to implement services and reduce their risk in the security industry. Because there is no clear definition of an MSSP, we compiled a list of security components based on our research for you to use to evaluate your offering and technology roadmap.



MSSP CHECKLIST WITH CORE SECURITY ELEMENTS

According to hundreds of hours of our own research from Collabrance, there is no clear definition or threshold of what currently defines an MSSP. Several different players in managed services offer different explanations of what an MSSP could or should be.

To help you evaluate your current security offering and your future technology roadmap, there is a checklist of security elements we identified and recommend to help you transition to be an MSSP:

Download a copy of the MSSP Checklist at **www.collabrance.com/mssp-checklist.**

WHERE MSPS LOOK FOR INFORMATION ON SECURITY

We are fortunate today to have several different resources at our disposal to collect information and help us make informed decisions. Some of the places MSPs are seeking information on security according to our survey include:

- Customers
- Peers
- Events
- Online Searches
- Blog/Newsletters

Other recommendations from webinar panelists:

- Krebs on Security: www.krebsonsecurity.com
- Bank Information Security: www.bankinfosecurity.com
- SANS Institute Newsbites: www.sans.org/newsletters/newsbites
- SANS @Risk Newsletter: www.sans.org/newsletters/at-risk
- Nuspire Blog: www.nuspire.com/resources/blog
- SC Magazine: www.scmagazine.com

For best practices in managed services, including network security, MSPs/MSSPs can subscribe to the GreatAmerica UC & IT and/or Collabrance blog for insight from industry thought leaders.

www.collabrance.com/blog
www.greatamerica.com/blog/unified-communications-it-blog

GREATAMERICA FINANCIAL SERVICES

A family-owned business, GreatAmerica was established in Cedar Rapids, Iowa in 1992 and has nearly 2 billion in assets. More than just a finance company, the Unified Communications & IT Group at GreatAmerica is dedicated to understanding the IT, Managed Services, Unified Communications and Low Voltage industries. Our exposure to thousands of telecom providers, MSPs and independent VARs contributes to our ability to help our customers evolve their businesses through targeted and innovative solutions. The collective knowledge and experience of GreatAmerica enhances the development of specialized programs and collaborative learning opportunities to complement our vendor's offerings. Visit **www.greatamerica.com** for more information.

GreatAmerica®
FINANCIAL SERVICES
HARD WORK • INTEGRITY • EXCELLENCE

COLLABRANCE

GreatAmerica built Collabrance, a Master MSP, in 2009 from the need of customers looking for ways to scale their managed services business faster and with fewer risks. Focused on the same core values and principles, Collabrance was built on extending the GreatAmerica experience to end-user subscribers for customers. In addition to the outsourced NOC and Help Desk, Collabrance offers several other value-add services to partners such as sales support, onboarding assistance, a standardized technology stack, vendor management, as well as access to best practices and discounted trainings with industry thought leaders.

The Collabrance Master MSSP Offering includes over 20+ different security components that have been fully vetted and are managed by our dedicated product development team who is also responsible for the dynamic roadmap of additional services to be continually added based on the needs of our partners and their end-user customers.

To learn more about the Collabrance Master MSSP portfolio, please visit**: www.collabrance.com/security**

COLLABRANCE®
A GREATAMERICA COMPANY