pennAware

MSSP BUSINESS MODEL

Whitepaper

www.pennaware.com | info@pennaware.com | @pennaware

Table of Contents

CONTENTS

Introduction

The evolution of cyberspace has outdated the most of our current security solutions and the rapid change of the IT world makes it difficult to ensure security for organizations. Hence, even the biggest organizations have been confronting security issues . Without the proactive tools, these issues are able to damage businesses. Today's cybersecurity world has some challenges:

To bring a solution to these issues and challenges, organizations have to have new strategies like abandoning traditional and reactive strategies and adopting more proactive ones. One of the ways to achieve this is to have multi-layered security tools and also security experitse. However, most organizations lack these resources. They lack the sources such as technology, budget and security expertise to develop and maintain an effective security stance.

Managed security services are a perfect solution to the challenges organizations have been facing. A managed security service provider (MSSP) partnership has the potential to resolve the internal resource problem organizations have and fills in the gap within the security issues organization to fight against cyber threats.

In this paper, we are going to reveal how MSSPs could be a perfect business model to fight against advanced threats and bring solutions today's security challenges organizations have been facing.

How MSSPs Works

Managed security service providers (MSSPs) have risen as an effective and practical alternative to support businesses in preserving and defending digital assets, like files, emails, networks, and sensitve data. Consequently, MSSPs have been growing attention among enterprises of all scopes since they significantly boost their security spending.

Managed security services providers provide outsourced management and monitoring of the security systems. An MSSP can control and manage your Firewalls (UTMs, NGFWs, etc.), Log monitoring and management (SIEM), Intrusion Prevention Systems (IPS), Web content filtering, Anti-virus (AV), Anti-spam, VPN, Vulnerability scanning tools, Patch management, Data loss prevention (DLP), Threat Intelligence, Identity access management (IAM) and Privileged access management (PAM) and more. Organizations adopt MSSPs to hand over the burden of managing and monitoring hundreds of security issues like handling of the incidents a day. MSSP is a perfect solution to those lacking in-house security resources, the expertise, the necessary tools and technologies, and the time to monitor and manage your security issues.

MSSP providers can bridge security gaps within your company by presenting on-demand and comprehensive cybersecurity solutions to suit the dynamism of today's changing cyberspace and security threat landscape according to your requrements. MSSP also eliminates the necessity to hire in-house units to do the work. MSSPs extend their services on a Software-as-a-Servce (SaaS) bass, and businesses receive only what they pay for without spending on hardware or employee training for the responsibilties that MSSPs can manage. MSSPs can render dedicated facilities; hence outsourcing particular parts of regular tasks to proficent third parties service providers helps decrease workload and investments, responsibilities, and costs.

MSSPs Facts and Figures

Organizations are continuously suffering advanced threats, and to protect themselves from these threats, advanced and multilayered products developed by leading security companies have gained importance. The evolution of cyberattacks activities and businesses endeavor to get more cost-effective solutions are critical factors that have increased the managed security services market size. Here are some facts and figures on MSSPs:

- According to Gartner, managed security services market size is expected to be $40.97 billion by 2022, registering a CAGR of 16.6% during the forecast period 2016-2022,[1] and USD 64.73 billion by 2025, at a CAGR of 15.2% over the forecast period 2020 - 2025 according to Mordor Intelligence.[2]
- According to Datto's research, the top 3 most critical security offerings according to MSSPs are anti-virus, advanced firewall, and remote monitoring and management (RMM) solutions. Also, 51% of MSSPs wear multiple hats and describe ther primary role as a mix between both technical and business responsibilities.[3]
- According to Cisco, 9% of companies do not have any dedicated cybersecurity professionals at their organizations.[4]
- 53% say an increase in data to manage/analyze has made their operations more complex and 41% of businesses surveyed cited ongoing maintenance costs as the reason for low ROI.

[1] Managed Security Services Market Outlook: 2022. Retrieved from https://cutt.ly/wjJDsFL
[2] Managed Security Services Market - GROWTH, TRENDS, COVID-19 IMPACT, AND FORECASTS (2021 - 2026). Retrieved from https://cutt.ly/1jJDQaB
[3] State of the MSP Report. Retrieved from https://cutt.ly/cjJDAcg
[4] Global Managed Security Services Market 2020-2024. Retrieved from https://cutt.ly/fjRB9NS
[5] 25 IT Industry Statistics MSPs Should Know. Retrieved from https://cutt.ly/XjJFJSj

MSSPs Business Models: How to Integrate

MSSP services work like an addition to or extend the organizations' security system or structure that executes, controls, and manages its dynamic security needs. MSSP services may be deployed in-house, such as team force development, or outsourced to a service provider as a blended or multilayer solution that the organization has needed.

MSSP Business models can be schemed according to following structures:

Clients

It is a challenging process to try different products from different vendors one by one, make Proof of Concepts (POCs), make purchases, track licenses, install, use and update the various security applications, and increase efficiency. Clients can resolve these issues using MSSP business models.

Resellers

Using the MSSP business model, resellers will possess off the shelf and reliable security solutions or structures that serve all ther customers. They will not invest in any resources and will not bother with the continuity of the technological system. They will add value to their services with security traning, support, product management experience, etc.)

Distributors

These businesses can have a lot of Resellers. Using the MSSP business model, Distributors can save serious time by integrating into the Resellers' CRM and automatically managing the upsell/cross-sell opportunities. Moreover, the MSSP business model can provide a platform that will help them expand ther business.

Government Organisations

Government organizations can comply with the regulations and get multilayered security products and cybersecurity expertise to their subsidiary institutions with zero investment.

Outsourcing the security services for management, different businesses will focus on ther profession in their field and do not have to invest in budget and staff.

Benefits of MSSP

Adopting an MSSP model offers more than a few advantages to an organization since MSSP manages and controls your security environment.

Reduce Your Costs & Boost Effectiveness

According to an article written by Cipher, organizations have to expend the following chairs cybersecurity while acquiring a full stack of security technologies and solutions in-house:

- Vulnerability and Configuration Management: $70-105K salary plus hardware/software licensing,
- Penetration Testing: $75-105K salary plus hardware/software licensing,
- Security Engineering: $70-110K salary,
- Audit and Compliance: $90-120K salary plus licensing for software,
- Project Management: $70-105K salary plus software licensing,
- Management: $100-150K salary,

"For single coverage on each chair, organizations are looking at $475,000 to $695,000, plus the costs of benefits. Add to that the costs of building your own 24×7 SOC and payroll doubles to up to $1.3 million. Facilities for them add yet more, and you're still looking for a security uncorn to bring it all together. Coming in on the low side of payroll estimates will bring you turnover and re-training, costs unto themselves."[6]
Hence, MSSPs and cybersecurity outsourcing shifts to a much more reasonable choice.

Other costs that are saved via MSSP business model:

- **No Hardware Expenses**: Capabilty to manage organization's IT security hardware costs for a fixed term service contract.
- **No Unexpected Expenses:** Anticipated operational expenses instead of facing new surprising costs
- **Complance Expenses:** Organisations might have to use the extra fund to guarantee compliance with the latest security standards, regulations, authority assessments, or security program developments to keep up with the laws. MSSPs already concentrate on updating their systems to ensure compliance such that they conduct vulnerability assessments

Moreover, with access to high-level and latest cybersecurity technologies using MSSPs, organizations can immedately optimize system relaibility. Security professionals offer monitorng and quick remediaton of security incdents that minimizes disruptions and the impacts. MSSP business model helps organizations with the skilled-team using the latest technologies to identify security issues, which provides excellent protection.

Staff Enhancement

The lack of adequate security staff puts a significant burden on businesses to hire, teach and preserve their security personnel. And typically, organizations realize that after investing a lot of money in security software, their personnel do not possess the capability to use this software accurately and effectively. Training this staff is too costly and time-consuming. Even recruiting the right person for this operation necessitates resources.

An MSSP business model will help organizations to have world-class security specialists. This business model can extend the organizations' team and provide a unique benefit, such that they will have continued services wherever or whenever needed thanks to an MSSP's global 24x7x365 Securty Operation Centers (SOCs). These SOC teams provide organizations the most advanced and the latest threat intelligence and visibility aganist high-level risks. MSSP business model basically extends any organizations' security team to a global security footprint.[7]

[6] 10 Managed Security Services Benefits To Know. Retrieved from https://cutt.ly/pjJG0ms
[7] ibid.

Focus on Business

Organizations can focus totally on developing their own business without considering security issues. The MSSP can deal with the security issues, and organizations can maintain their business. It will improve businesses' profitability, give them more space to realize their development and have nonstop achievement.

A business exists to serve clients and create value for the owners and its shareholders. An MSSP model helps businesses to maintain this task by assisting them to focus on their mission. The security issues are kept under control by MSSPs that help companies concentrate on their mission and duties, strategies, core business operations, and new opportunities.

Flexibility and Adaptability

An MSSP business model provides multiple delivery options that are flexible and do not require any additional infrastructure investments. Should an organization's requirements or priorites change, the MSSP solutions can change with minimum trouble.

Also, it becomes more manageable for companies to adapt to evolving technologies that present a superior competitive position.

Using An Advanced Technology

MSSPs have been continuously testing most of their technology, products and they have been creating orignal solutions from what they've tested.

Today, almost every organization has utilized a layered model of security however, "best-of-breed technologies are not designed to communicate with each other and every technology leaves gaps that need to be addressed in order to have a bulletproof solution". An MSSP resolves this problem.[8]

MSSPs present cybersecurity tools to assist businesses around the globe to mitigate security risks. This experience and skill have progressed MSSPs to create advanced security tools for different clients and industries. They have developed technologies to assess controls, address gap analysies, test system and organizational security vulnerability, and fix crucial risks.

Moreover, an MSSP offers multi-layered security solutions, a security package that uses numerous tools and processes to protect an organization in multiple levels or layers.

Furthermore, an MSSP manages security services for thousands of clients and their networks and systems and leverage this practice and experience to ensure that all clients are always ahead of the latest risks.

Benefiting from MSSPs' Security Specialists

Cybersecurity is more than technology, and it encompasses the people, processes and technology elements together. Moreover, creating a cybersecurity process, setting up controls, examining controls, managing vulnerabilities, and performing security tests; all require a range of skills and experience. MSSPs can create the conditions to apply the best security practices for organizations using their specialists and experience which maximize return on investment while addressing the most complex cyber threats.

[8] Top 5 Benefits Of A Managed Security Service Provider. Retrieved from https://cutt.ly/fjRB9NS

How to Qualify your MSSPs

A company might wish to adopt an MSSP business model and cooperate with an MSSP for many reasons like limited budget, lack of skilled staff, the burden of monitoring the latest threats. However, organizations must be very cautious while selecting an MSSP before their engagement

Security Maturity & Certifications

Certifications such as SOC and ISO 270001 are vital indicators of an MSSP's security maturity level and capability. It is also possible to evaluate MSSP's maturity according to their expertise, like how long they've been in business. Moreover, before engaging with an MSSP, organizations must thoroughly control their references and see who they work with.

Service Range and Category

MSSPs may present a variety of security services. However some deliver services in only particular security areas. Depending on their mission, vision and clients' demand, organizations can choose the best MSSP model that will serve to their best interest and be more valuable in gaining profit.

Multitenancy

MSSPs can handle and control multiple platforms and products with various solutions and configuration levels. Moreover, according to product, the special support conditions changes which makes the management of platforms complex once the number of clients and the variation of solutions offered increase. Multitenancy feature put an end the chaos created by circumstances that all services have to be controlled and managed independently. Hence, by integrating various products and platforms through multitenancy feature, organisations are able to offer an extensive service level which provide multilayer security capacity.

Service Level Agreements

Organizations must concentrate on the language in the SLAs, and qualify the security services that will be managed by the MSSP, and their maintained process whether or not they are operated by the in-house team. Or during the emergency circumstances, e.g. during security breach, how the MSSP deliver special services or work out more hours?

Dedicated Infrastructure & Portal

An MSSP should own and control ther Securty Operations Centers (SOCs) and work on a 24x7x365 support bass. Hence organizations should be careful when selecting an MSSP that provides this level of services and should be specific on the support given and the timely response during an incdent. Organizations should be looking for an MSSP with a dedicated infrastructure built wth the most advanced technologies to support analysis, investigation, response, and prioritization. An equipped MSSP service provider will have a dashboard-ready portal and comprehensive documentation that renders an understanding of all processes.

References By Global Customers

An organization can qualify an MSSP provider by looking at its references, global clients and validating its skills and performance. Hence to qualify any vendor, organizations should look for an MSSP that received credit from the industries.

Compliance to Regulatory Standards

Organizations can also qualify an MSSP by looking at their various compliance and regulatory standard levels. They should look for ther compliance level to the standards such as PCI DSS, HIPAA, FISMA, SOX, and FFIEC. Regulatory conditions and the emerging threat landscape is changing continually, and it becomes very challenging for an organization to track these changes. An MSSP should have a proficient team that knows these new standards and correctly apply the right strategies to conform to them.

PennAware Business Model for MSSPs

As a security vendor, PennAware provides various email security solutions in one platform to the MSSPs. If you are an MSSP or a business that considers to operate as an MSSP, the PennAware business model will be a perfect solution for you.

The MSSP business model offered by PennAware helps institutions manage cyber security solutions in a scalable and integrated way which creates an efficient, automated process against email attacks.

PennAware MSSP business model allows you to transfer your unlimited business partners (reseller, distributor) or direct customers to the platform either automatically with a single click or manually.

PennAware MSSP business model offers you level 1 and level 2 support, you will never be left behind whilst delivering support services to your customers.

PennAware MSSP business model, allows you to license 6 different technologies individually or as a package and to create flexible sales models.

You do not need an infrastructure investment and you can use our data centres in the EU or other countries which are fully compatible wth GDPR and other local laws and regulations.

Providing a customizable product, this business model gives you the opportunity to demonstrate your brand power with your own domain name, your own logo and all other white-label customizations. Your customers feel your presence more.

With API support, your chance to integrate with almost any solution, your orchestration and reporting capabilities increase.

This business model supports you in doing things that reveal your added value and meets the different reporting needs of your customers.

ABOUT US

PennAware protects businesses throughout the full lifecycle of email-based cyber-attacks. We have developed a full spectrum suite of cyber-security defence, threat monitoring, security management and user awareness products that encapsulate an integrated approach to people, processes and technology thus reducing the threat in all areas of cyber risk. We are committed to continuous innovation and expansion of our suite of security products in order to meet the needs of a dynamic and rapidly growing networked population in a constantly evolving cyber-threat environment. Our cyber defence strategy adopts three holistic elements: people, process, and technology:

People: we focus on the "human factor", using engaging, structured, content to raise cyber awareness and engender "active defence" behaviours.

Process: we support the development and management of user security awareness plans, monitor user compliance and Key Performance Indicators and embed cybersecurity as an intrinsic part of the corporate culture.

Technology: we scan and isolate malicous attachments and email content and provide system administrators with "one-click" management across the enterprise.

PennAware improve overall organizational security posture and mitigate cyber-risk by;

- Real-time analysis and management of email-borne threats
- Threat simulation designed to test the organizations' security posture.
- The availability of timely threat intelligence
- Realistic, but safe, phishing simulation
- Supporting security awareness training programmes

Our internal corporate strategy creates a stimulating and innovative environment where the PennAware team has the opportunity to continually enhance their skills and creativity while contributing to growth.

pennAware

www.pennaware.com
info@pennaware.com
@pennaware