WHAT IS THE BUSINESS CASE FOR MSSP?

The National Institute of Standards and Technology (NIST) advises that similar to financial and reputational risk, poorly managed cybersecurity risk may negatively affect performance and place an organization at risk by reducing its ability to innovate. Decision makers and executives are repeatedly experiencing losses due to their inability to be fully knowledgeable about properly managing cybersecurity risk and complying with guidelines of the established frameworks (such as following some of the key elements of the NIST Cyber Security Framework).

Leaders of companies, big and small, recognize that security plans must be created, implemented and continuously updated to protect an organization's basic requirements in areas including (but not limited to) technology, processes and user awareness. The key question is whether to manage these risks in-house or outsource (transfer risk or share mitigation) to a managed security-as-a-service provider (MSSP).

LYNX TECHNOLOGY PARTNERS

+1 (800) 314-0455 | www.LynxRiskSolutions.com

OVERVIEW

This managed security approach transfers the expense and management of 'in-house' security to a third party having existing expertise and capabilities. But, the struggle arises in how to decide if an 'in-house,' on premise, security management program is effective enough? What is the cost-benefit analysis when deciding to budget expenses for in-house verses out-sourcing? Organizations (big and small) desperately need a quick reference guide for deciding how to manage and implement their security program.

The proposed MSSP "Scorecard" provides an outline that helps an organization better understand if there may be a competitive advantage for them in choosing to outsource to an MSSP. It also serves as a resource that aids in calculating the Return on Investment (ROI) of this decision. This "scorecard" approach considers how cyber security investment decisions map directly to managing business priorities. An organization examines the priority and value associated with having consistent operations that are associated with their networks, software, hardware, and data. Hence, depending on your threats, specific strategies will differ. For example, an industry affected via unintended disclosure may devote more attention to stricter access control rather than a more robust logging and monitoring architecture.

Executive leaders should first conduct a quick self-assessment to help decide which cyber risks to accept, transfer, mitigate, or avoid; a framework to validate the financial incentives in information security management. As the perceived threat has risen, companies must either build in-house security expertise or outsource as a response. In this white paper, we outline a process to assist in making a business case for or against the MSSP route and provide a checklist to help simplify the decision-making process. This paper will address three approaches, in-house security, partially outsourced security, and fully outsourced security.

CONTENTS

1 **CONDUCT AN INTERNAL SELF-ASSESSMENT – WHAT IS THE THREAT?**

What is the threat to my Cyber Domain?

2 **WHAT CHOICES DO I HAVE TO MITIGATE THE THREATS?**

Cyber exposure extends throughout the organization, adding risks to successfully achieving multiple business objectives.

3 **SCORECARD – IS AN MSSP A GOOD FIT FOR ME?**

Help identify if your current process is providing the value your organization requires.

4 **SCORECARD INTERPRETATION**

Review your aggregate scores from the perspective of two broad categories.

5 **CONCLUSION**

Security is one of the most important decisions you can make for your organization because security is a tradeoff with usability.

1 | CONDUCT AN INTERNAL SELF-ASSESSMENT – WHAT IS THE THREAT?

WHAT IS THE THREAT TO MY CYBER DOMAIN?

WHAT ASSETS DO I NEED TO PROTECT?

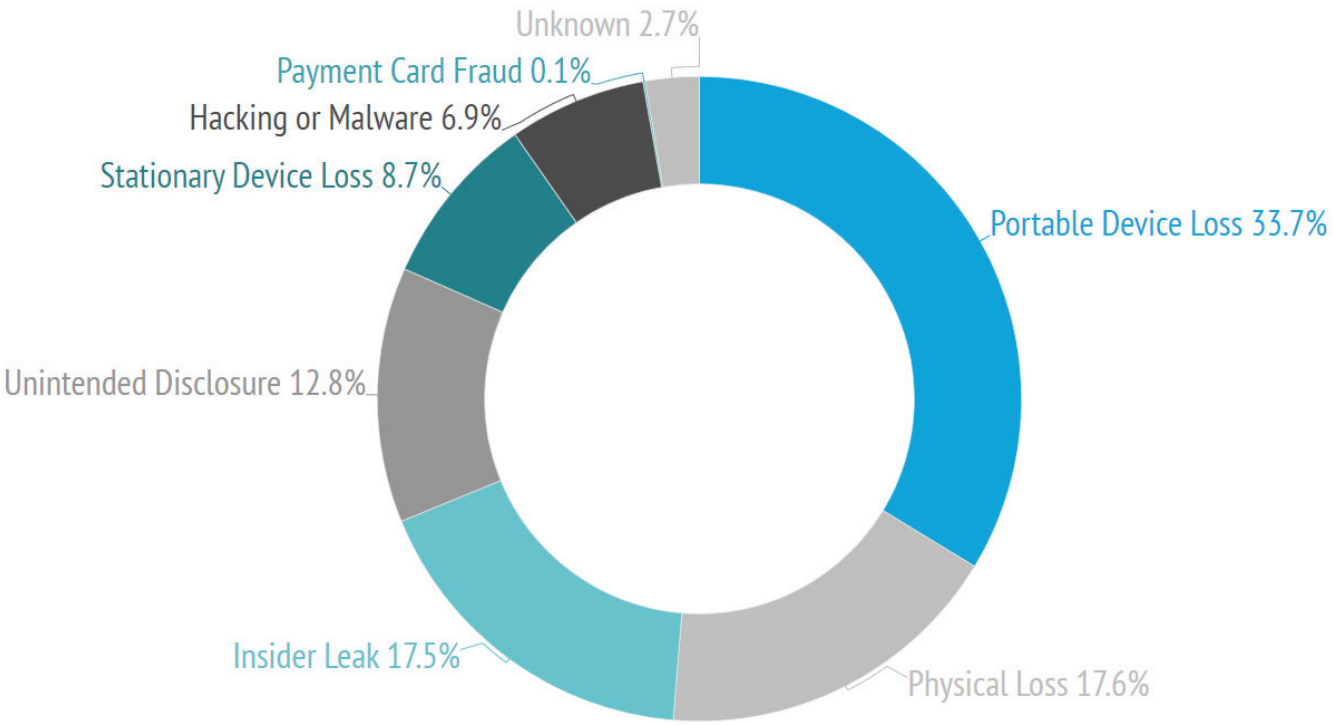
WHAT IS THE COST OF LOSING AN ASSET?

Cyber-attacks cost U.S. enterprises $1.3 million and small and medium-sized businesses $117,000[1]. Sector by sector, businesses are faced with a unique prioritized set of cyber threats[2]. Your organization cannot afford to have positions unfilled in cybersecurity. An attacker can be on the network for 5 or more months undetected, all while you're trying to staff your security division. Finding a latent threat on the network (cyber threat hunting), is far harder than setting up adequate defenses in the first place to make sure your organization isn't the "low-hanging fruit". Per FireEye's M-trends 2018 report[3], an attacker is present on internal networks for an average of 3 months.

[1] https://usa.kaspersky.com/about/press-releases/2017_kaspersky-lab-survey-cost-of-cyberattacks-for-large-businesses-in-north-america
[2] https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-analyzing-breaches-by-industry.pdf
[3] https://www.fireeye.com/content/dam/collateral/en/mtrends-2018.pdf

Depending on your sector, you face a different cross-section of security threats. Trend micro shines some light on this; for example, the healthcare industry faces the following threats:

HEALTHCARE INDUSTRY THREATS



As this graph suggests, your interal assessment should outline what your biggest threats might be and what or how you will protect your critical assets. Also ask yourself, what is the cost of losing an asset?

https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-analyzing-breaches-by-industry.pdf

2 | WHAT CHOICES DO I HAVE TO MITIGATE THE THREATS?

Cyber exposure extends throughout the organization, adding risks to successfully achieving multiple business objectives. Managers then quickly encounter the challenge of selecting from an increasing number of security controls that can be brought to bear. Moreover, merely collecting an inventory of access to all data and IT related assets may not be feasible with the proliferation of expanded connectedness of smart devices, smart supply chains, smart cities and 24/7 data accessibility.

Yet, cyber security prioritization and investment strategies may differ from industry to industry. Small, medium and large sized companies all face similar concerns, yet the conditions, constraints, and structure may mandate a different set of decisions. Focus will also depend on your competitive advantage and the intellectual property you consider most valuable to your organization. Additionally, compliance standards such as HIPAA and PCI-DSS can dictate required behavior. It is important to look at what companies in your sector and across others do. To stay secure involves avoiding being the "low-hanging fruit" given your assets.

And so, managing security prioritizing and keeping up with security threats continues to be daunting. Even once you have a rough idea of your company's concern levels, you then ask how to manage the security –mitigating threats, protecting networks and data, preserving consumer trust and privacy, and compliance with regulations? Finally, you need to decide whether to manage all this in-house or outsource? Key considerations include:

1

Developing your in-house security requires spending time and resources such as:

1. Specialized technical expertise
2. Specialized toolsets for detection and protection, such as firewalls, intrusion detection, scanning software, mitigation, monitoring and altering system

2

Managed security service providers (MSSP) - Outsourcing security services.

In Economics of Information Security and Privacy, the authors explain that traditional research dictates MSSP outsourcing be done if it provides a quality or cost advantage. However, in the case of a perceived risk (existent or not), firms may outsource even if the MSSP doesn't provide a quality advantage[4].

The following section provides a quick scorecard to guide you through a personalized decision-making process for managing inhouse or outsourcing the protection of your systems.

[4] https://books.google.com/books/about/Economics_of_Information_Security_and_Pr.html?id=PsLKmEQdRuAC

3 | SCORECARD – IS AN MSSP A GOOD FIT FOR ME?

The answer given to the question "why I need an ongoing partner who will provide security-as-a-service?" tends to be "I do not have resources in house to do this effectively". But, what process or metrics assisted in making this decision?

Remembering that cybersecurity and risk are intertwined and dynamic in nature, we suggest you start by identifying the areas of your programs which are most critical to your mission and organizational objectives and what level of risk you currently may have towards achieving the objective. This will help identify if your current process is providing the value your organization requires.

3 STEPS TO IDENTIFY IF YOUR CURRENT PROCESS IS PROVIDING VALUE

STEP 1

Lynx Quick Tip Check List (Ref) is a great reference guide for beginning the process of creating your IT risk program (it follows some of the key elements of the NIST Cyber Security Framework).

Review the following checklist for a high-level overview of the steps to consider when creatng your IT Risk Program.

A copy of the Lynx Quick Tip Check List is included in this paper.

CSF QUICK TIP CHECKLIST

This document is a quick reference guide for creating your IT risk program following some of the key elements of the NIST Cyber Security Framework.

Identify

The organization identifies its mission objectives, related systems and assets, regulatory requirements, and overall risk approach.

Create a Current Profile

Beginning with the Categories specified in the Framework Core, the organization develops a Current Profile that reflects its understanding of its current cyber security outcomes based on its implementation of the Identify Function.

Conduct a Risk Assessment

The organization analyzes the operational environment in order to discern the likelihood of a cyber security event, and the impact the event could have on the organization. It is important that critical infrastructure organizations seek to incorporate emergent risks and outside threat data to facilitate a robust understanding of the likelihood and impact of cyber security events.

Create a Target Profile

The organization creates a Target Profile that focuses on the assessment of the Framework Elements (e.g., Categories, Subcategories) describing the organization's desired cyber security outcomes.

Determine, Analyze, and Prioritize Gaps

The organization compares the Current Profile and the Target Profile to determine gaps, and then determines resources necessary to address the gaps. The organization creates a prioritized action plan that draws upon mission drivers, a cost/benefit analysis, and understanding of risk to achieve the outcomes in the Target Profile.

Implement Action Plan

The organization implements the steps defined in the action plan and monitors its current cyber security practices against the Target Profile.

Three Keys to Remember:

1

Risk is the context in which you apply your security program. It is the language that business will understand. The foundation of a risk program is based on the controls, which in turn are influenced by regulatory and statutory mandates.

2

Be careful with absolutes, as risk is about gray areas – probability X impact. Probability by it's nature is often qualitative; Impact can be quantitative, but at some point, you'll always have to make a best guess backed by the facts at hand. So don't be afraid to use both methods to communicate risk. But no matter how you calculate risk, keep it simple.

3

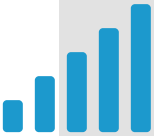
The CSF is just a framework – think of a house and the blueprint/framework that guides the structure of the house, but not the make-up. The walls can be stone, brick, wood, or compound materials – these elements can be customized to your needs. Similarly, the elements of the CSF will vary by each organization's specific need, and you will have to customize these to your use cases.

STEP 2

The checklist from Step 1 and the following questions should spark the process of considering big-picture aligned security questions with respect to your IT risk overview from Step 1. Each of the questions below include a case example for reference.

What security needs are necessary to achieve my company's primary business objectives?

Example: I am a large-sized organization with revenue streams that are data-intensive and depend on customer data. My biggest concerns are data theft and leakage of our unique analytics platform. I have IT security staff, but not enough to meet my needs. My most pressing needs are continuous monitoring, and potentially some assistance with migrating firewalls/ids/etc.



What level and scale of service is necessary to meet my organization's security policy requirements?

Outline your basic risk assessment and security policy.

Example: While we meet most of our risk management objectives, recent assessments have shown some gaps or areas of improvement. I would like to mitigate or transfer additional risks in the areas of spam/phishing protection and hardening our newly implemented VPN concentrators on multiple sites.

What is the level of the organization's cyber threats/risk concerns that threaten the objectives listed in question 1 above?

Example: I perceive a medium cyber threat level. One of our employees has recently fallen victim to a phishing email which resulted in an increased in attacks against our networks.

What are the threat levels when reviewing an inventory of your assets and necessary security architecture?

Example: After examining assets we found 400 endpoint desktops devices (low), 10 cell phones (high), 100 user laptops (medium), 10 management/executive laptops (high). On our development server 3 virtual machines with source code and sensitive user data (high).

To assist with framing the answers to the broad considerations above, consider the following which will guide alignment of security management needs from the perspective of your core business objectives. Keep the following operational and strategic level requirements in mind (which apply to your organization) as you complete the following MSSP Scorecard:

SECURITY OBJECTIVES

FROM THE PERSPECTIVE OF THE EXECUTIVE MISSION

1. Risk and Compliance Management (RCM) Requirements

a Financial Obligations (SOX)
b Customers (GLBA, PCI, GDPR)
c Human Resources (HIPAA)
d Policies and Procedures

2. Threat Intelligence and Incident Remediation (TIIR) Requirements

a Networks
b Cloud Services
c IOT
d Mobility – 24/7 Availability
e Enterprise Systems

3. Security Asset Management and Monitoring (SAMM) Requirements

a Completing Evaluations/Risk of your Vendor list
b Deploy, Configure and Manage security technologies and infrastructure

4. Security as a Competitive Advantage

a Creating Unique Solutions that only your company possesses?
b Customers' Trust
c What are Competitors doing? Industry standards.
d Getting new customers requires security

STEP 3

The MSSP Scorecard provides a high-level guide for decision making based on your organization's individual needs (use the key that follows and follow the question-by-question instructions to help you formulate your score for each question).

Question	1	2	3	4	5	N/A
1. What level of threat do I perceive my organization to be under?						
2. What is the size of my network?						
3. How much sensitive client-data do I handle?						
4. How much valuable intellectual property data do I handle?						
5. What are my cost of downtime, customer loss and other expenses due to attack?						
6. How big is my security budget relative to my risks?						
7. How well does my current security architecture meet my needs?						
8. Do I need specialized security technical expertise?						
9. What are my costs to maintain multiple tools such as firewalls intrusion detection and scanning software?						
10. What are my current costs/maturity model to manage and mitigate threat vectors?						
11. What is the size of my organization?						
12. How do I compare to my competitors?						
Total Value						

1	2	3	4	5
LOW		MEDIUM		HIGH

1 What level of threat do I perceive my organization to be under?

Considerations: Consult with your IT department to determine this rating.

Low - Regular scanning of internet, general phishing attempts
Medium - Lower level attacks (i.e. phishing/spearphishing) in abundance, Attack patterns in Web Application Firewall (WAF) logs. Perceived high level of company-owned mobile/portable devices connected to potentially unsecure networks. Indicators of additional probing.
High - Suspected or known targeted attacks. Otherwise, known organizational shortcomings: Insufficient code review, Unpatched devices or devices past End-of-Life (EOL) support. Exposed Amazon S3 buckets, etc.

2 What is the size of my network?

Considerations: Remembering there is no such approach as one-size-fits- all in the realm of security. The higher the number of links you have in the network, the more vulnerable and the more expertise needed to protect the network.

Low - Only client machines - all services managed by cloud providers.
Medium - Managing multiple linkages: security of networked databases, servers, APIs, Internet security
High - Managing all linkages across organization: network and IT components, databases, cloud servers and endpoint security. Many points of entry into your network.

3 How much sensitive client data do I store?

Considerations:

a. May be measured in # of data records multiplied by sensitivity (i.e. credit card information, etc). This can then be subjectively aligned with the 5 levels.
b. Keep in mind the compliance and regulations within your industry when it comes to data protections.
c. Higher cost if mandatory expenses like regulatory compliance and budget out the annual cost of staffing the positions you have created to handle this task.

Sample record sensitivity levels:

Low – Basic information: names, email addresses, password
Medium – Credit Card information, addresses, attributable usage information/statistics
High – Personal Health Records, Detailed financial information, etc.

4 How much valuable intellectual property data do I handle?

Considerations: What level of digital/technological assets do I have? Measured in estimated approximate dollar value.

Low – Administrative/Financial data.
Medium – Detailed user accounts/records, digital content libraries, software (i.e software engineering firm)
High – Highly Proprietary Research/Valuable Software, High risk medical devices (i.e. Life support)

5 What are my cost of downtime, customer loss and other expenses due to attack

Considerations: What is probability that attack would create downtime? Which is less costly - be compliant and have less downtime in long term, or savings short term?

Low – breaches will be rare and do not create customer loss or major expenses
Medium – breaches and downtime create losses, but can recover quickly from them
High – consumer confidence would be shaken and downtime create loss in revenue in short run and major issues in long run

6 How big is my security budget relative to my risks?

Considerations: IT spending to revenue ratio (Subjective estimate)
- Small companies spent 7% of revenue
- Midsize spent 4.1% of revenue
- Large spent 3.2% of revenue

Low – I need more money to adequately handle risks
Medium – I am not managing all risks as I'd like to
High – I can comfortably manage cyber risks

7 How well does my current security architecture meet my needs?

Considerations: Point values can/should be adjusted for more granularity.
Consider known attacks, detection time, known gaps in security solutions. Also, improperly mitigated risks or an incomplete risk modeling.

Low – Needs overaul
Medium – Could use improvement in certain areas but meets regulation.
High – Satisfied with current ability to meet regulation, maintain security

8 Do I need specialized security technical expertise?

Considerations: What sort of assets do I need protected? Do I need this expertise full time or part-time? How crucial is the asset (for which the specialist is needed to protect) to my organization?

Low - IDPS, Firewalls, Endpoint Protection, Patch management
Medium - Extensive MDM/mobile device security, web-centric business, compliance audits
High - Custom Web/Mobile Application penetration testing, additional on-site consulting

9 What are my costs to maintain multiple tools such as firewalls intrusion detection and scanning software?

Considerations: Measured as a percentage of IT budget

Low - 0-6% of budget
Medium - 8-12%
High - 15% or more

10 What are my current costs/maturity model to manage and mitigate threat vectors?

Note: this will determine how easy it is to transfer current solutions to an MSSP.

Low - Out-of-box security solutions employed, occasional consulting
Medium - Employ security professionals in addition to IT professionals
High - Established infrastructure (i.e. SOC), Security leadership employed

11 What is the size of my organization?

Number of Employees – How many endpoint users are within the organization (think of how many individuals touching high level data, which increases your risk)

Low - Small size company (i.e. <50 employees)
Medium - Medium size company (i.e. <250 employees)
High - Large size company (i.e. >250 employees)

12 How do I compare to my competitors?

Considerations: Within your industry, what percent of companies use MSSP? What other information can be informally gleaned about competitors' security posture after attending conferences, presentations, etc.?

Note: According to Trustwave's 2018 Security Pressures report, 33% of respondents partner with an MSSP and 45% plan to in the future[5]. This appears to make sense given the model and the increase in network attacks in the past few years.

Low - Significant perceived gaps in security measures comparatively
Medium - On-par with other companies
High - Have additional measures (tools/procedures/policies) in securing client/company data, as compared to other companies

[5] https://www.trustwave.com Company/Newsroom/News/New-Trustwave-Report-Uncovers-Key-Drivers-Steadily-Increasing-Cybersecurity-Pressures/

4 SCORECARD INTERPRETATION

Total your score and review your aggregate or average scores from the perspective of these two broad categories:

1: Cost-of-Service (CoS) Metric Perspective Questions

How valuable is the sensitive client data that I store?
Note: both sensitivity of data and amount of records are relevant

How valuable is the intellectual property data I store?
Note: both the quantity (i.e. large sets of mined data) and uniqueness (custom software, etc) can be considered

My cost of downtime, customer loss and other expenses due to attack
What standards am I required to comply with? (HIPAA, PCI-DSS, SOX, GLBA, GDPR, etc)
Note: the metric can be thought of as "cost of compliance"

How well do I perceive my budget to meet my needs?

2: Quality-of-Service (QoS) Metrics – Effectiveness

How well does my current security architecture meet my needs?
Note: How quickly do I need a secure solution implemented?

Do I need Unique specialized security technical expertise?
What is my timeline for a secure/compliant environment? This takes into consideration the recruitment and potentially lengthy onboarding period for your new employees. Consult with HR for a more detailed answer. Contracting out security will have a shorter "spin-up" time.

Ability and cost to maintain multiple tools as firewalls, intrusion detection and scanning software?
Note: threat runs the spectrum from automated attacks/scans against a weak/out-of-date system to targeted attacks against a hardened system. Notably, automated scans/attacks vs a hardened system would not affect the score of this metric.

How important is active 24/7 monitoring?
How important are on-premise/accessible security staff?

THE DECISION

An organization can take on more risk (based on the risks you high-lighted above) by choosing the lower quality coverage, with the expectation of some medium to long term gain (either shift budget to operations or use it to train your security team). You can take on less risk by choosing the higher quality coverage, ensuring more peace of mind.

Interpretations of scoring include:

- IF average scoring of Cost Metrics is low – medium, review options which may be less expensive, possible in-house solutions
- IF average scoring of Quality is Medium - High, you should focus on outsourcing for expertise and having continuous high quality security, possible MSSP solution

Two sides of this are:

- Can I get higher quality coverage for the same cost with an MSSP?
- Can I get lower cost coverage with the same quality with an MSSP?

Using your score and potential decision considerations above, review each MSSP and In-House option as it aligns with your answers and scoring.

THE MSSP OPTION

Much has been written about the benefits of an MSSP, especially if you are a big organization, since it allows for a consistent, centralized, and transparent view into your organization's security platform. One aspect common across industries is that although the organization still owns information security risk and business risk, contracting with an MSSP allows them to share risk management and mitigation approaches.

MSSP assisted secure operations provide a competitive advantage through:

1. Experience

- Allows you to defer your cyber risk management to a resourceful, fully functional third party with labor, expertise and up-to-date toolsets.
- MSSP has the experience working with other companies in your sector, transferring that knowledge into your tailored solution takes the guesswork out of architecting an appropriate solution.
- Security and risk management leaders struggle to attract and recruit qualified, experienced personnel with expertise to properly managed risk & compliance.

2. Availability

- For the right price, MSSPs potentially provide flexible 24/7 monitoring and a range of tailored services to satisfy organizational needs from remote device management, to SOC services, to penetration testing.
- MSSP eases the burden of recruiting and retaining the right cyber security staff. It's hard to recruit qualified candidates when there is 0% unemployment in Cyber Security.

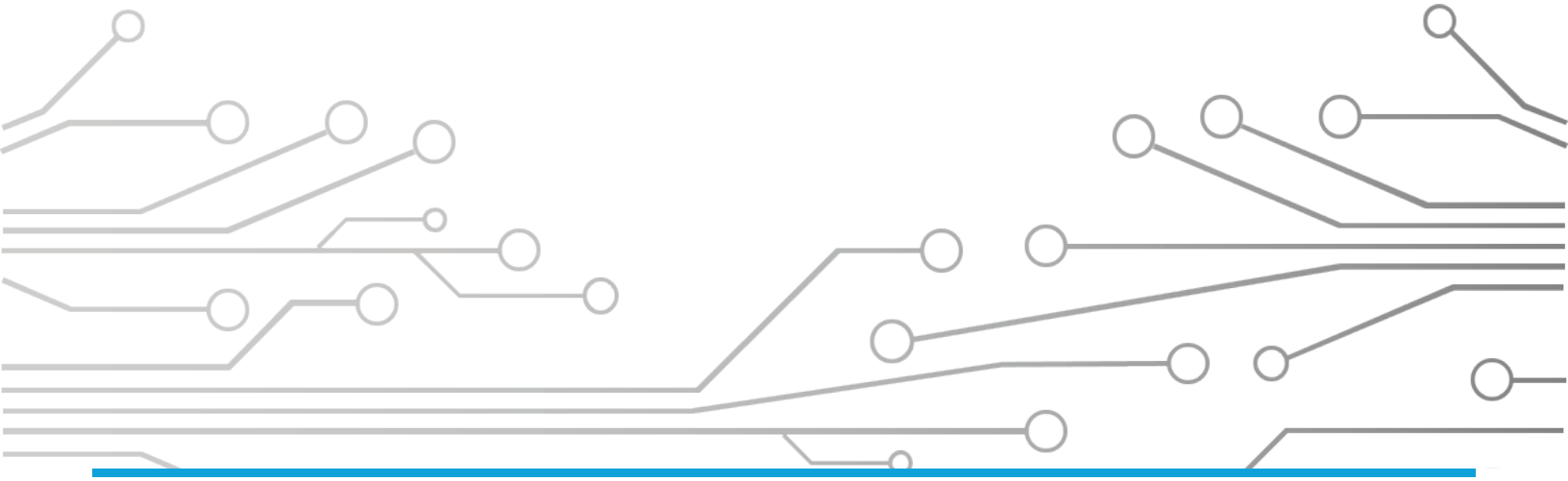
3. Cost savings:

- Think of it as an investment towards a unique selling point, not a mandatory cost.
- Calculate the cost breakdown for each employee in the security team vs an MSSP
- Time is money: In the time you assemble the right in-house security team, you may have already been breached.
- Customer trust in your security brings in revenue. Marketing your company's strong, experienced security and protections is a competitive strategy.
- Your Insurance companies may not cover your cyber breach data and IS loses if YOU were not compliant with set security standards and regulations, of which an MSSP would absolutely be aware to implement.

WHY NOT CHOOSE AN MSSP?

Unfortunately, the decision isn't entirely straightforward--there are potential risks associated with outsourcing. A few big questions to ask are:

- Do you want to retain control over sensitive data/intellectual property?
- What tasks will they handle? What won't they handle?
- Is it a single point-of-failure? What will happen in the event of the MSSP going under? Will your data be securely disposed?
- How fast are we growing? Will it pay off in the long run to start an in-house security team if it's in your future anyway.?
- Are you comfortable with the risk of entrusting some or all of your most valuable data to a third party?



5 | CONCLUSION

There is No "one-size-fits-all" MSSP out there. You must calculate your ROI for using an MSSP. Consider interviewing and getting advice along the following:

- How are you assessing if the security team of the MSSP is experienced enough and do they have all the tools to meet your needs?
- Is the MSSP you are selecting remaining current with new threats and cyber-attacks – potentially guaranteeing a level of accuracy in informing real-time actionable alerts which will assist YOU in making business decisions (Remember, company leaders make the response decisions)?
- Your security professionals (your MSSP) must understand how security relates to the organization from the perspective of the executive mission/objectives.
- Do they provide a tailored solution specific to your needs?
- What is their overall reputation?

Shop around for quotes from various MSSP providers. Account for differences in their services provided and what you would be able to do in-house.

The final decision should incorporate the perceived mitigation of the weighted risks. While the NIST Cyber Security Framework is a good starting point, industry-specific guidance is available and should be used when tailoring a security program[6]. Architecting a proper security program and staffing security personnel can be a daunting task.

One might envision the decision as wrestling between losing control over digital assets and an in-house model with holes in coverage. Fortunately, outsourcing security is not a binary decision, many companies choose to use both in-house and managed services together.

Security is one of the most important decisions you can make for your organization because security is a tradeoff with usability. A bad security program will not only allow threats in, but also hurt employee productivity/company growth.

If you would like help interpreting your scorecard or just want to discuss your security and risk programs, contact Lynx Technology Partners today. You can also visit our website at www.LynxRiskSolutions.com for tools and resources or to schedule a call with one of our security experts

[6] https://www.nist.gov/cyberframework/general-resources