IJICTR
International Journal of Information & Communication Technology Research

Volume 11- Number 1 – Winter 2019 (57 -70)

A Novel Maturity Model for MSSP Assessment

Mohammad Gholami Mehrabadi
Ph.D. student of Industrial Management, Faculty of Management and Accounting, Shahid Beheshti University, Tehran, Iran
Mo_gholami@sbu.ac.ir

Massoud Kassaee
Assistant Professor, University of Shahid Beheshti, Tehran, Iran
massoudkass@yahoo.com

Abouzar Arabsorkhi*
ICT research institute, Tehran Iran
abouzar_arab@itrc.ac.ir

Received: 25 August 2018 - Accepted: 17 December 2018

Abstract **Nowadays growing threat and security risks in information and communication technology and also increasing use of information and communication technologies are two main decision makers for organizations, service providers and the general public. Resource limitation and the lack of expert in cyber security have made lots of major challenge for different service providers in dealing with and managing security threats. In many developing countries, this problem has been solved using Managed Security Service Providers. Managed Security Services are network-based security services that are outsourced by a trusted third party. The diversity of Managed Security Service Providers affects the effectiveness and efficiency of decision making in this area. Therefore, in order to outsource the security services, the assessment of these organizations is inevitable. This assessment can be done by various mechanisms. One of the acceptable strategies in the security is the maturity model. Maturity models are step-by-step solutions to grow organizational capabilities Along with a predicted, desirable, and logical path. In fact, maturity models provide standard way to assess process maturity along with business process improvement. Until now, no maturity model has been developed to assess the Managed Security Service Providers. Therefore, in this paper, we have proposed a novel model to external evaluation of the Managed Security Service Providers based on maturity model. The evaluation of the proposed maturity model is based on multiple case studies. We have optimized our proposed model by using these case studies in three different MSSPs.**

Keywords- Maturity model;MSSPs; Assessment; maturity factors;Security maturity.

I. INTRODUCTION

Today's world is moving forward to networking and electronics. This trend is reflected in variety of sections, including banking, finance, government services, and many other critical infrastructures. Cost and time savings, fast pace computing and thousands of other benefits are the main reasons for moving toward electronic world [1]. The amount of ICT investment in 2018 was more than $4 trillion [2]and estimations show that this number may increase to more than $6 trillion in 2022 [3][2]. By enhancing the technologies in cyber penetration and increasing the skill of security attackers, it can be seen that security organizations and groups are always a step behind the attackers [1].In fact, since the threat agent acts as an external element outside of control, security concerns always exist. Increasing threats in cyberspace and information infrastructure make the security and safety issues as the main concern of business executives. Increasing amount of financial investments is the good evidence for this issue. Based on Gartnerin 2017, global security investment was about $102 billion, and in 2018 it was $114 billion Based on [4] [5] and it will increase by more than $205 billion by the year 2024. On the other hand, the cost of security attacks in 2017 was $600 billion [6][7].This trend represents that cybercrime attacks are drastically increasing and it highlights that defeat against cyber threats requires not only cost but also special decision making and control. Due to the importance of security,

* Corresponding Author

organizations can take three different approaches as: 1) internalization, 2) outsourcing, or 3) the combination of these two methods [8].The emergence of novel technologies -such as cloud computing, the Internet of Things, big data, cyber-physical systems, quantum computing and their widespread use in industries. Executives have concluded that securing their systems using their own resources is not feasible. So, outsourcing of information security and its related services is a feasible and better solution for organizations [9] there are many other reasons for outsourcing such as lack of funding and security experts [8][10], high demand from customers for the use of managed security services, increased access to and compliance with cloud computing ,IT services, defence in depth implementation problems [8], maintenance costs [8][11][10], Covering new security requirements using a 24/7 model and increasing the focus on security [10].

Security service providers have designed new solutions to identify and address advanced cyber threats resulting in a market for cyber security services [11].These suppliers have efficient hardware and software capabilities along with specialized services and solutions to deal with security threats. These services and solutions are known as cyber security components. With increasing security threats and security implications in cyberspace, active companies in this area are focusing on reducing their costs [1][12]. Cyber security market consists of three basic components: 1) training, 2) consulting, and 3) security management services. On the other hand, this market has two managed and specialized components. Managed security services allow the provision of solutions without the need for expert and security hardware [1]. The global market is estimated to reach $ 61.4 billion in 2024 from $16.8 billion in 2014 [13].In general, the cyber security market is expected to grow more than 10% by 2023 [14][15]. Managed security services market can be categorized by type, security maintenance methods, organization size, deployment status, and security areas [1].Suppliers provide a variety of cyber security services in this area. These services can be classified in governance and security consulting [16][17][18], access control [19][16], malware protection [19][20], web security [19][20], firewall [19][20][21], applications [16] mobile security [16][21], endpoint security [21][20], data security [16][20][21], and etc. services. Over the years, managed security services diversity has been accompanied by the increasing number of suppliers of these services.

Utilizing the benefits of outsourced managed security services depicts the importance of cyber security service provider selection. The organizations will face a lot of problems if they make mistake in the case of MSSP selection. Hence, the assessment of the capabilities of these organizations is inevitable [9]. Some assessment parameters are as following: the operational ability [9], comprehensive services [22][23], the expertise and skill [22][23][24][25], the reputation of MSSP [22], the robustness of web-based management tools, Advanced back-end technology[22], multi brand support for different security agencies [22][23], guaranteed and flexible performance based on SLA [22][25], financial stability [23][22], capabilities of services in life-cycle [25][24], presence in different geographical regions [24], development strategies [24], accessibility [25], etc. Measuring these capabilities for a regulator that is responsible for issuing a certification service provider is also vital. In general, for the use of managed security services, two categories of questions must be answered:

- From the customer viewpoint, what companies are the better providers?
- From the Regulatory viewpoint, what companies have the qualifications to work in this market?

security assessment means testing a system to determine its compliance with a security model, standard, or specific features [26]. The maturity model as an evaluation and decision support mechanism can help in this regard to meet the different needs of the two previous mentioned groups. To sum up, this model is a process improvement approach based on a process model. Process Model is essentially a structured set of operations and exercises that improve over time [35][32].The main purpose of maturity models is to determine the stages of the maturity roadmap, which includes the characteristics of each stage and the logical relations between them [34].

Up to now, different definitions have been proposed for the maturity models [27][28][29][30][31][32]. In general, the maturity model is a structured set of elements that describe the characteristics of an influential process and create a space to start benefiting from previous experiences, creating a common language and vision in the organization [27][28]. Capability Maturity Model (CMM) was first introduced in the mid-1980s by the Software Engineering Institute (SEI) [33]. Other references have introduced other models that differ in the number of levels or level definitions, while preserving the comprehensiveness of the basic maturity model. Maturity models cover vast areas and field including software engineering, system engineering, project management, system management, staffing, and information security services [34].Each of these cases is considered in this paper, and analyzed according to the requirements of the maturity model. Consistency, cost saving, satisfying business/performance demand and process improvement are some of the most highlighted benefits of using maturity models to assessment or improvement of a business.

In This paper, we introduce a novel maturity model to measure the managed security service providers. The proposed maturity model can be used as a mechanism for external evaluation of MSSPs and their continuous improvement. In the following, the background of the research is first presented, then the research objectives and innovations are explained and then the research method is examined. Finally, the proposed method is thoroughly assessed and the results evaluated.

II. RELATED WORK

A. *The ICT infrastructure development and the growth of security threats and investments in this area*

The presence of information and communication technology in Society and business is undeniable. The

applications of information technology in businesses have led organizations to take advantage of this platform as a competitive advantage [36][37][38]. IT market revenue will increase from 2,037€ billion in 2011 to 4,460€ billion in 2019.This growth reflects a dramatic increase in the size of the information technology market [38]. Enhancement in the use of IT services in one hand and the dependency of a large part of the software and hardware assets on this platform, on the other hand can cause the increase of attacks and threats in this area [1][12]. In countering cyber-attacks Organizations and countries investment have also increased significantly [39][40]. McAfee reports depicted that the number of malware in the first quarter of 2018 has risen by almost 30% since the first quarter of 2017 mostly Zero-day attacks [41][41][42]. Based on Gartner [43] the amount of organizations investment in information security has increased by more than 8% in 2018 compared to 2017 [4].

Customers of a company will be more likely to use the platform in case of 24*7 user access capability to organization systems. Also, offering different systems to create a competitive advantage or customer satisfaction cause to increasing the complexity of IT systems in organizations [44] that requires a very high level of security and needs cost, human resources and significant equipment in security services [45][46]. Outsourcing the security services can help organizations to overcome these issues [47]. Moreover, the organizational needs in security and services offered in this area are different. Different definitions for security services are provided [48-53]. Definitions show that security services can cover security requirements and policies and are implemented by security mechanisms. Based on NIST 800-35 [52] security services can categorized in technical, operational and management groups. In other viewpoints, categorization is based on security features [52-60].

B. The needs for security outsourcing and the emergence of managed security services

In 2017, due to the difficulties and limitations in organizations, roughly 45% of organizations have outsourced the security of their information resources [61]. 59% of outsourcing was for IT security, 37% for disaster recovery, and 9% for the security service desk [62]. Some problems in organizations that show the needs for outsourcing including financial limitation and human resources [62][63][64], lack of monitoring facilities [63], and resources shortage [62][63][64].

Managed Security Services (MSS)mean network security services that are outsourced by their organization, and managed and delivered by trusted third parties [65][52]. In other words, managed security services are a systematic approach to managing the security needs of an organization using another security company. These services may be internalized or outsourced to other Managed Security Services Provider (MSSP)[52][53].Indeed, MSSPs are third parties that provide security services for other companies[65][52][53]. Different definitions for MSSPs are provided in [65-69]. A quick look to managed security services leads us to optimized service management, security services hosting, service delivery insurance mechanisms and outsourcing security services. According to Gartner [71], the managed security services market grows by 9.5% and earned $10.3 billion in 2017. The market share in 2018 was $ 24.7 billion [72].The market share is expected to increase 14.7% CAGR by 2025[73][72][52]

Based on MSSP market increasing, nowadays, thousands of MSSPs are introduced in the world. By increasing the number of providers, the competition among the marketplaces to attract customers is raised. Different organizations use some methods and indicators to assess MSSPs. For example based on IDC Marketplace some competitive advantages that can attract the customer are price, service types, service delivery time [84][85], and reliability [86]. On the other hand, small businesses that cannot provide such services for the customers will inevitably be eliminated or at least be excluded from competition [87]. Based on Fortinet, Competitive cost, innovative [88][89] and wider service [23][90] are among the assessment indicators of MSSPs. In general, Gartner introduces two categorizes to assess suppliers and MSSPs: 1) completeness of vision and 2)ability to execute [9].

In order to evaluate a MSSP, stakeholders should be able to use an appropriate assessment mechanism. An effective assessment mechanism requires suitable and right measures. Assessment of MSSps, just based on their current state (as mentioned in previous paragraph) cannot assess the supplier's progress. To overcome this lack of ability, the maturity model is one of the standard methods for evaluation. The maturity model is a set of operations and processes that improves over time to help businesses to reach their [91][33]. Until now, to the best of our knowledge, there is no security maturity model for MSSP assessment. The base maturity model was first introduced in the mid-1980s by the Software Engineering Institute (SEI) at the University of Carnegie Melon [91][33].

C. The concept of maturity model as one of the decision support methods for MSSPs

The Capability Maturity Model (CMM), a comprehensive and leading model was first introduced by the Software Engineering Institute (SEI) of Carnegie Mellon University in 1987 [92][93].This model has five maturity levels, including initial, repeatable, defined, managed and optimized level. using this model, an organization can implement improvement measures to gradually achieve their strategic goals from an initial to optimized processes[94].Companies are expected to use this model to offer customized services, help them make better decisions and improve their market share. There is variety of definitions for the maturity model in different resources [27][92][95][33][32]. Numerous maturity models have been developed based on the basic maturity model (CMMI) [92][28][32][96] [92][32][97][98]. For example, some of the most well-known maturity models are ISM3, PRISMA. IBM ISF and C2M2 (Table I) [122-128].

TABLE I
EVALUATION OF DIFFERENT SECURITY MATURITY MODELS

Maturity model	indicators	Maturity Levels
Capability Maturity Model Integration (CMMI)	• System engineering • software engineering • product integration and process development, supplier organization	• Initial. • Managed • Defined • Quantitatively Managed • Optimized
Gartner Maturity Model	• Vision • Strategy • Metrics • Information Governance • Organization and Roles • Information Life Cycles • Enabling Infrastructure	• Unaware • Aware • Reactive • Proactive • Managed • Effective
Information Security Management Maturity Model (ISM3)	• evaluate the level of security maturity in an enterprise information system, improve information systems by gap analyzing and prioritizing the investment process	• Thread based 5 levels
PRISMA	• Information Security Management & Culture • Information Security Planning • Security Awareness, Training, and Education • Budget and Resources • Life Cycle Management • Certification and Accreditation • Critical Infrastructure Protection • Incident and Emergency Response • Security Controls	• Policy • Procedures • Implemented • Tested • Integrated
IBM ISF	• People • Data • Application • Infrastructure	• Basic • Proficient • Optimized
The Cyber-security Capability Maturity Model (C2M2)	• Risk Management • Asset, Change, and Configuration Management • Identity and Access Management • Threat and Vulnerability Management • Situational Awareness • Information Sharing and Communications • Event and Incident Response, Continuity of Operations • Supply Chain and External Dependencies Management • Workforce Management • Cyber security Program Management	• MIL0 to MIL3

Mostly, these models are developed for services, information technology and information security.The global economy conditions have created a difficult environment for decision makers. Effective decision making is based on accurate, comprehensive, timely and analyzed information. There are many models that are introduced to show various steps that should be involved in the decision-making process. The maturity model helps managers make better decisions to achieve the desirable situations. In this paper, we are going to address the proposed maturity model in the field of MSSPs by addressing the key success factors (CSF) and key performance indicators (KPIs) in the evaluation cycle.

III. GOALS AND INNOVATIONS

Due to increase in the number of MSSPs, the assessment of this business market is getting more curtail, because customers need to have measures to choose the best and most suitable option. Hence, the main objective of this study is to provide a method for evaluating MSSPs. Innovations of the proposed method can be addressed in two circumstances that described following:

- *knowledge creation:* using Multi-paradigm methods (Proof and Interpretation)
- *modelling:* introducing a novel assessment model foe MSSPs based on existing maturity models in other fields

To the best of our knowledge, there is no maturity model that has been provided to measure MSSPs. So in this paper, we provide a conceptual model of maturity analysis parameters for MSSPs. The purpose of this model is:

- Determine the measures for MSSPs to assessing their current position.
- Determine the method for decision making, based on MSSPs operations and developments.
- Provides a tool for measuring progress of MSSP based on their objectives.

IV. RESEARCH METHODOLOGY

This research is based on descriptive-exploratory methodology due to the application and method of collecting information. The method of this research can be studied in three distinct but interconnected sections. The first part of the study examines and analyses the

proposed model of maturity assessment parameters for managed security service providers. This section is based on related works. These researches were more qualitative and related to the subject of research, but none of them provided a framework and engineering maturity model in this area. Hence, the researcher used the Meta Synthesis (MS) method to organize the findings of the research in the form of a maturity model. To do this, researcher have used more than 200 papers. Since the performance measurement factors are based on the development of the maturity model, the meta synthesis method elaborates on key performance indicators (KPIs) and key success factors (CSFs), that can be evaluated and assess in the proposed model. Meta synthesis is a qualitative study method in which the information and findings extracted from other qualitative studies are examined with related and similar topics. This method represents a research that evaluates other research. Hence, it is referred to as "evaluation of evaluations" [130]. This method seeks to discover new and fundamental themes and metaphors using a systematic approach to combine various qualitative researches. Meta synthesis approaches improve the findings and provide a comprehensive view on various issues. This method integrates multiple studies into comprehensive and interpretive operational findings [131]. This method represents an engineering and refinement approach and focuses on integrating the results, the findings of existing research and existing studies. Therefore, the sample that is intended to use in Meta synthesis selected from qualitative studies and based on their relationship with the research question [132]. Due to the capabilities of this method, we have organized the findings related to the evaluation of MSSPs, and have represented the parameters of the maturity assessment in the proposed model.

To formulate the proposed maturity model, we studied a large number of reference models in different domains. At first we have used more than 200 papers for different maturity models in various fields. The main references for these papers were Scopus, ScienceDirect and IEEE. These papers have been filtered based on their citation, our goal and papers quality. Using these papers we have proposed our models' indicators and levels. Therefore, prior to the development of engineering maturity assessment model, the security requirements in the area of providing managed security services were selected from the perspective of the requirements development process. This model has been selected based on the measures named by Comprehensiveness, Application area, Usefulness and Simplicity [132][196].

In the first part of the research, the main question will be asked. In this regard, and in order to achieve the desired goal using the method of Meta synthesis, the following question is set:

"What are the main components of MSSPs maturity model?"

After that, we have used various search engines to carry out research activities based on well-known keywords. In the use of any search engines, one or a set of main resources may be evaluated and analyzed. Beside the search engines, we have employed lots of scientific papers databases. Each of these databases contains a number of valid scientific journals. In order to find out related articles about measures and decision-making indicators in the field of MSSPs, a specific set of these databases and valid journals listed within them were studied.

The next part of research is about reviewing and selecting the appropriate articles based on a set of indicators. Based on the selection criteria for the articles, the process of searching method and the selection of final papers is based on Meta synthesis. Throughout the Meta synthesis, the researcher reads selectively and finalized articles in order to achieve findings related to identifying key indicators of MSSPs performance. In the analysis and combination of qualitative research findings, the researcher seeks for topics or themes that have emerged among the selected studies and are related to the topics of the MSSPs performance or can be used to explain the components of the maturity model. After studying the related works, KPIs are identified, and then researcher can classify the subjects. This kind of analysis is essentially formulated in a single scheme.

The final issue in Meta synthesis is the qualitative control of findings about MSSPs performance KPIs. In order to select the articles, researcher has used a set of standard criteria in the process of Meta synthesis based on CASP-method. In addition, the researcher uses both electronic and manual search strategies to find related articles. Based on the above-mentioned set-up, we presented a model to assess MSSPs maturity using related work. As a result, we have presented a maturity model to map the indicators affecting the evaluation of MSSPs on maturity levels of security parameters in this space. In the second part of the research, the way of organizing proposed factors is considered in the form of MSSP assessment based on maturity model. Accordingly, the following question has been set:

"What are the levels of MSSP evaluation maturity model?"

In this regard, a comparative study is being conducted between the maturity reference models. This comparison is based on comprehension, application area, application rate and simplicity. Finally, parameters to assess MSSPs based on maturity model are defined based on the selected model levels and are presented in the final model.

V. RESEARCH FINDINGS

According to research methodology, the integration of models and frameworks of security requirements, from the requirements development process point of view, led us to Finding a set of factors and sub-processes of this area. The analysis of the selected articles is based on CASP method and their content analysis is based on the coding method. The results of the content analysis of these articles are presented below. Regarding to the theme analysis, we can categorize the indicators of this maturity model to four main sub-categories (Figure 1).

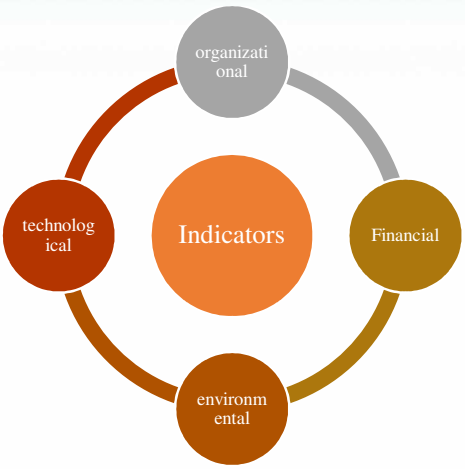

Fig 1. Indicators of Proposed Maturity model

A. *Organizational Category*

The organizational part of this maturity model is determined by the two main following factors: 1) Human resources profiles that represent the indicators that measure the ability, competence and expertise of HR who work in different parts of the provider's organization. 2) MSSP organization Profile represents the indicators that express the capacity and ability of the service provider organization, and assess the competence of the organization.

B. *Financial Category*

The economic Category of this maturity model is characterized by two main factors: 1) sales and pricing that represent the indicators that determine the competitive cost of service delivery in order to attract customer, protect the position of the organization among other competitors and customers. 2) Financial health of the organization that reflects the indicators that are important for organizations, the profitably and operation.

C. *Environmental Category*

The environmental category of this maturity model is characterized by two main factors: 1) market comprehensiveness and the ability to implement represents the indicators that show the market share of organization and the ability of a service provider to serve different security services. 2) The organizations reputation that represents those indicators that demonstrate the organization's reputation related to compliance with its obligations.

D. *Technological category*

The technological category of this maturity model is characterized by the four main indicators. 1) Service delivery infrastructure represents the indicators and requirements without which it is not possible to provide services and delivery of products, and the products and services provided on that platform do not have the required productivity. 2) Technology used represents the indicators that measure the role of technology and its associated capabilities in the process of utilizing services and products. 3) Web management tools show those indicators that measure the impact on how services or products are delivered based on the variety of tools. 4) Provision of security services and technologies are indicators that measure the organization's ability to provide customized service for customers and maintenance of those services.

Considering these measures, the popular models presented in the field of security maturity can be evaluated in Table II. In this study, the ISM3 model, which was presented in 2007, was identified as the base model.The reasons for this can be 1) ISM3 covers information security management and key indicators of the organization's security performance, and is a suitable option for analysing security breaches. And 2) ISM3 is used in IT-based organizations and is therefore well suited for testing in this area.

In the following, the key performance indicators in the MSSPs domain are mapped to the ISM3 Security Maturity Model.Based on this, the proposed model rows are functional indicators and key success factors, and its columns are ISM3 maturity model levels. Based on this, the proposed maturity model is proposed in Table III.

Finally to assess our model, we used Multi-model Analysis and interception methodology. In fact we have tested the model in three MSSPs in Iran and finally based on our use-cases we have been able to optimize in based on MSSPs requirements.

TABLE II

EVALUATION OF DIFFERENT SECURITY MATURITY MODELS

Model	Comprehensiveness	Application area	Usefulness	Simplicity
ISM3[122]	High	Organizational	High	Yes
C2M2[128]	High	Organizational	Medium	Yes
PRISMA[123][124]	Low	Non-Operational	Medium	Yes
ISF[126] [127]	High	Non-Operational	Medium	Yes
FFIEC[197][198]	High	Organizational	Low	No

I. CONCLUSION

More development in electronic equipment increase people and organizations dependency and their investment to technology. This investment and development entice attackers to make mal-behaviors. Organizations can take internalization, outsourcing or the combination of these two methods. Lack of funding and security experts, high demand from customers MSSP, increased emphasis on security surveillance and information disclosure detection are some reasons for outsourcing. Security service providers have designed new solutions to identify and address advanced cyber threats resulting in cyber security market. These providers are partners that can provide a cost-effective alternative to manage the monitoring, alerting and responding to cyber threats that named by MSSPs. Due to increase in the number of MSSPs, the external assessment of this business market is getting more crucial. Effective decision making is based on accurate,

comprehensive, timely and analyzed information. Maturity model is a well-known decision support method for organizations to help them for implementing improvement measures to gradually achieve their strategic goals from an initial to optimized processes. In this paper, we tried to answer this main question as "What are the main components of MSSPs maturity model?" and "What are the levels of MSSP in maturity model?" To answer the first question we categorized the indicators of this maturity model to four main sub-categories named by organizational, financial, environmental, and technological, and 40 sub categories. Using different maturity models and based on their Comprehensiveness, Application area, Usefulness and Simplicity we have chosen ISM3 model as the levels of our proposed model. Since the domains and sub domains of the proposed security maturity model have been identified based on the analysis of various reference models, systematic literature review and regarding the experts' opinion, it can be used in many different areas of security. To use this model, we need to define the maturity characteristics of cyber security capacity and determine the parameters of their representations. The maturity characteristics are defined and documented based on the systematic literature review. Using the proposed maturity model allows the accurate assessment of the security situation and allows managers to improve their decision making process in different domains.

TABLE III
PROPOSED MSSP ASSESSING MATURITY MODEL

Indi		Measure	Maturity Levels					References
			Initial	Formed	Defined	Managed	Optimized	
Organizational	Human Resource Profile	Experienced/ Sophisticated HR	There is very low number of specialist HR in security services. Provision	The organization employs part time security experts in organization.	The organization has experienced experts in the field of providing security services.	There is a clear system for identifying, organizing, training and managing security professionals in the organization.	The organization will periodically improve its human resources based on its technical development and marketing plan.	[9][23][24][25][46] [133][134][135][135][136][137][138][140][62][64] [141][142] [143][144] [99] [100][105][111][123] [124][125][126][128] [139][101][127]
		Educational Degree	organization does not use educated people to provide security services.	There are a number of educated personnel for providing security service.	using educated people to provide security services is in organization's short time planning.	Individual's employs based on their academic education in the field of providing security services.	The organization has a plan for increasing security knowledge and academic level of personnel's.	[22][23][46][133] [145][134][135][136][62] [139][140][99] [100] [101][111][123] [124][125][126] [127][128]
		Passed Training Course	Security services providing Personnel have passed limited on-job training courses.	Security services providing Personnel have completed a number of on-job training courses, based on personal interest.	Security services providing Personnel anticipant in on-job training courses.	Security services providing is based on the training system/ human resources development plan in organization are passing on-job training courses.	Professional training courses are reviewed and upgraded based on the security services of the organization.	[23][99] [100] [101][105][111][123] [124][125][126] [127].[24][46][133][134][135][139]
		Certificates	The security service do not make personnel have valid and relevant security credentials.	Only a number of security service personnel have valid and relevant security credentials.	By The security service that personnel have received valid and relevant security certifications in limited fields.	The security services personnel have received valid security certificates based on the work requirements.	The security certifications required by the personnel of the organization are reviewed and upgraded based on security services.	[9][22][23][24][46][133][134][135][136][62][145][146][139][140][99] [100] [101][105][111][123] [124][125][126] [127][128]
		work experience	People involved in providing security services have no prior security experience.	A number of organizational units have experienced personnel in providing security services (20%).	A number of organizational units have experienced personnel in providing security services (20%).	All key personnel of the organization are considered to have experience in their field of activity.	The work experience required by each organization is reviewed and refined periodically according to the organization's security services.	[22][23][24][46] .[133][134][135][146][14 0]
	MSSP Organization Profile	Organization security personnel rate	organization does not have the minimum personnel required to provide its own security services	The organization uses the part-time personnel to provide security services.	The organization has the necessary personnel to provide security services.	The organization has the efficient personnel to provide security services to large companies.	The personnel rate helps the organization to provide new services and attract customers.	[140][150][105][111] [127][128][146][139][140][99] [100][126]
		Number of Certificates / Related	organization does not have a unique certification in the field of security services	The organization has received some certifications in the form of a security planning	During its years of operation, the organization has received security certifications.	The organization follows a system of specific security certifications for the management, supply and services guarantee.	The organization's security certificates are renewed periodically and reviewed on the basis of changes	[9][22][23][24][46][136][62][138][64][149][146][1 39][140][150][105][111][126] [127][128]
		Learning and education system	organization has no credit and program for security	The organization has some ad-hoc programs in security training courses.	Each organization unit holds some security training courses for its personnel.	The organization has set of routines for conducting regular training courses, and all	The organization revises and improves the structure of the security system in a systematic and consistent manner.	[23][24][46][137][150][9 9] [100] [101][105][111][123] [124][125][126] [127][128][142]

Volume 11- Number 1 – Winter 2019 (57 -70)

Indi		Measure	Maturity Levels					References
			Initial	Formed	Defined	Managed	Optimized	
			training courses.			activities in this area are systematically tracked.		
		Organization's Annual contract rates for security services	The organization's security service contract rates are negligible.	In some areas the use of security services contracts signed with clients	The annual contract rates are acceptable and the organization has contracts with different applicants	The organization has a specific program for developing business interactions with security service applicants and tries to maintain its profitability	The company's annual security contract rates are optimal and the organization uses its current capacity to manage and deliver services	[46] [147]
		Performance guarantee	No service agreement has been completed so far.	In some cases, the organization has attracted the employer's satisfaction with the security services provided.	The organization has sought to obtain the satisfaction of the employer in security services.	The organization uses specific mechanisms to measure the employer's satisfaction as well as management and quality assurance of security services.	The organization uses the system of excellence in the field of service delivery management and tries continuously to improve the quality of service	[9]
Financial	Sales and pricing	Sales revenue from security services	The total number of security service contracts is low	The total number of security service contracts is medium	The total number of security service contracts is general	The total number of security service contracts is high	The organization has no limits on security services contracts	[22][23][24][25][46][133] [134][135][147][137][62] [64][151] [152] . [141][153] [154][123] [124][125][155]
		Pricing, fines, rewards and contractual exceptions	organization does not have a mechanism for contracts and the pricing model	The organization, based on the request of the security service applicant, uses an agreed framework for pricing.	The organization uses a default framework for pricing, fines, rewards, and contractual exceptions.	The organization uses the standardized and regulated trading regulations for pricing, fines, rewards and contractual exceptions.	The Trading Regulations and Pricing Terms will be reviewed and upgraded to determine the fines, rewards and contractual exceptions based on changes.	[24][155][25][123] [124][125] [156]
	Organization's Financial health	Financial statements	Organization currently is not profitable and financial statement is based on this situation.	The financial statement of the organization is set up on the basis of a request from the authorities.	The financial status of the company is discussed in the annual basis committees.	The financial status of the company is specified in accordance with the established standards and presented to the relevant authorities.	The organization provides financial status to the authorities and benefits from its discounts and incentives.	[9][22] [23][24] [25][133][134][135] [147][62] [138][64] [140][144][141][155][123] [124][125]
		Annual turnover	Organization has not reported its turnover in providing security services.	The organization's turnover Reports are provided based on request.	The organization provides Annual Reports at Board Meetings.	The organization acts on the basis of a standard and set of criteria to provide regular financial statements.	The organization's turnover is reviewed and updated based on reporting and resources required by structural changes and security services.	[9][22] [23][24] [25][46][133] [134][135][123] [124][125][147][136][62] [138][64][140] [144][141][155]
Environment	**Comprehensive service and MSSP's ability in operation**	variety of services	The service scope is very limited	Security services are provided irregularly and at the request of the applicant	The organization provides certain security services to the applicants	The organization provides a level-based managed security service.	The organization is capable of reorganizing and changing the services and levels of managed security services dynamically.	[157] [22] [23][24][25][46]. [62] [145][149][146][141] [92] [102] [103] [104][107][120]
		Service scope	The organization can provide managed security services for a single business type.	The organization provides security services based on the request of stakeholders and various industries.	The organization provides joint security services for various industries.	The organization is able to handle specialized security service requests from various industries.	The ability to manage and provide security services for any industry in the organization has been optimized.	[157] [22][25] [145][149] [146] [140][92] [102] [103] [104][107][120]
		Geographic scope of service delivery	organization does not serve in different geographic areas	In some areas, the organization provides its services in a limited way	organization has several locations providing security services in different geographical areas.	The organization follows a specific strategy for the provision of services in different geographic areas and operates on the basis of it.	The organization, based on its market strategy, reviews and updates the geographic scope of the provision of security services periodically.	[157] [22] [23][24] [25][135][147] [62][145][146][92] [102] [103] [104][107][120]
		Marketing Strategy	Organization has no specific marketing activities providing security services.	The organization has security services marketing in some areas.	The organization has marketing for its security services.	The organization uses customized for marketing and introducing its security services.	The effectiveness of marketing methods for security services is periodically reviewed and they change the strategy based on the feedback received from the market.	[157] [24] [62]
		Sale Strategy	Organization does not have a specific strategy to sell its services.	The organization sells its services using brokers in some areas.	The organization uses a variety of methods to provide security and sale.	The organization is trying to sell its services directly to the applicants, using advertisements and discounts.	Selling Methods are reviewed and corrected in periodic basis.	[157][147] . [62]

Indi		Measure	Maturity Levels					References
			Initial	Formed	Defined	Managed	Optimized	
		Service providing Strategy	Organization does not use any special technology to provide security services.	The organization complies with its facilities and the applicant requests use one of the service delivery methods	The organization provides a special security service using various delivery methods	The organization has the ability to provide services in a variety of ways.	Delivery models are evaluated periodically and are reviewed and revised based on performance.	[157] [24][25][46] [147][137][62] [145] . [140][92] [102] [103] [104][107][120]
		Service Level Agreement	Organizational security services are not standardized in terms of quality and features.	Leveling and determining the service characteristics are done only on the basis of the customer's needs.	Based on its technical and specialized capabilities, the organization measures security services.	The organization has a framework for leveling services and pricing based on this and will carry out all its contractual activities in this framework.	The organization is able to quantitatively and quantitatively characterize the security services dynamically and flexibly.	[22][24][25] [133] [135][136][138] [139][140] . [141]
		Non-disclosure Agreement	Organization has not provided a special prediction about customer information disclosure	organization takes considerations into account regarding the non-disclosure of information based on the needs of customers.	The organization has the ability to comply with the obligations set in the agreement.	The organization organizes all its security services based on the requirements of non-disclosure.	The organization is able to redefine and re-engineer non-disclosure requirements in line with changes in structures and security services.	[25] [133]. [134][136]
		Accessibility level of service	organization, based on its technical limitations, can only provide limited security services	The organization provides only a limited number of security services at standard work hours	The organization has the ability to provide security services in regular office hours	The organization has the ability to deliver security services in 24 hours.	The organization has the technical infrastructure and specialized staff necessary to continuously improve the level of access to security services.	[22][24][25][46] [136][137][62] [148][145][151][93] [140][107][120]
	Reputation	Customer recognition of the service	The candidates do not have access to the organization and security services they provide	The applicants are familiar with only a limited number of companies and have requested them in a case	The applicants have relative recognition of the security services of the organization	The organization has a customer relationship management system and the client's knowledge of the services is systematically received and the result is reflected.	Customer satisfaction / dissatisfaction and its reflection on the organization are continuously influenced by the design and improvement of security services	[157] [22] [23][24][25] [133] [135][147][138][62] [64] [146] [139][140][123] [124][125]
		Customer Database	The customers of the organization are very limited.	The organization has acceptable customer in some security services	The organization has an acceptable customer in all security services.	The organization has been able to be trusted for significant part of its customers.	The security services of the organization have significant loyal customers.	[24] [25][133] [138][140]
		Organization experience in service delivery	organization has little background in providing security services	The organization has an experience in providing security services	The organization is particularly experienced in providing security services	The organization has a long term work experience in all areas of management and security services	The organization uses the mechanism for improving security services during the management and service delivery cycle	[22][23][46] [133] [135] [138] [64][146] [140]
		Organization Brand	organization's market share is negligible	The organization operates only in a limited area of the security services market	The organization is ranked as a Security services provider in the security market.	The organization is known and ranked as a leading provider of specialized services in the security market	The organization is ranked as an exclusive provider of new generation services in the security market.	[22] [23][24][25][46][133] [135] [145][146][139][94] [142] [143][123] [124][125]
Technology	Infrastructure	Datacenter Quality	Organization does not have data centers for monitoring, sending and storing data.	The organization has an initial data center for providing services.	The organization has a credible data center - in terms of security, size and quality.	The organization has a specific system and structure to manage and deploy the data center appropriately.	Managing and organizing resources The data center is tailored to the services of the organization reviewed and refined.	-
		Datacenter Location	Organization has no specific climatological evaluation of its data center.	Preliminary climatically assessments are used to select the data center.	The organization considers a set of climatic requirements for selecting the data center.	The organization data center has required safety and environmental certification.	The climatic conditions, governing the organization's data centers, are reviewed periodically and the relevant requirements are updated.	[157][22] [62][151][149][113] [114][115] [116] [117][120][123] [124][125][126] [127]
		Datacenter Ownership	The organization does not have a data center.	The organization uses its rental data center to provide its services.	The organization uses a data center from other service providers.	The organization uses its own property and monitoring data center to provide services	Data center ownership terms are determined by a specific structure and system and reviewed periodically.	[157][22] [62][149][113] [114][115] [116] [117][120][123] [124][125][126] [127][190]

Indi	Measure	Maturity Levels					References
		Initial	Formed	Defined	Managed	Optimized	
	SOC Ownership	organization does not have an SOC.	The organization uses its rental SOC to provide its services.	The organization uses an SOC from other service providers.	The organization uses its own property and monitoring SOC to provide services	SOC ownership terms are determined by a specific structure and system and reviewed periodically.	[157] [22] [120][24] [135][62][149][113] [114][115] [116] [117][120][123] [124][191][125][126] [127]
	Customer Relationship portal	Organization does not have an active portal that supports on-line customer requests and requirements.	The customer relationship portal is in the organization, but it is not updated, and users do not have access to it at 7 * 24.	Depending on service delivery scope, the organization has an active portal to communicate with customers and meet their needs.	The support of customer service and management, and the accountability and complaint system are provided through the Customer Relationship Portal.	The customer relationship portal is periodically reviewed, monitored and updated in accordance with customer requirements and requirements.	[157][22][23] [24][25] [133][135][147][62] [64][151] [140][150] [141][143] [144][192]
	Reporting Dashboard	organization does not have a dashboard or an online reporting mechanism in the service area	The organization uses the reporting mechanism and Dashboard in some parts of the organization	Compliant with service statistics, the security reporting system is used	The organization uses an online reporting mechanism and dashboard to follow the service level agreement, accident management, and compliance with regulations.	Service quality, supply and operating conditions are evaluated periodically through the dashboard, and if necessary, the infrastructure and supply structure are corrected.	[157] [22] [25][133] [147][62] [151] [143] [150] [144][149][113] [114][115] [116] [117][120][123] [124][193][125][126] [127]
Used Technology	Technology type	Organization does not use any internal technology to provide security services.	The organization uses private and open source security technologies in some areas	The organization provides its security services using licensed technologies	The IT organization customizes the provision of security services depending on the client's needs.	The ability and the security of technology used in the organization are up to date and vary according to the needs of the client.	[22][24][133] [134][135] [137][138][64][151] [140][150] [142][141][149][113] [114][115] [116] [117][120][123] [124][194][125][126] [127]
	Technology Brand	Organization does not use a well-known and valid security technology brand to provide services.	The organization uses a limited number of security technologies in the organization.	The organization uses well-known brands, but the same, not diverse in the area of providing security services.	In most areas of security services, several tested brands are tailored to the type of service.	Based on changes in services, the structure and scope of the brand security technology company will be evaluated and updated on the basis of needs.	[22][24][133] [134][135]
	Technology ownership	Identity and ownership of the security technologies used in the organization are unclear.	The organization uses leased security technology in some sectors and in a specific case.	The organization uses its own security technology.	The organization follows a specific structure and system for renting and purchasing security technology.	The terms in technology ownership are reviewed periodically by the organization.	[22][24][133] [134][135]
	Providing technology	Organization simply provides essential security technologies.	In some sensitive areas other technologies such as IDPS are provided.	Applicants for all sectors of the organization and their security technologies can be provided.	In addition to common security technologies, the organization also provides some solutions.	Depending on the organization's needs, the goal is to customize Multi Brand security technologies.	[22][149][113] [114][115] [116] [117][120][123] [124][125][126] [127][46][148][140][150] [141]
Web based management tools	Ticketing system	Organization does not generate ticket and workflow in the management and supply chain.	The organization uses the ticketing system as a part of its services.	The organization has implemented a ticketing system to support the management and provision of security services.	The organization follows a specific structure and system for ticketing activities and workflows related to security services.	The organization is able to improve its ticketing system in line with changes in the organizational structure and scope of security services.	[194]
	Device maintenance	Organization does not have the ability to support the security equipment provided to the client.	In some cases, the organization can provide support to its customers for a certain period of time.	In many sectors, the organization has the ability to support the security equipment tailored to the customer's needs.	The organization is able to personalize its existing platform in accordance with the customer's needs and the security equipment provided to them.	The organization has many experiences in managing multiple technologies and platforms, in addition to packaging its products.	[22][149][113] [114][115] [116] [117][120][123] [124][195][125][126] [127][46] [148][140][150][141]
Provide security	Technology production methods	Organization does not produce any technology to customize customer service.	The organization requests the vendor to customize the service, if required by the client.	For the sensitive parts of the client organization that is highly confidential, the service organization is customized.	The organization generates and customizes all the required services and supports it for a limited period, depending on the client's requirements	Depending on the customer's requirements, the organization maintains all custom and manufactured products and maintains its lifespan.	[22][149][113] [114][115] [116] [117][120][123] [124]

Indi	Measure	Maturity Levels					References
		Initial	Formed	Defined	Managed	Optimized	
	Technology Implementation Techniques	Organization does not implement any security technology.	The organization uses full open source software in implementation of security.	Commercial security programs are being customized and validly licensed in critical parts.	For all parts of the organization, there are customized commercial security plans and are licensed for implementation.	Maintenance and support of implemented services are carried out in a lifelong way.	[125][126] [127][46][148][140][150] [141]

REFERENCES

[1]. "Security market Research Report," GrandView, 2015.

[2]. "Global ICT investment will hit $4 trillion in 2018 – with cloud and hybrid IT infrastructure driving it," 2018.

[3]. "ICT Spending Forecast 2018-2022," 2018.

[4]. "Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019," 2018.

[5]. "Cyber Security Market Size To Reach $205.51 Billion By 2024," August 2016.

[6]. R. McCullen, "Cyberthreats: A 10-Year Perspective," Forbes, 2018.

[7]. "Threat Intelligence Market worth $12.9 billion by 2023," Markets and Markets", 2015.

[8]. J. Faile, "Security Outsourcing," SANS Institute Information Security Reading Room, 2001.

[9]. T. Bussa, K. M. Kavanagh, S. Deshpande and P. Shoa, "2018 Magic Quadrant for Managed Security Services, Worldwide," Gartner, 2018.

[10]. "IT Outsourcing: The Reasons, Risks and Rewards," [Online]. Available: http://www.corpcomputerservices.com/articles/outsourcing-reasons.

[11]. M. Zhao, J. Wang and J. Zhang, "Multilateral Contracts in Information Security Outsourcing," 2017.

[12]. "Cyber Security market 2015-2025,," 2015.

[13]. Statistica, 2018. [Online]. Available: https://www.statista.com/statistics/595182/worldwide-security-as-a-service-market-size/.

[14]. "EMEA Managed Security Services Market, Forecast to 2021," 2016.

[15]. "Managed Security Services (MSS) Market Size 2018 – Top Key Players, Adoption Trends, Growth Prospects, Forecasts by 2023," 2018.

[16]. Centrify, 2018. [Online]. Available: https://www.centrify.com/partners/managed-security-service-partner/.

[17]. 2019. [Online]. Available: https://www.ibm.com/security/services/managed-security-services.

[18]. 2019. [Online]. Available: https://www.emc.com/about/news/press/2014/20140224-01.htm.

[19]. 2019. [Online]. Available: https://www.cisco.com/c/en/us/products/security/service-listing.html.

[20]. 2019. [Online]. Available: https://www.fireeye.com/solutions.html.

[21]. 2019. [Online]. Available: https://www.checkpoint.com/support-services/support-plans/.

[22]. "Electing a managed security services provider: The 10 most important criteria to consider," 2014.

[23]. A. Pollard, C. McClean, J. Blankenship, C. O'Malley, T. Lyness and P. Dostie, "The Forrester Wave™: Managed Security Services Providers, North America, Q3 2016," 2016.

[24]. M. Vazquez, "IDC MarketScape: Worldwide Managed Security Services 2017 Vendor Assessment," 2017.

[25]. J. Allen, D. Gabbard and C. May, "Outsourcing Managed Security Services," 2003.

[26]. M. E. hitman and H. J. Mattord, Principles of Information Security, Cengage Learning, 2017.

[27]. B. Curtis, B. Hefley and S. Miller, "People capability maturity model version 2.0. No. CMU/SEI-2009-TR-003," 2009.

[28]. Team, "Capability Maturity Model® Integration (CMMI), Version 1.1--Staged Representation," 2002.

[29]. B. Acohido, "Improving Detection, Prevention and Response with Security Maturity Modeling," 2015.

[30]. Z. Lianying, J. He and X. Zhang, "The project management maturity model and application based on PRINCE2," Procedia Engineering, vol. 29, pp. 3691-3697, 2012.

[31]. G. Kumta and S. Mitul, ""Capability maturity model." A Human Perspective," 2002.

[32]. M. C. Paulk, B. Curtis, M. B. Chrissis and C. V. Weber, ""Capability maturity model, version 1.1"," IEEE software 10.4, pp. 18-27, 1993.

[33]. M. C. Paulk, "A History of the Capability Maturity Model for Software," Software Quality Professional Magazine, vol. 1, 2009.

[34]. W. K. Brotby, Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement, Auerbach Publications, 2009.

[35]. P. Byrnes and M. Phillips, "Software Capability Evaluation Version 3.0 Method Description," 1996.

[36]. J. Carvalho, R. H. Pereira and Á. Rocha, A Comparative Study on Maturity Models for Information Systems in Higher Education Institutions, Digital Science, 2019.

[37]. B. Alena, "Green ICT maturity model for Czech SMEs," Journal of Systems Integration 6.1, pp. 24-36, 2005.

[38]. 2019. [Online]. Available: https://www.statista.com/statistics/268584/worldwide-ict-revenue-since-2005/.

[39]. [Online]. Available: https://www.grandviewresearch.com/industry-analysis/cyber-security-market.

[40]. "The threat is growing more serious by the minute…," 2014.

[41]. "McAfee Labs Threats Report," 2018.

[42]. "McAfee Thread Labs Report," McAfee, 2018.

[43]. 2018. [Online]. Available: https://www.gartner.com/newsroom/id/3836563.

[44]. "Top 10 criteria for selecting a managed services provider," 2017.

[45]. "Selecting a Managed Security Services Provider: The 10 most important criteria to consider," 2011.

[46]. A. VAULT, "10 Tips for Selecting a Managed Security Service Provider (MSSP)," ALIEN VAULT, 2018.

[47]. "Outsourcing Managed Security Services," 2003.

[48]. "X. 800 security architecture for open systems interconnection for ccitt applications," 1991.

[49]. "National Information Assurance (IA) Glossary," 2003.

[50]. "Guide to Secure Web Services," 2007.

[51]. Feb 2004. [Online]. Available: https://www.w3.org/TR/ws-arch/.

[52]. "Guide to Information Technology Security Services," 2003.

[53]. 2019. [Online]. Available: https://www.gartner.com/technology/it-glossary/mssp.jsp.

[54]. A. Abbas and A. Saddik, "A State of the Art Security Taxonomy of Internet Security: Threats and Countermeasures," GESTS Int'l Trans. Computer Science and Engr, vol. 19, no. 1, pp. 27-36, 2005.

[55]. A. Usher. [Online]. Available: http://www.sharp-ideas.net/ia/information_assurance.htm.

[56]. T. Sveinsdottir, "Taxonomy of Security Products, Systems and Services," 2014.

[57]. 2000. [Online]. Available: http://www.opengroup.org/public/arch/p3/trm/tx/tx_secur.htm

[58]. 2017. [Online]. Available: https://www.cloudnav.com/2017/08/07/taxonomy-microsoft-security-services/.

[59]. J. McCumber, "Information Systems Security: A Comprehensive Model," in Proceedings 14th National Computer Security Conference. National Institute of Standards and Technology, 1991.

[60]. V. Maconachy, C. Schou, D. Ragsdale and D. Welch, "A Model for Information Assurance: An Integrated Approach," in Proceedings of the 2001 IEEE Workshop on Information Assurance and Security. U.S. Military Academy. West Point, NY, 2001.

[61]. 2017. [Online]. Available: https://www.computereconomics.com/custom.cfm?name=postPaymentGateway.cfm&id=2431.

[62]. K. M. Kavanagh and J. Pescatore, "Magic Quadrant for MSSPs, North America, 1H07," 2007.

[63]. "Eight important criteria for selecting a managed security services provider," 2019.

[64]. "How to Choose an MSSP," 2016.

[65]. 2019. [Online]. Available: https://en.wikipedia.org/wiki/Managed_security_service.

[66]. "Managed security services Helping organizations prevent, detect,and respond to evolving threats," 2018.

[67]. 2018. [Online]. Available: https://www.gartner.com/it-glossary/mssp-managed-security-service-provider.

[68]. R. Gupta, "Managed Security Services (MSS): An Opportunistic It Security Segment, Globally," 2015.

[69]. Karmer, "Magic Quadrant for Global MSSPs," 2014.

[70]. S. Kairab, A Practical Guide to Security Assessments, AUERBACH PUBLICATIONS (A CRC Press Company), 2005.

[71]. S. Deshpande, 2018. [Online]. Available: https://www.gartner.com/doc/3876285/market-share-managed-security-services.

[72]. The global MSS market size is expected to grow from USD 24.05 billion in 2018 to USD 47.65 billion by 2023, at a Compound Annual Growth Rate (CAGR) of 14.7%, 2018.

[73]. 2017. [Online]. Available: https://globenewswire.com/news-release/2017/12/04/1219775/0/en/Global-18-Billion-Managed-Security-Services-Market-Outlook-to-2025.html.

[74]. R. Drew, 2018. [Online]. Available: https://www.esecurityplanet.com/products/att-mssp.html.

[75]. 2018. [Online]. Available: https://atos.net/en/solutions/cyber-security.

[76]. [Online]. Available: https://www.baesystems.com/en/cybersecurity/capability/managed-security-services.

[77]. R. Drew, 2018. [Online]. Available: https://www.esecurityplanet.com/products/bt-mssp.html.

[78]. [Online]. Available: https://www2.bt.com/static/i/media/pdf/managed_security_services_wp.pdf.

[79]. "Symantec™ Managed Security Services".

[80]. [Online]. Available: https://www.symantec.com/en/au /services/cyber-security-services/managed-security-services.

[81]. [Online]. Available: https://enterprise.verizon.com/resources /articles/managed-security-services/.

[82]. [Online]. Available: https://www.nttsecurity.com/en-us/services/managed-security.

[83]. [Online]. Available: https://us.nttdata.com/en/services /managed-services/managed-security-services.

[84]. C. Richmond, "IDC MarketScape: Worldwide Managed Security Services 2014 Vendor Assessment," IDC, 2014.

[85]. C. Huang, "IDC MarketScape: Asia/Pacific Managed Security Services 2015 vendor assessment," IDC, 2015.

[86]. "Top 10 Tips for Selecting an MSSP," MSPmentor.

[87]. "Serro Solutions Enables Managed Security Service Providers to Optimize Networking Performance and Cost," Serro, 2015.

[88]. "Fortinac: Expanded Security Services Opportunities for MSSPs," Fortinet, 2018.

[89]. "Managed Security Service Provider Program," Fortinet.

[90]. NTTSecurity, "How to Choose an MSSP," NTT Group (Nippon Telegraph and Telephone Corporation), 2016.

[91]. W. S. Humphrey, "Characterizing the Software Process: A Maturity Framework, Software Engineering Institute," IEEE Software, vol. 5, no. 2, pp. 73-79, 1988.

[92]. T. Bernard, B. Gallagher, R. Bate and H. Wilson, CMMI Acquisition Module (CMMI-AM), Version 1.1, Carnegie Mellon University, 2005.

[93]. G. D. Pires and J. Stanton, "EXPLAINING CONSUMER SELECTION OF A SERVICE PROVIDER," Marketing and Enterprise Group; University of Newcastle, 1990.

[94]. A. OKe, A. Maltz and P. Christiansen, "Criteria for sourcing from developing countries," Strategic Outsourcing: An International Journal, vol. 2, pp. 145-164, 2009.

[95]. Wikipedia, "Managed Security Service," Wikipedia, 30 May 2018. [Online]. Available: https://en.wikipedia.org/wiki/Managed_security_service.

[96]. K. Margaret, K. Kulpa and A. Johnson, Interpreting the CMMI: a process improvement approach, 2008.

[97]. B. Curtis and J. Alden, "The Business Process Maturity Model," in BPM & Organizational Maturity, 2007.

[98]. R. Weerdmeester, C. Pocaterra and M. Kefke, "Knowledge Management Maturity Model," in in KM World Proceedings, Santa Clara, 2003.

[99]. C. Bill, W. E. Hefley and S. Miller, "Overview of the People Capability Maturity Model," 1995.

[100]. M. Vivaldi and U. Berg, "Influencing the People Perspective at Ericsson using the People CMM," in in Proceedings of the European SEPG 1999 Conference, 1999.

[101]. "People Capability Maturity Model (P.CMM)," SEI (software Engineering Institute), 2001.

[102]. "Capability maturity model® integration (CMMI SM), version 1.1," CMMI-SE/SW/IPPD/SS, 2002.

[103]. "Capability Maturity Model® Integration for Development Version 1.2," Software Engineering Institute, 2006.

[104]. "CMMI® for Development, Version 1.3, Improving processes for developing better products and services," oftware Engineering Institute, no. CMU/SEI-2010-TR-033, 2010.

[105]. R. René, "The Maturity Model of Corporate Foresight," Corporate Foresight, pp. 71-121, 2010.

[106]. S. Essam, "Business Intelligence Maturity Models," 2011.

[107]. "ITIL Process Maturity Framework," ITSM Solutions, 2006.

[108]. P. Crosby, "Quality Is Free. "The art of making quality certain."," Americam Library, Newyork, 1979.

[109]. P. Crosby, "Quality is free: The art of making quality certain," Signet, 1980.

[110]. P. Crosby, "Quality is still free: making quality certain in uncertain times," McGraw-Hill Companies, 1996.

[111]. D. Fisher, "The business process maturity model: a practical approach for identifying opportunities for optimization," Business Process Trends, vol. 9, no. 4, pp. 11-15, 2004.

[112]. R. Welke, R. Hirschheim and A. Schwar, "Service oriented architecture maturity," Computer.

[113]. A. Arsanjani and H. Kerrie, "Increase flexibility with the service integration maturity model (simm)," IBM developerworks, 2005.

[114]. A. Arsanjani and H. Kerrie, "The Service Integration Maturity Model: achieving flexibility in the transformation to SOA," in IEEE International Conference on Services Computing, 2006.

[115]. Gartner, "Enterprise Information Management Maturity Model," December 2008. [Online].

[116]. Gartner, "Gartner's Enterprise Information Management Maturity Model," 02 March 2016. [Online].

[117]. "Gartner's Enterprise Information Management Maturity Model," Gartner, 2018.

[118]. R. Nolan and D. C. Croson, "A six-stage process for transforming the organization," Harvard Business Press, 1995.

[119]. D. THAKUR, "Nolan's Six-stage Model," [Online]. Available: http://ecomputernotes.com/mis/information-and-system-concepts/nolanssixstagemodel.

[120]. "Cloud Computing Maturity Model Guiding Success with Cloud Capabilities," Oracle, 2011.

[121]. "A Business Framework for the Governance and Management of Enterprise IT (COBIT 5)," ISACA, 2012.

[122]. "ISM3 1.0. Information Security Management Maturity Model," ISECOM, USA.

[123]. P. Bowenl and R. Kisse, "rogram Review for Information Security Management Assistance (PRISMA)," NIST-7358, 2007.

[124]. NIST, "Program Review for Information Security Management Assistance – PRISMA," 2007.

[125]. S. Woodhouse, "An ISMS (Im) – Maturity Capability Model," in Proceedings of the IEEE 8th International Conference on Computer and Information Technology Workshops, 2008.

[126]. "Using the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security," in IBM, 2013.

[127]. "Using the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security," IBM, 2003.

[128]. "CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2)," in DHS, 2014.

[129]. "Cyber Security Capability Maturity Model (CMM) – V1.2," in Global Cyber Security Capacity Center, 2014.

[130]. D. Bruin and M. Rosemann, "Towards a business process management maturity model," 2005.

[131]. M. Weed, "A systematic review of knowledge and a meta-evaluation of methods," Journal of Sport and Tourism, vol. 11, no. 1, pp. 5-30, 2002.

[132]. L. Zimmer, "Qualitative meta-synthesis: A question of dialoguing with texts," Journal of Advanced Nursing, vol. 53, no. 3, pp. 311-318, 2006.

[133]. M. Kaddoura, "Motivations for engaging a Managed Security Services Provider: Criteria for successfully selecting a MSSP," DarkMatter, United Arab Emirates, 2018.

[134]. "Choosing an MSSP – 4 Point Checklist," Contemporary Computer Services Inc (CCSI), 2018.

[135]. A. Shahrasbi, M. Shamizanjani and M. Alavidoost, "An Aggregated Fuzzy Model for the Selection of a Managed Security Service Provider," International Journal of Information Technology & Decision Making, vol. 16, no. 3, 2017.

[136]. SecureWorks, "Top Five Evaluation Criteria When Selecting an MSSP," 2016.

[137]. R. Kamat, "Managed Security Services: Risks and Benefits," 2014.

[138]. "10 Considerations When Selecting A Managed Security Services Provider," Secure-24, 2016.

[139]. K. Wheiler, "Referrals between Professional Service Providers," Industrial Marketing Management, vol. 16, pp. 191-200, 1987.

[140]. "Considerations when Choosing a Managed IT Services Provider," OneNeck (IT Solutions a TDS Company), 2016.

[141]. E. Ferrara and N. Hayes, "Emerging Managed Security Service Providers," The Forrester Wave, 2013.

[142]. L. Navarro, "Information security risks and managed security service," Information Security Technical Report 6, pp. 28-36, 2001.

[143]. AT&T, "AT&T Managed Security Services," AT&T Company, 2013.

[144]. E. Ferrara, A. Rose, C. McClean and N. Hayes, "Information Security Consulting," The Forrester Wave, 2013.

[145]. K. Ramune and S. Laimouna, "A cross-national investigation of service provider selection criteria in the lithuanian and nordic mobile telecommunications sectors," EsicMarket, vol. 128, pp. 27-44, 2007.

[146]. P. L. Dawes, G. R. Dowling and P. G. Patterson, "Criteria Used to Select Management Consultants," Industrial Marketing Management, vol. 21, pp. 187-193, 1992.

[147]. J. Pollard and C. O'Malley, "The Forrester Wave™: Global Managed Security Services Providers (MSSPs), Q3 2018 (The 14 Providers That Matter Most And How They Stack Up)," Forrester, 2018.

[148]. "Nine Key Criteria for Selecting Nine Key Criteria for Selecting," Dynamic Quest, North Carolina, 2015.

[149]. L. Yang and J. Peng, "Comprehensive Evaluation for Selecting IS/IT Outsourcing Vendors Based on AHP," Journal of Information & Computational Science, vol. 9, no. 9, pp. 2515-2525, 2012.

[150]. "Selecting a managed security services provider: The 10 most important criteria to consider," IBM Global Technology Services, 2017.

[151]. E. L. Li, "Study of the Decision-Making Model of Outsourcing Service Provider Selection," International Journal of u- and e-Service, Science and Technology, vol. 6, no. 2, 2013.

[152]. J. Wang, Z. Lin and H. Huang, "A Decision Model for Information Systems Outsourcing:Using a Multicriteria Method," Serv. Sci. & Management, vol. 1, pp. 1-9, 2008.

[153]. M. Lacity and L. Willcocks, "Interpreting information technology sourcing decisions from a transaction cost perspective: Findings and critique," Accounting, Management and Information Technologies, vol. 5, pp. 203-244, 1995.

[154]. J. Fisher, R. Hirschheim and R. Jacobs, "Understanding the outsourcing learning curve: A longitudinal analysis of a large Australian company," Information Systems Frontiers, vol. 10, pp. 165-178, 2008.

[155]. N. Lord, 2018. [Online]. Available: https://digitalguardian.com/blog/what-are-managed-security-services-why-organizations-hire-managed-security-service-providers.

[156]. W. Dickson, "An analysis of vendor selection systems and decisions," Journal of Purvhasing, vol. 2, no. 1, pp. 5-17, 1966.

[157]. K. Kavanagh and J. Pescatore, "Magic Quadrant for MSSPs, North America, 1H07," Gartner, 2017.

Mohammad Gholami Mehrabadi Received his B.Sc. in Electronic Engineering in 2003 from Islamic Azad University, Arak Branch, Iran. Received his M.Sc. in Executive Master of Business Administration in 2013 from Allameh Tabatabaei University, Tehran, Iran. He is currently pursuing the Ph.D. degree in the Faculty of Management and Accounting Shahid Beheshti University, Tehran, Iran. His current research mainly focuses on MSSPs and their Maturity Assessment Model.

Massoud Kassaee received his BBA in management and computer science from the University of Toledo. Ohio(USA) in 1984 and MBA in management from University of Montana in 1987 and Ph.D from University of North Texas (USA) in 1992. Between the years 1992 to 1999 served as an associate professor at the University of Tehran and after 1999 served as a full time faculty member of University of Shahid Beheshti in Tehran. His research interests include manufacturing strategy , productivity and quality issues and many other management topics. He has published various books and research papers within the above stated fields.

Abouzar Arabsorkhi received his Ph.D. Degress from the University of Tehran in the field of Information Systems Management. He is a faculty member and the head of the Network and System Security Assessment Unit at the Information and Communications Technology Research Institute. Over the past few years, he has been involved in Security Management and Planning, Security Achitecture, Risk Management, Security assessment and Prototype Certification, and the Design and Implementation of Specialized Security Labs. The Internet Security of Objects is one of his main research interests. During the past 10 years, he has been teaching in the field of Information Systems and E-Commerce Security.