GAIA-MLIS: A Maturity Model for Information Security

Roger W. Coelho
Computer Science Department
State University of Londrina, UEL
Londrina, Brazil
rogercoelho04@uol.com.br

Gilberto Fernandes Jr.
Computer Science Department
State University of Londrina, UEL
Londrina, Brazil
gil.fernandes6@gmail.com

Mario Lemes Proença Jr.
Computer Science Department
State University of Londrina, UEL
Londrina, Brazil
proenca@uel.br

Abstract— **Information security management has become one of the most important areas for organizations in recent times. This is due to the increased need to protect data which is, in turn, one of the most important assets for any organization nowadays. Managing security risks is an ardous task which requires investments in support and technology management in order to succeed. Thus, there is great demand for a tool which is able to demonstrate the maturity level of an information security system, with the main objective of identifying key strengths and weaknesses in IT processes utilized by an organization. The GAIA-MILS model presented in this article has, as its main goal, to analyze the maturity level of an organization's information security system and supply them with key data on how they can improve. This proposed model presents descriptions of each different level in the areas of hardware, software, people and facilities. Its main objective is to diagnose and aid in the improvement of any identified weaknesses in the management of each specific area.**

Keywords - Maturity Level; Information Security; IT Governance.

I. INTRODUCTION

In the business world, asset information is seen as one of the most important within organizations. There are three distinct types which are considered most valuable: people, facilities and information [1]. Thus, security risk management is usually based on technology support and investment management [2].

The risks posed by information systems are not only complex but also difficult to quantify, since the damage can directly impact on the goal of the organization [5].

Organizations and service providers must develop protection tools in order to avoid misappropriation of user data. Thus, security threats such as viruses, worms, denial of service, submission of data by third parties, among others, cause concern for both users and service providers [3].

The Governance of Information Technology, aligned with good information security, is vital to the organization and service providers, since its credibility and reliability are tested every day. In addition, assessment methods can provide prescriptive data on how to improve the company management, as well as define who is responsible for the information and how it will be transmitted or maintained [15].

In conjunction with IT (Information Technology) governance, information security means keeping three main pillars: confidentiality, as information must be accessible only to authorized persons; integrity, to ensure that information is entirely transmitted; and usability, to guarantee authorized personnel access to the information and related resources when needed [4].

Organizations should assess their level of safety maturity through a formal model and utilize it as a parameter to measure the security risk. The model GAIA Maturity Level Information Security (GAIA-MLIS) aims to assess the maturity level of information security used in the evaluated network. For the purpose of implementing improvements in these processes, GAIA-MLIS enables companies to identify weaknesses in security processes, like hardware, software, human resources, facilities and information.

This article is organized as follows: Secion II deals with IT Governance and Information Security; Section III presents GAIA-MLIS Maturity Model Information Security; Section IV shows tests and results; and finally, Section V concludes the article.

II. IT GOVERNANCE AND SECURITY OF INFORMATION

Technological infrastructure is critical to daily operations within an organization and should be managed with defined processes. Accordingly, IT governance should focus on risk and resource management and strategic alignment to ensure that the technology and the active information adopt corporate objectives, maximizing benefits and opportunities as a means of acquiring competitive advantage [1].

IT governance has emerged as an auxiliary tool for managers, both in IT and other sectors of an organization, to help them comprehend the importance of all sectors working in alignment and, therefore more efficiently, in order to achieve their common goal [6]. IT is a strategic sector for an organization and it aids in revenue generation, contributing to the development of new technologies and technical support for other sectors. The Chief Information Officer

(CIO) must establish an effective governance, to improve the performance and success of the organization, supporting business strategies and plan of action [5].

Effective governance requires that the managers set standards and regulations for information assets. Information security is not only restricted to minimizing risks and failures, but it also affects the reputation of the organization, depending on how it acts on disaster recovery. The recovery organization defines the values and access permission information, thus everyone involved, customers, employees, among others, come to rely on the credibility of the organization [7]. Almost all organizations have their automated processes in their information systems, in order to ensure the efficient delivery of their services [17].

It is know that security is a method to protect the information against various types of threats ensuring continuity of business, higher return on investment and minimized risk. It is also the practice of ensuring the information can only be read, heard, altered or transmitted by people or organizations that have the right to do so. The main goals are confidentiality, integrity and availability. Confidentiality is the protection against theft and espionage. Integrity is the protection against non-authorized changes. Availability is the automated and secure access to the information users [12] [18].

Information security is achieved by means of an appropriate set of controls, which might include, policies, procedures, software, hardware, among others. All these controls need to be established, implemented, monitored, reviewed and improved in order to achieve the company’s business targets. Likewise, security metrics have attracted the attention of the community for many years. However, the field is still lacking a formal model [16].

It is necessary that these controls are carried out in conjunction with security metrics to measure and compare the value of the security provided by different systems and settings [8].

The organization should always conduct audits at intervals of predetermined time in order to ascertain whether the control objectives, processes and procedures are meeting the security requirements of information identified, and if all objectives are maintained and implemented by executing them as expected. Control Objectives for Information and Related Technology (COBIT) aims to help businesses create an ideal value, referring to the IT sector, balancing and maintaining the resources from this area. Thus, COBIT version 5 allows organizations to manage their resources in a holistic way, with the goal of an end-to-end IT and functional areas considering both internal and external interest business [9].

For the development of a model of maturity level in information security, COBIT serves as a helper tool. Thus, the asset information gains importance in verifying the actual efficiency of the resources used for protection and obtaining a level of acceptance that is risky or not for the organization, since the information and its security must be established during the process of governance. The COBIT maturity model is used as basis for the GAIA-MLIS maturity model.

Information, systems, processes that support the organization, and even computer networks, are important assets to the organization's business. With the view to ensure greater competitiveness and visibility, the security information assets should be reviewed each time period and verified whether the initial planning is under execution or, the initial idea does or does not comply with the reality of the organization [7].

It is a fact that organizations often undergo various types of threats to their systems and computer networks, which may include, espionage, malicious persons within the enterprise and electronic fraud [11]. It is well known that organizations should understand the need for improvements in regards to risks they face and what targets and plans are in place [10].

Information security is important for any organization, whether a public agency with a model of electronic government (e-gov), or for a private enterprise [11].

Many systems are not designed for security. Some organizations do not have appropriate processes and procedures. It is essential that the requirements of information security are identified, analyzed and monitored, so that through continuous improvement, targets relating to information and its security are being met.

It is important to evaluate and establish a standard on an enterprise maturity level, so that both can be used to research through questionnaire or the construction of baselines about characteristics related to the use of technology. The use of baseline, or digital signature, has been used, for example, for establishment of standard and profile to network usage, as may be viewed in [21] and [22].

The standards ISO / IEC 27001:2005 and 27002:2005 aim to help IT managers and others, to establish what the security requirements are for the information which should be adopted. The standards serve as a guideline to develop practices and procedures for information security and assist in confidence building activities focusing on inter-organizational guidelines [19] [20].

III. Model of GAIA-MLIS

Information is considered by many organizations as the asset which causes the most concern [13]. Defined processes help managers and employees to identify the requirements for decision making in order to protect all assets related to information [14].

The GAIA-MLIS maturity model aims to evaluate the level of maturity in information security and examines five areas, which are: Hardware, Software, Staff, Facilities and Information. All these areas are related to information. Through this model, organizations can verify the level of maturity in information security, identify if there is any deficiency and correct it in order to implement the improvement.

Figure 1 shows that the information has a centralizing role among all assets. Keeping information secure is one of the most difficult challenges that organizations have. Given that, many resources and processes should be measured by GAIA-MLIS model.

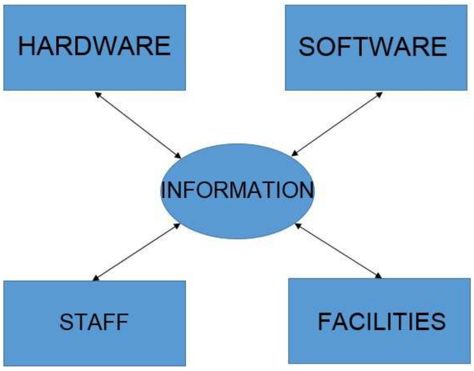

Figure 1. Relationship Areas.

A. *Maturity Level GAIA-MLIS*

Organizations are concerned with constant intrusions into computer systems. Processes in information security should be stored in environments that require more efficient security not only in computational media, but also in the physical environment with committed employees and a series of rules and procedures laid down in order to protect their information assets.

Since this procedure is not always carried out by the companies, along with the lack of knowledge of the importance of information, or non-commitment from the directors to the other employees, the creation of tools able to verify the security level of information is necessary for organizations. Thus, the GAIA-MLIS, model aims to analyze the level of maturity in information security in a particular company.

Through GAIA-MLIS, companies can verify what their weaknesses are in relation to information security and what targets they need to meet to achieve a certain level of information security. Through continuous planning, corporations can use the model in order to check whether goals are being met. The proposed model has five levels of maturity, which are goals and objectives describing what should be achieved by companies regarding the information security with a fully managed process.

The maturity model GAIA-MLIS is based on recommendations of COBIT 5 [9] and ISO / IEC 27001 [10] and 27002 [11] standards. The GAIA-MLIS maturity levels are described below.

Level 0, no insurance: Processes are not defined in information security. There are no defined responsabilities for information security policies. Employees and partners are unaware or are not trained with awareness programs on the importance of information security. Employees, partners and third parties do not suffer disciplinary proceedings upon the discovery of an information security incident. Shutdown policy of employees, partners and third parties policies are not applied upon termination and the return of organization’s information assets. There is no security or access control defined process. Physical facilities are unsecured. There is no protection of equipment against external threats, whether human or environmental. There is no an efficient management for the network, avoiding or minimizing loss, damage or theft to information assets. Asset information is not encrypted. There is no backup policy with copies stored in monitored environments with access control in an environment protected against external threats. Inventories of assets are not identified and there are not established or documented. There are no classificaions of the importance and values of information.

Level 1, entry level insurance: Some processes are defined in information security. There are no defined sets for information security. Staff and partners are unaware or are not trained with awareness programs on the importance of information security. Employees, partners and third parties do not face disciplinary proceedings upon the discovery of a security incident information. Shutdown of employees, partners and third parties policies are applied haphazardly when closing the active. There is no security and access control process defined. Physical facilities are unsecured. There is some equipment protection against external threats, whether they are human or environmental. There is a basic management for the network without defined processes to avoid or minimize loss, theft or damage to information assets. Asset information is not encrypted. There are backup policy, but there are no copies stored in environments with access control, monitored and protected from outside threats. Assets inventory are not identified and are no established or documented. There are no classifications of the importance and values of information assets.

Level 2, regular insurance: Processes are defined in information security. There are few sets of defined responsibilities for information security. Staff and partners know, but they are not trained in awareness programs on the importance of information security. Employees, partners and third parties do not suffer disciplinary proceedings when some information security incidents are discovered. Shutdown of employees, partners and third parties policies are applied haphazardly when closing the active. There are some control access security set. Physical facilities are unsecured. There is some equipment protection against external threats, whether they are human or environmental. There is a basic management for the network without defined processes to avoid or minimize loss, theft or damage to information assets. Asset information is not encrypted. There are backup policy, but there are copies stored on environments without monitoring, access control and external threat. Inventories of assets are identified and established, but are not documented. There are no classifications of the importance and values of information assets.

Level 3, partially safe: Processes are defined in information security and there are sets of defined responsibilities for information security. Staff and partners are trained in awareness programs on the importance of information security. Employees, partners and third parties sufferers disciplinary proceedings when an information security incident is discovered. Shutdown of employees, partners and third parties are partially documented. There is security and access control procedures defined. Physical facilities are protected. There is some equipment protection against external threats, whether they are human or environmental. There is an efficiently network managed, with some defined processes to avoid or minimize loss, theft or damage to information assets. Asset information is encrypted. There are backup policies and the copies are stored in monitored environments with access control and with protected against external threats to the environment. Inventories of assets are identified and established, but they are partially documented. There are classifications of the importance and values of information assets are partially documented.

Level 4, fully insured: Processes are defined in information security. Sets of responsibilities defined by security policy information. Staff and partners are trained in awareness programs on the importance of information security. Employees, partners and third parties sufferers disciplinary proceedings when an information security incident is discovered. Shutdown policies of employees, partners and third parties are totally documented. Access control are defined. Physical facilities are protected. The facilities are protected against external threats, both human and environmental. There is an efficient network management, avoiding or minimizing loss, damage or theft to information assets. Asset information is encrypted. There are backup policies and the copies are stored in monitored environments with access control and with protected against external threats to the environment. Inventories of assets are identified, established and registered. There are classifications established and the importance and values of information assets fully documented.

The maturity levels possess the following percentages: Level 0 has a percentage from 0% to 35%; Level 1 from 36% to 55%; Level 2 from 56% to 75%; Level 3 from 76% to 85%; and Level 4 above 85%. The percentages were assigned as described metrics of security levels. The empirical study was carried out to create an evaluation model for information security by analyzing the areas (hardware, software, staff, facilities and information), and these weights are an adaptation to what is suggested in the groups of ISO/IEC 27002. As observed, the levels are described as the overall organizational structure an organization might have, due to their maturity in information security. It is noteworthy that, through measurements of the formal model to assess GAIA-MLIS, organizations can plan and check the weaknesses in security processes.

The five ares (Hardware, software, facilities, staff and information) on GAIA-MLIS is addressed as in ISO/IEC 27002 standard. We may relate the areas of ISO/IEC 27002 (security policy, organizing information security, asset management, human resources security, physical and environmental security, communications and operations management, access control, information system acquisitions, development and maintenance, information security incident management, business continuity management and compliance) with five areas of GAIA-MLIS.

The evaluation will provide all companies, whether public or private, the ability to measure, manage and verify the asset information and use metrics to target higher levels by structuring its processes according to their needs and realities. Thus, the results obtained by supplementation of data areas provide greater control of the process used in information security, as well as manage the risks that organizations are subjected to every day.

IV. TESTS AND RESULTS

As means to verify and validate the maturity model GAIA-MLIS, three organizational structures were analyzed. The companies were not divided into sectors groups (service provider, bussiness company, etc), because we wanted to have a general sampling.

A questionnaire with thirty questions was administered in order to identify strengths and weaknesses in the processes of the five areas. The objective of the questions is to perform a diagnostic analysis of each area (hardware, software, people and facilities). The questions were developed based on the suggested groups of ISO/IEC 27002. There are five questions for the groups hardware, software, people and facilities, and ten questions related to the information area. The diagnose performed involves the application evaluation of security requirements related to policies and rules on the five suggested areas, assessing the investment degree and the use of technologies to guarantee each one of these areas. The weights of the questions were defined in an empirical way, and the information area has a higher number of questions than the other areas due to the fact that it is the analysis focus of the model. The mentioned areas have an assigned weight of: 30% for information, 25% for hardware, 25% for software, 15% for employees and 5% for facilities. These weights are an adaptation to what is suggested in the groups of ISO/IEC 27002.

Figure 2 below is a comparison of results from the analysis of different companies.

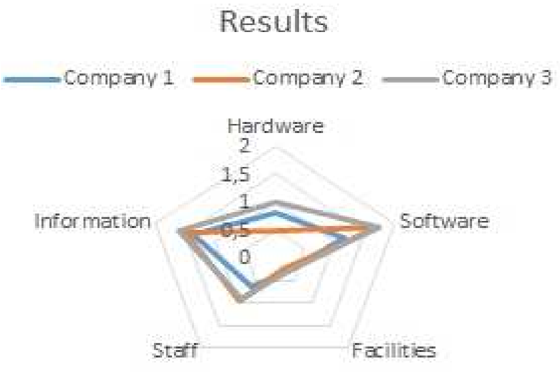

Figure 2. Results.

According to figure 2, Company 1 and 2 are at Level 1 maturity in information security. Meanwhile, Company 3 is at Level 2. Results show that the software area has more investment than others and facilities area has the lowest investment. A monitored environment may be able to inhibit harmful actions caused by employees or people who do not work in the organization. However, if the company does not provide training in accordance with the rules and punishments applied to employees, they face the risk of information security threats caused by internal factors.

These results indicate that there are more weaknesses than strengths in processes of the assessed networks, leaving companies with a level of information security level which is fragile and more susceptible to certain information security situations. Thus, companies should check and improve their processes, and directors may have GAIA-MLIS system as an analysis tool.

The system has proved to be efficient in indicating what level of maturity in information security the companies fall under. Figure 3 shows the trend lines for the three companies analyzed. These lines show their current status. Thereby, the results obtained in the tests enable defined strategies for improving processes and also indicate what their weaknesses are.

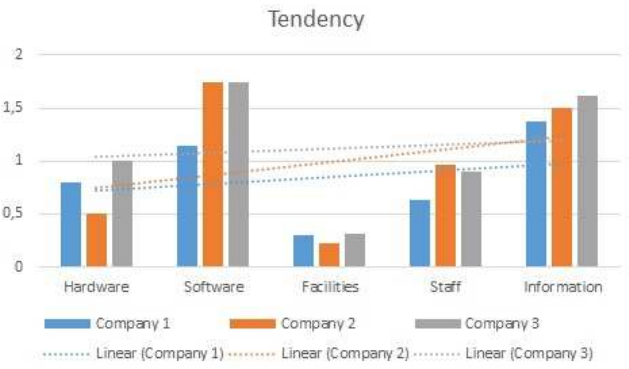

Figure 3: Tendency.

The GAIA-MLIS model contributes to a better management of information assets, analyzing five areas (hardware, software, staff, facilities and information), aiming to formalize metrics and levels of security. It creates value, in the sense that it allows for planned investments and formal documentation, defining standards and procedures for IT processes.

V. Conclusion

We presented the GAIA-MLIS model that aim to analyze maturity level for information security in enterprise, observing five areas (hardware, software, staff, facilities and information) through a diagnostic evaluation. We used three enterprise as object of analysis and we may see strengths and weaknesses in their areas of safety. With the results, we may evaluate what are the strengths and weaknesses of enterprise in each area, and what needs investments to improve the information security level.

The model helps organizations focus their efforts to solve specific problems in each one of the areas where the diagnostic evaluation identified a problem. The questionnaire application allows the exact identification of the area that needs investments in order to strengthen the security and, thus, improve the maturity level of the organization.

The flexibility of the analysis demonstrates that GAIA-MLIS system is able to state clearly the needs of each evaluated area. With the obtained results, the CIOs discuss the investment needs for all evaluated areas. Therefore, the CEO knows that the organization must change or create new policies and targets in order to aim at a better standard for the level of information security, demonstrating to partners and customers their concern with the integrity of all company assets, mainly with information.

Companies should establish policies and goals to aim for a higher level of security. GAIA-MLIS system provides companies metrics to identify the strengths and weaknesses of the processes. Investment in equipment and software techniques are important. However, if employees are not committed and if there is no a physical infrastructure able to protect the information assets, the organization will not be able to provide security for its network.

The proposed model achieved its objective of performing a security diagnosis evaluation, more specifically in hardware, software, people, facilities and information. It also helps the organizations on focus efforts to solve specific problems in each one of the areas in which the diagnostic evaluation found a problem.

An advantage of the model is the simplicity and the fast way with which it evaluates and diagnoses security maturity levels on the proposed subareas.

The corrective actions are directed according to the result of the diagnostic evaluation, and they aim to define policies of investment and adjustment on the analyzed areas in order to improve the information security.

In future works, we intend to analyze other companies separated by sector (service provider, public agencies, etc), aiming to adjust and improve the results according to characteristics common to organizations.

ACKNOWLEDGEMENTS

This work was supported by: SETI/Fundação Araucária and MCT/CNPq for Betelgeuse Projects' financial support.

REFERENCES

[1] R. V. Solms, K. L. Thomson and P. M. Maninjwa, “Information security governance control through comprehensive policy architectures”, Proc. IEEE ISSA, IEEE Press, Aug 2011, pp 1-6.

[2] X. Yuan, Y. Zhou and Z. Qian, “Information Security of Power Corporations and its Reinforcement Measures”, Proc. IEEE CICED, IEEE Press, Sep 2012, pp 1-7.

[3] P. I. Wang, “Information Security Knowledge and Behavior: An Adapted Model of Tecnology Acceptance”, Proc. IEEE ICETC, IEEE Press, June 2010, pp v2-364 – v2-367.

[4] L. Qingguo and Z. Wei, “Strengthen Militaru Academy's Information Security Management”, Proc. IEEE MINES, IEEE Press, Nov 2009, pp 182 – 186.

[5] J. Zhang, W. Yuan and W. Qi, “Research on Security Management and Control System of Information System In IT Governance”, Proc. IEEE CSSS, IEEE Press, Jun 2011, pp 668-673.

[6] P. Weill and J.W. Ross, IT Governance: How top performers manage IT decision rights for superior results, Boston: Harvard Business Press, 2004.

[7] M. Sajko and N. Hadjina, “Information Security Governance and How to Accomplish it”, Proc. IEEE MIPRO, IEEE Press, May 2011, pp 1516 – 1521.

[8] K. Sun, S. Jajodia, J. Li, Y. Cheng, W. Tang and A. Singhal, “Automatic Security Analysis Using Security Metrics”, Proc. IEEE MILCOM, IEEE Press, Nov 2011, pp 1207-1212.

[9] ISACA, COBIT 5, A Business Framework for the Governance and Management of Enterprise IT. ISACA. 2012.

[10] ISO/IEC, Information technology – Security techniques – Information security management system - Requirements. ISO/IEC. 1ed. 2005.

[11] ISSO/IEC, Information technology – Security techiniques – Code of practice for information security management. ISO/IEC. 1ed. 2005.

[12] M. Moyo, H. Abdullah and R. C. Nienaber, “Information Security Risk Management in Small-Scale Organisations: A Case Study of Secondary Schools Computerised Information Systems”, Proc. IEEE ISSA, IEEE Press, Aug, 2013, pp 14 – 16.

[13] L. Hong-li and Z. Ying-ju, “Measuring effectiveness of information security management”, Proc. IEEE CNMT, IEEE Press, Jan, 2009, pp 1 -4.

[14] M. Ratchakom and N. Prompoon, “A Process Model Design and Tool Support for Information Assets Access Control using Security Patterns”, Proc. IEEE JCSSE, IEEE Press, May, 2011, pp 307 – 312.

[15] M. Simonsson and P. Johnson, “The IT organization modeling and assessment tool: Correlating IT governace maturity with the effect of IT”, Proc. IEEE HICSS, IEEE Press, Jan, 2008, pp 1 – 10.

[16] L. Krautsevich, F. Martinelli and A. Yautsiukhin, “Formal Analysis of Security Metrics with Defensive Actions”, Proc. IEEE UIC/ATC, IEEE Press, Dec, 2013, pp 458 – 465.

[17] A. Chakraborty, A. Sengupta and C. Mazumdar, “A Formal Approach to Information Security Metrics”, Proc. IEEE EAIT, IEEE Press, Dec, 2012, pp 439 – 442.

[18] B. Karabey and N. Baykal, “Information Security Metric Integrating Enterprise Objectives”, Proc. IEEE ICCST, IEEE Press, Oct, 2009, pp 144 – 148.

[19] J. Anttila, K. Jussila, J. Kajava and I. Kamaja, “Integrating ISO/IEC 27001 and other managerial discipline standards with processes of management in organizations”, Proc. IEEE ARES, IEEE Press, Aug, 2012, pp 425 – 436.

[20] A. Iqbal, D. Horie, Y. Goto and J. Cheng, “A Database for Effective Utilization of ISO/IEC 27002”, Proc. IEEE FCST, IEEE Press, Oct, 2009, pp 607 – 612.

[21] E. Gomede, M. L. Proença JR and R. M. Barros, “Networks Baseline and Analytic Hierarchy Process: An Approach to Strategic Decisions”, IADIS International Conference Applied Computing 2012, 2012, Madrid. Processing of IADIS International Conference Applied Computing 2012. Madrid, 2012. p. 34-41.

[22] M. L. Proença JR, C. Coppelmans, M. Bottoli and L. S. Mendes, “Baseline to help with network management”, ICETE 2004 – Springer. (Org.). e-Business and Telecommunication Networks. Dordrecht: Springer, 2006, v. 1, p. 158-166.