Service Management for Cybersecurity Projects: Defining a service management strategy under Cybersecurity framework and ITIL

Luis G. Morones-Alderete[1], José E. Guzmán-Mendoza[1], Paola Y. Reyes-Delgado[1], Jaime Muñoz-Arteaga[2], Héctor Cardona-Reyes[3]

1 Universidad Politécnica de Aguascalientes, Dirección de Posgrados e Investigación, 20342 Aguascalientes, México
2 Universidad Autónoma de Aguascalientes, Departamento de Sistemas de Información, 20131 Aguascalientes, México
3 CIMAT Zacatecas, Pendiente 36023 Zacatecas, México

Abstract

Cybersecurity is now a real concern in all companies around the globe, new threats and risks are discovered day by day, and the cybersecurity organizations inside the companies and the IT services companies needs to be up to date regarding threat management, risk management, information security, network management, etc. A lot of new standards and methodologies that helps to improve the cybersecurity and mitigate the risk level are available now, but most of them are not oriented to the service management, now, the cybersecurity organizations beside to ensure the security of the company, has the responsibility to delivering high quality services, cybersecurity needs to be watched as an IT project, and a service management strategy to accomplish the goal of delivering quality services and products needs to be applied. Using the most commonly used frameworks for IT service management along with security standards and maturity models a strategy for service management inside cybersecurity organizations can be proposed for further implementation.

***Keywords* — Cybersecurity, methodologies, framework.**

I. INTRODUCTION

The cooperation between different teams in every aspect on the organizations now is a need, the informatics systems beside to provide a fast and easier way to complete the organizations goals brings to the front the need of cooperation between the teams, different teams or areas of an organization now are not isolated and the success depend on how they interact between them.

Cybersecurity is not the exception, there are a lot of different software and technologies that are used to meet the organization's standards of security and these technologies are managed by different teams, even to have these ones in place is needed the cooperation of different teams that maybe are not related to cybersecurity directly, but this cooperation shows that cybersecurity is not responsibility only for the the network team, just as an example, cybersecurity is responsibility of all the organization.

There are a lot of different methodologies and frameworks that could help to understand how an organization can meet the cybersecurity needs but there are not a standard strategy or framework that could help the organization to join the cybersecurity goals with a management strategy that could help them also to measure their maturity on the processes related to cybersecurity.

II. RELATED WORKS

It can't be denied that the informatics systems are presents in how we organize and manage a lot of aspects of or life, a lot of industries trusts huge amounts of data to their informatics systems including a lot of personal information from a big number of people, but beside the efforts to automatize and make easier our life, there is a constant need to make most secure systems and reduce the probability of being attacked by malicious people ore organizations, that could represent that a lot of sensitive data could be lost or leaked.

Kemmerer [1], defines cybersecurity as "defensive methods used to detect and thwart would-be intruders. The principles of computer security thus arise from the kinds of threats intruders can impose", and Rea-Guaman[2] sustains that the efficiency, effectiveness and sustainability of the cybersecurity implementations in an organization depends on how this one is boarded.

Since cybersecurity implementations depends on the organization needs, "the choosing of one direction can be at the expense of another direction, whereas there are arguments for going both ways" [3].

As part of Cybersecurity the Information Security Management (ISM) is defined in ITIL library "as the Process that ensures the Confidentiality, Integrity and Availability of an organization's Assets, information, data and IT Services" [4].

"Supported by the need for confidentiality, integrity, availability and other concerns, security features have become standard components of the digital environment which pervade our lives requiring use by novices and experts alike" [5].

But even when the most used IT governance and management frameworks includes cybersecurity

recommendations, such as COBIT and ITIL "these frameworks have a very limited focus on cybersecurity, with a small number of controls considered alongside other areas like service desks" [6].

Payette [7] confirms that there is already enough related precious work that could give a perspective about how cybersecurity is managed under the IT project management, but also Payette [7] says that right now, the IT project management methodologies, standards or frameworks are not oriented to provide cybersecurity beside the good practiced that those standards proposed to the correct management of the project.

"Current cybersecurity capability maturity models overwhelmingly focus on evaluating how organizations protect existing systems (i.e., processes to maintain cybersecurity) rather than evaluating how organizations securely develop and deploy new secure information systems (i.e., processes to create cybersecurity)" [7].

Even inside the teams coexists different technologies and the needing to coordinate between them is more relevant day by day, there is not a service management strategy that can help to standardize the service under the cybersecurity framework created by NIST., which is an adaptable or flexible document for its application even though it was designed for the security of banking institutions [8].

"Integration of security best practices like ISO/IEC 27001 into service management best practice processes like ITIL enables the organization to lower the overall cost of maintaining acceptable security levels, effectively manage risks and reduce overall risk levels" [9].

Miron [10] proposes the usage of maturity models to have a trustable source to measure and report on how the organization is handling and implementing cybersecurity with the usage of frameworks.

The maturity models on cybersecurity considers the cybersecurity through different areas/dimensions, understanding that each dimension is not necessarily independent from the other ones.

Finally, Donaldson[11] propose that one of the most important steps to get the organization protected against cyberattacks is to organize people.

III. STATEMENT OF THE PROBLEM

The way to work for the cybersecurity areas is not the same than a few years in the past, now beside of the rules and standard processes to keep the information´s security, cybersecurity areas are divided in different teams that needs to cooperate be-tween them, there is not a standard of operations for the different areas of cybersecurity, the network areas need to coordinate whit Infosec areas, Infosec areas needs to coordinate with cryptography areas, the needing to share information and support between them is a reality that helps to ensure the best results.

A standard that helps to coordinate this cooperation and kept a high level of security on the business infrastructure is now a needing.

IV. SOLUTION PROPOSAL

Develop a strategy derived from IT project management methodologies that is focused on the administration of cybersecurity areas.

A. Phase I – Analysis

The first task on this phase is to know the enterprise organization, in every organization exists the CIO (Chief Information Officer) and CISO (Chief Security information Officer) positions, may have different names or be merged into the same position, however, following the standards proposed by ITIL these two positions exist and in each there are large areas shown below:

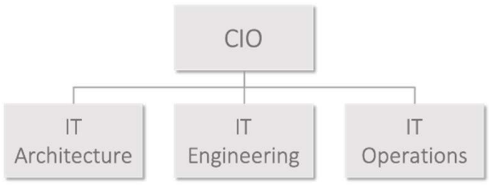

Fig. 1. Organizational chart for the CIO organization baseb on ITIL[11]

CIO is the highest IT authority, under the CIO organization there are another roles:

•IT Architecture: is responsible for guiding the architecture and strategy of the IT organization.

•Engineering: is responsible for designing, implementing, maintaining and withdrawing business technologies. A key principle of ITIL is a formal separation of engineering functions from operations functions to reduce costs and guarantee responsibility.

•Operations: are responsible for operating IT technologies efficiently and profitably in accordance with formal service level agreements (SLA).

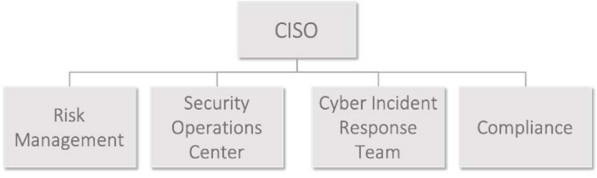

Fig. 2. Organizational chart for the CISO organization (Donaldson, 2015).

The CISO, like the CIO, is the highest authority for cybersecurity, there are four principal functions under cybersecurity organization:

•Risk Management: includes evaluation of assets, vulnerabilities, threats and risks, defining policies to manage those risks, committing to IT projects to identify and manage risks due to business changes.

•Security Operations Center (SOC): involves the operation of security controls and services on an ongoing basis to maintain company security and identify cyber incidents when they occur.

•Cyber Incidents Response Team (CIRT): is responsible for responding to cybersecurity incidents and supervising their investigation and remediation.

•Compliance: is responsible for compiling security infrastructure and operational artifacts that provide evidence that security controls and policies are functioning as planned.

The research will focus on the organization in charge of the CISO, specifically the area of SOC (Security Operations Center).

Inside this area there are technologies that provides to the organization an easiest way for monitoring, tracking, administration, cryptography, etc.

These technologies must be managed under the service life cycle and a system proposed by ITIL and must comply with the security standards proposed by frameworks and libraries dedicated to cybersecurity.

Under this subarea there must exist the positions or roles proposed under the management of the CIO, the architecture, engineering and daily operations of the different technologies that supports many of the cybersecurity tasks.

After get knowledge about organization the next step will be identify where the enterprise is positioned regarding the cybersecurity service, identify how the enterprise deals with their information and how they protect it.

According to the needs of the organization, identify which is the main need according to the information that is handled:

•Confidentiality.
•Integrity.
•Authenticity.

To minimize the impact and control possible threats during the service life cycle, as mentioned above, must be defined what is more important to handle the information, high confidentiality, low integrity and low authenticity, or Different possible combinations.

TABLE I.
Table showing different security scopes for information (Donaldson 2015).

Security Scope Type	Confidentiality	Integrity	Availability
Non-Critical	*Low/Med*	*Low/Med*	*Low/Med*
Confidentiality Critical	*High*	*Low/Med*	*Low/Med*
Integrity Critical	*Low/Med*	*High*	*Low/Med*
Availability Critical	*Low/Med*	*Low/Med*	*High*
Confidentiality Non- Critical	*Low/Med*	*High*	*High*
Integrity Non-Critical	*High*	*Low/Med*	*High*
Availability Non-Critical	*High*	*High*	*Low/Med*
All factor Critical	*High*	*High*	*High*

According to (Donaldson, 2015) The eight security scope types can be defined as follows:

•A non-critical security scope is where none of the three factors is critical and there is tolerance for failures of all three factors. Most business administrative systems fall into this category.

•A confidentiality critical scope is where data needs to be protected from breach or disclosure, but integrity and availability are not major concerns. Employee data is an example of this category.

•An integrity critical scope is where data integrity is of concern, but confidentiality and availability are not major concerns. Internal financial systems tend to fall into this category.

•An availability critical scope is where systems need to be highly available, and confidentiality and integrity are not major concerns. Public-facing web sites tend to fall into this category.
•A confidentiality non-critical scope is where availability and integrity are critical, but confidentiality is not. An example of this scope is an enterprise directory that is used for authentication and access control.

•An integrity non-critical scope is where confidentiality and availability are critical, but integrity is not. This scope type is seldom used.

•An availability non-critical scope is where confidentiality and integrity are critical, but availability is not. An example of this scope is a customer account or application where data must be carefully protected, but temporary outages are acceptable.

•An all-factors critical scope is where confidentiality, integrity, and availability are all critical, and there is little tolerance for failures of any kind. Examples of this scope are online transaction processing systems (for example, amazon.com) and the security infrastructure that supports those systems. Security infrastructure needs to operate at the highest security and availability levels.

The next step is to identify the basic objectives, the Operations Team from the SOC must achieve the following objectives to

ensure that a quality service will be delivered using standard that will help to maintain the risk levels between the allowed levels:

•Infrastructure: ITIL defines infrastructure assets as "layers defined in relation to the assets they support, specially people and applications. They include information technology assets such as software applications, computers, storage systems, network devices, telecommunication equipment, cables, wireless links, access control devices and monitoring systems" (Cannon, D., 2011).

•Supporting Policies, Services, Processes, and Tools: Policies, services and processes must have a privileged place in a strategy, these elements are the backbone to deliver a strategy that will provide value to the organization.

•Operating Systems and Applications: Operating systems and Application must be considered as an essential asset and must be considered as an important part of the strategy, upgrades, patches, vulnerabilities.

B. Phase II. Identify the Maturity of the Objectives and Activities

On phase II the maturity of the processes of the organization will be established, the parameters to determinate the maturity level of the processes (objectives and activities) are reviewed and the requirements needed to achieve a level up on the maturity levels.

The basics of CMMI was onboarded previously on the Theorical Framework, the level where the organization is located depends on how the organization manage all their processes, the criteria is shown below:

Level 1: Chaotic

•Not defined Processes.
•Not processes documented.
•Unpredictable behavior of the environment.
•Minimal IT operations

Level 2: Managed

•Only waiting on incidents to happen.
•Have only a basic list of components.
•No problem investigations.
•No plans or track of activities occur.
•The organization provides adequate resources.
•The organization assigns responsibilities and trains people.
•The adherence to processes starts to be evaluated

Level 3: Defined

•A standard for processes is stablished and replicated to lower-level processes.
•Proactive analysis leading to creation of problem investigations.
•Inventory contains all details, including end-of-life information.
•OS and App patching and upgrade efforts happen during a specific window and do not wait on others to report.
•Alerts and logging monitor and report on events related to performance, not only on basic events.
•Documenting ongoing activities and keeping track of progress and ownership.

Level 4: Quantitative Measure

•Performance and availability reports are generated and published.
•Full asset and configuration management is in place and live reports can be accessed.
•Critical and high issues are prevented by the detection and elimination of thresholds.
•Automation for well-known issues is in place.
•Clear plan for continual improvement is documented and followed along the cycle.

Level 5: Optimizing

•Innovation and improvement plans are aligned with stakeholders' goals and are reviewed periodically with them.
•Availability reports are reviewed periodically with stakeholders and management.
•Asset and configuration management is reported live and is updated with any change to the infrastructure.
•Patching and upgrades status are reported and accessible to stakeholders.
•General operations reports/dashboard is available to stakeholders.
•Hardware and software are upgraded or replaced according to a plan (done long before their EOL).

As proposed by CMMI, the organization only can achieve a level when all the criteria is accomplished, each activity of every objectives and every objectives described on section 5.1.3, must be evaluated to determinate the level where belongs according on if the activity and/or objective is executed and if so, how is executed.

TABLE II
Matrix to evaluate objectives.

[C]haos(level 1)
[M]anaged (level 2)
[D]efined (level 3)
[Q]uantitative Measure (level 4)
[O]ptimazing (level 5)
[N/A]Not Applicable

Current Level	Goal	Description

V. PHASE III. MAKING A STRATEGY

There is not a magic recipe that will help an organization to have all the elements to provide a quality service but is not a

secret neither that the first step to achieve it is to start defining standardized processes.

Remember that process is a leverage point for an organization's sustained improvement, so the core of a strategy is to develop the processes that will define how to complete successfully each one of the basic activities that compose an objective.

With this information we will define the strategy as a set of standardized processes developed to successfully complete each one of the activities related to each specific object that will drive the organization to develop a quality service.

Each organization must develop their own processes according to their own needs, and each organization must select the activities and objectives that will help them to achieve their goals.

On this paper there is a selection of activities and objectives that could help an organization to achieve their goals, but the use of this set is not restricted only to those objectives and activities, if the organization believes that is necessary to add or remove objectives and activities, they could do it to adjust it to their needs.

VI. CONCLUSIONS

This research contributes to have a standardized, structured and improvable processes inside the organizations, focused on the Cybersecurity areas, as mention previously in this research, these areas has no balance between management, measure of processes and security, these area's main purpose is to maintain the security on the entire organization and is pretty common the inexistence of documented and standardized processes for their daily operations, with this strategy these areas will have a base of activities and objectives that will help them to align to the goals and standards of the entire organization.

REFERENCES

[1] R. Kemmerer, "Cybersecurity," 25th International Conference on Software Engineering, 2003. Proceedings., 2003.

[2] Rea-Guaman, Á. M., Sánchez-García, I. D., San Feliu Gilabert, T., & Calvo-Manzano Villalón, J. A. (2017). Modelos de madurez en ciberseguridad: una revisión sistemática.

[3] J. Nurse, et al. "Guidelines for usable cybersecurity: Past and present". In 2011 third international workshop on cyberspace safety and security (CSS). IEEE. p. 21-26, 2011.

[4] J. Clinch." ITIL V3 and information security. Best Management Practice", 2009.

[5] J. Nurse, et al. "Guidelines for usable cybersecurity: Past and present". In 2011 third international workshop on cyberspace safety and security (CSS). IEEE. p. 21-26 , 2011.

[6] D. D. Goss,. Operationalizing Cybersecurity—Framing Efforts to Secure US Information Systems. The Cyber Defense Review, 2(2), 91-110, 2017.

[7] J. Payette, et al. Secure by design: Cybersecurity extensions to project management maturity models for critical infrastructure projects. Technology Innovation Management Review, vol. 5, no 6. 2015.

[8] L. Shen, "The NIST cybersecurity framework: Overview and potential impacts". Scitech Lawyer, vol. 10, no 4, p. 16., 2014.

[9] R. Sheikhpour, N. Modiri. "A best practice approach for integration of ITIL and ISO/IEC 27001 services for information security management". Indian journal of science and technology, vol. 5, no 2, p. 2170-2176, 2012.

[10] W. Miron, K. Muita. "Cybersecurity capability maturity models for providers of critical infrastructure". Technology Innovation Management Review, vol. 4, no 10, 2014.

[11] S. E. Donaldson, et al. "Cybersecurity frameworks. En Enterprise Cybersecurity". Apress, Berkeley, CA, p. 297-309, 2015.C.J. Kaufman, Rocky Mountain Research Laboratories, Boulder, CO, private communication, 2014.