Calculation Model of the Status and Staffing for Security Management – A Case Study

Lilian Noronha Nassif, Daniel Silva Carnevalli
Information Technology Department, Public Ministry of Minas Gerais, Belo Horizonte, Minas Gerais, Brazil
liliannassif, dcarnevalli{@mpmg.mp.br}

Abstract - *Security management involves a great variety of themes. The easiest way to make an organization more secure is by installing and appropriately configuring several security tools. Nevertheless, this is insufficient. Usually processes and methodologies are put in a second plane, allowing gaps that can be explored. However, analyzing whether an enterprise security status is adequate and if the number of security staff is sufficient remain difficult. This work presents a method to measure the security status in an organization. It also presents an analytical model with metrics to calculate the security staff size. Both models are simulated using real data collected in surveys from 28 organizations. The results are feasible and can be used as benchmark.*

Keywords: *security metrics; information security management; security auditing*

1 Introduction

Information security management is a dynamic area. Technological factors alone cannot prevent security problems. Other factors such as institutional organization, supplier interactions, and information security training of users and the Information Technology (IT) team are also key instruments to provide confidentiality, integrity, and availability of information resources.

A challenge that Chief Information Officers (CIOs) face is determining how many people are necessary to manage security issues. This decision must consider several factors such as environment complexity and security attributions.

This paper presents comprehensive analytical models to calculate the information security status in an enterprise and the security staff required. A survey with 51 questions was conducted within 28 organizations. The results can help IT leaders structure their security departments according to their main faults and compose a security team appropriately.

The paper is structured as follows: section 2 presents studies about security demands and staff sizing. Section 3 presents a case study conducted in 28 organizations. Section 4 shows our models to calculate the security status and staffing, presenting real numbers according to metrics obtained from interviews. Finally, section 5 concludes the paper.

2 Information security management and staffing metrics

Defining the information security department procedures and the number of staff to carry on such procedures are elementary aspects that concern IT leaders. The following sections discuss information security management and IT staffing metrics based on standards and surveys.

2.1 Information Security Management

The activities associated with information security management are widely discussed in IT. Standard organizations such as the International Organization for Standardization (ISO) [1], the Control Objectives for Information and related Technology (COBIT) [2], and the Information Technology Infrastructure Library (ITIL) [3] propose guidelines that can be widely applied in organizations. The focus of this paper is on the ISO 27001:2013 [4], as it is a detailed description about the suite of activities concerning information security management.

Adopting an Information Security Management System (ISMS) is a strategic decision for an organization. The ISO 27001:2013 standard was prepared to provide a process model to implement, maintain, and improve the ISMS. This standard defines 114 controls grouped in 14 domains as related below:

1. Information security policy
2. Organization of information security
3. Human resources security
4. Asset management
5. Access control
6. Cryptography
7. Physical and environmental security
8. Operations security
9. Communications security
10. System acquisition, development, and maintenance
11. Supplier relationships
12. Information security incident management
13. Information security aspects of business continuity management
14. Compliance

Although the ISO 27001:2013 standard is one of the most complete references about IT security activities, it must be

adapted to the individual institution objectives, processes, employees, size, and structure. Section 3 presents real data of these domains in 28 organizations.

2.2 IT staffing size metrics

An efficient management must adjust the staff size according to work necessities and environment reality. The following studies relate which metrics can help estimate the number of people on the information security staff.

The Computer Security Institute (CSI) estimated that an information security team is composed of 3% to 5% of an IT team [5].

The work conducted by Computer Economics in 2008 relates that an information security team corresponds to 2% of an IT team. This study refers to security teams limited to security auditing, management, developing, and policy and process implementations. This low percentage is because other groups contribute to ensure the information security at the organization, including network and system administrators, helpdesk, and other operational areas[6].

Another study made in 2003 by Deloitte Touche Tohmatsu (DTT) recommends one information security professional for each 1,000 users [6].

A study realized in a university environment by Educause, concluded that one information security professional is necessary for every 5,000 interconnected network devices [7].

Vostrom [8] presented another way of calculating the adequate number of professionals on an information security team. The analysis was made considering the time spent on each security topic. The calculation model used the concept of Full Time Equivalent (FTE) and is presented in Table 1. The FTE is a method that measures employee workload in a year contract. An FTE of 100% means the employee is a full-time worker, while an FTE of 50% means the employee is a part-time worker. Table 1 shows that 3.8 people/year in a minimal situation and 6.15 people/year in an ideal situation would be necessary to execute information security functions.

Although these studies confirm that some best practices are related to IT security team size, it is important to consider other factors such as environment complexity and the quality of the IT solutions. The next section presents a case study that identifies such questions.

Table 1: Amount of time spent per key security area. Source [8]

Security Staff Function	**Ideal % of time**	**Minimum % of time**
Audit	50%	35%
Physical Security Technologies	10%	5%
Disaster Recovery / Contingency Planning	25%	15%
Solution Investigation / Procurement	15%	5%
Security Education, Training, and Awareness	100%	75%
Personnel / Credential Issues	100%	75%
Risk Management / Planning	50%	15%
System and Network Management	100%	50%
Telecommunications Security	50%	25%
Helpdesk	15%	5%
Maintenance of Security Program	100%	75%
TOTAL	**6.15 staff years**	**3.80 staff years**

3 Case Study

The demand for information security services was identified in a case study addressed to 28 CIOs from different state government organizations. The study contained 51 questions concerning aspects of the methodology described in [9], the quantitative metrics described in section 2, the 27001:2013 standard [4], and the IT security benchmark conducted by Wisegate [10].

The study involved a total of 76,651 employees, 2,101 IT employees, and 117,036 units of interconnected equipment.

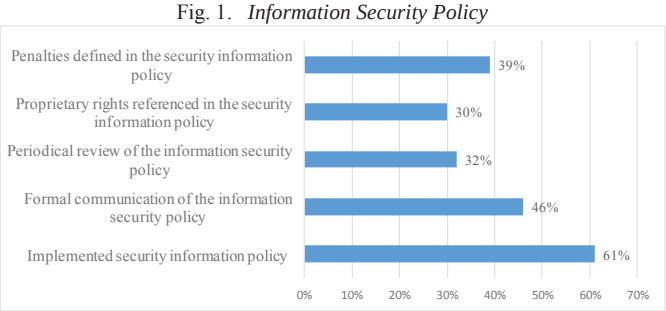
These organizations can be defined as: 57% having fewer than 2,000 employees, 56% having an IT team up to 50 employees, and 48% having fewer than 2,500 units of interconnected equipment.

The following sections 3.1 to 3.14 analyze all obtained answers according to each domain in the 27001:2013 standard.

3.1 Information Security Policy

The domain "information security policy" is presented in Figure 1. It shows that 61% of participants had an information security policy. Nevertheless, this policy was reviewed in only 32% of organizations and formally communicated to employees in only 46%. It is also possible to verify that the security policy was frequently incomplete, since 30% neglect to mention intellectual properties, and 39% include no penalties for policy violations.

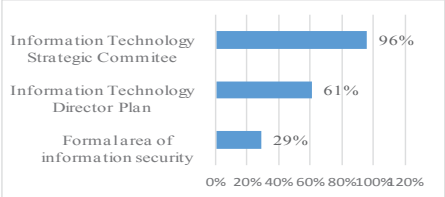
Fig. 1. *Information Security Policy*



3.2 Organization of Information security

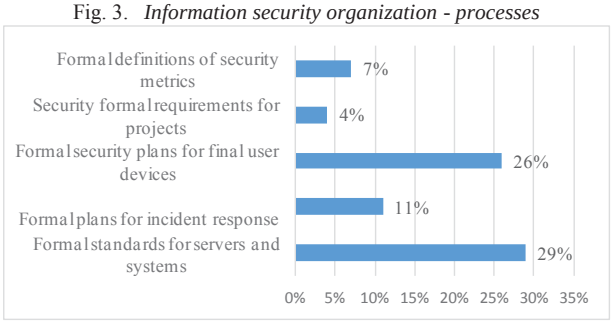
The domain "organization of information security" is presented in Figure 2. It shows that only 29% of participants had a formal information security area installed. However, 61% had an Information Technology Director Plan, and 96% had an Information Technology Strategic Committee.

Fig. 2. *Information security organization – structures*



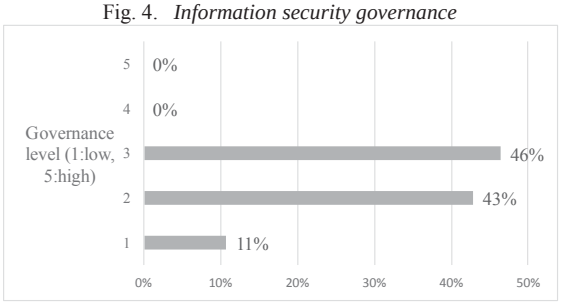
Nevertheless, Figure 3 demonstrates that only 29% of participants had formal standards for servers and systems, 11% had formal plans for incident responses, 26% had security plans for final user devices, only 4% had formal security requirements for projects, and 7% had formal definitions for security metrics.

Fig. 3. *Information security organization - processes*



According to Figure 4, 46% of participants related that the information governance level was medium (3, on a scale from 1 to 5). All participants believed that the governance was below or equal to medium level.

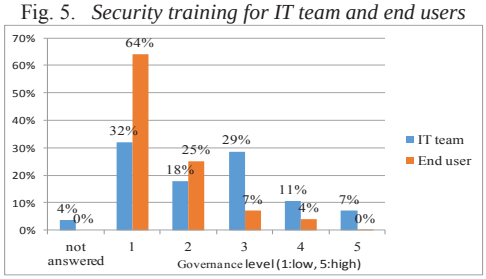
Fig. 4. *Information security governance*



3.3 Human resource security

Figure 5 presents the training level of the IT team and final users. The IT team training level in information security was below 3 for 79% of the participants. The user training level in information security was 1, for 64% of the participants.

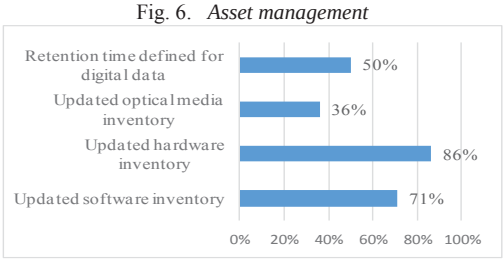
Fig. 5. *Security training for IT team and end users*



3.4 Asset management

Assets were relatively well managed. Figure 6 shows that 86% of the participants had an updated hardware inventory, 71% an updated software inventory, 36% an updated media inventory, and 50% a predetermined time to retain digital information.

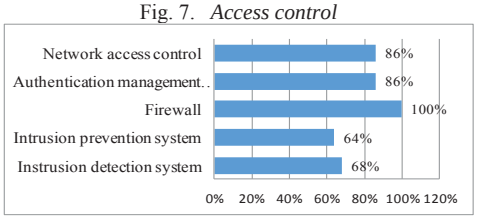
Fig. 6. *Asset management*



3.5 Access control

Access was well controlled. According to Figure 7, all participants had a firewall, 86% had an authentication system, and a network access control system, 68% had an intrusion detection system, and 64% had an intrusion prevention system.

Fig. 7. *Access control*



3.6 Cryptography

Cryptography here is associated with data transmission and storage. Figure 8 verifies the risk level of confidentiality, integrity, and availability in the environment. The risk level was 3 for 39% of participants, and 89% believed this risk level was low to medium.

Fig. 8. *Risk of confidentiality, integrity, and availability*

3.7 Physical and environmental security

Figure 9 presents aspects of physical and environment security in IT. In datacenters or server rooms, an Uninterruptible Power Supply (UPS) was installed in 96%, a fire protection system in 89%, restricted access in 79%, suspended floors in 68%, and temperature, dust, and humidity control in 57%.

Fig. 9. *Physical and environment security in datacenters*

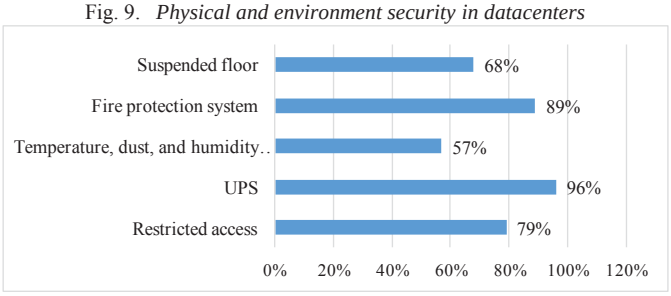
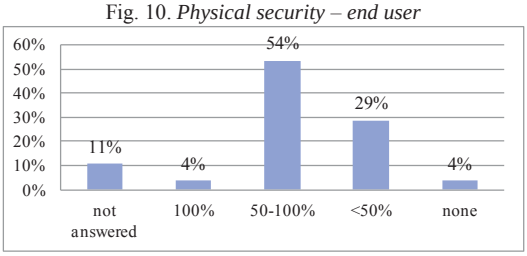


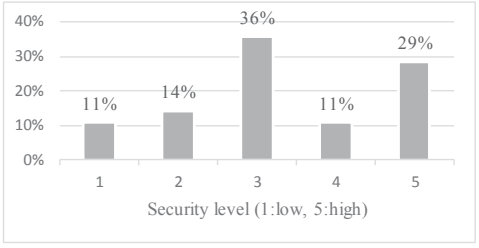
Figure 10 shows that 54% of IT leaders evaluated the physical security level for end user access between 50 to 100%, and 29% evaluated it under 50%.

Fig. 10. *Physical security – end user*



The security level of hosting environments varies from medium to high for 75% of the participants as Figure 11 demonstrates.

Fig. 11. *Server hosting*



3.8 Operations security

Figure 12 presents a list of implemented systems and processes. Backup procedures were documented by 86% of the participants; the backup was retained accordingly to the institution definition by 75% of the participants; and the backup was restored periodically by 71% of the participants. Firewall and application logs were maintained by 89% of the participants.

Fig. 12. *Operation security – installed solutions*

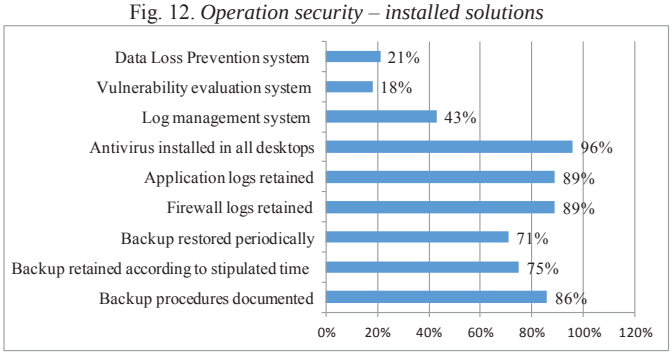
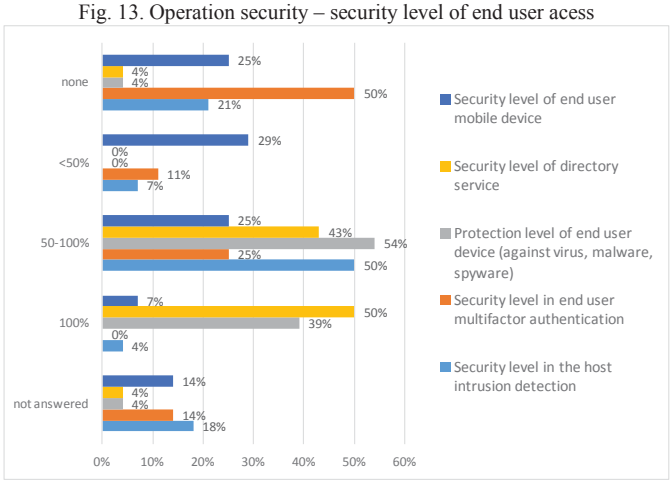


Figure 12 also shows that 96% of the participants had antivirus installed in all desktops, 43% had a log management system, 18% a vulnerability evaluation system, and 18% data loss prevention software.

Figure 13 demonstrates that from all items analyzed, the directory service had the highest trust index (100%) for half of the participants. The graph has the highest concentration in the group of 50-100% of security level.

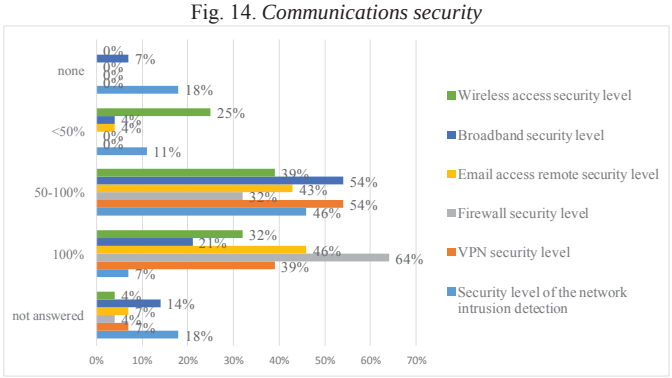
Fig. 13. Operation security – security level of end user acess



3.9 Communications security

Communications security is presented in Figure 14 under several factors. The confidence level in this service concentrates at the 50-100% range and 100%. The security level is 100% for the firewall functions for 64% of the interviewed. For 46% of the interviewed, the confidence level is 100% for email remote access.

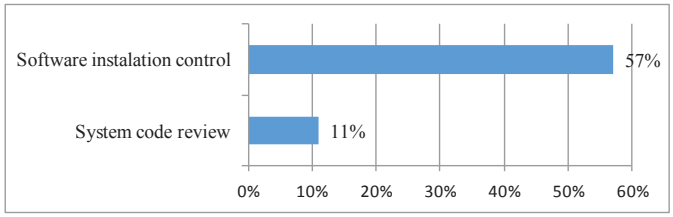
Fig. 14. *Communications security*



3.10 System acquisition, development, and maintenance

Figure 15 shows that 57% of the participants had a mechanism that avoided or controlled the installation of non-authorized software. Only 11% had code revision software.

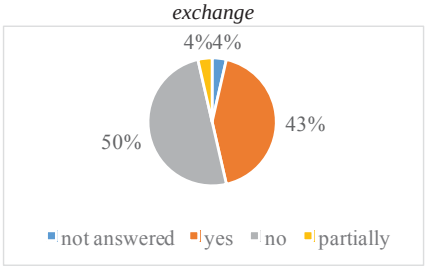
Fig. 15. *Installation control and code review*



3.11 Supplier relationships

Figure 16 demonstrates that 43% of the participants had formal third party contracts that established requirements for electronic data exchange using the internet.

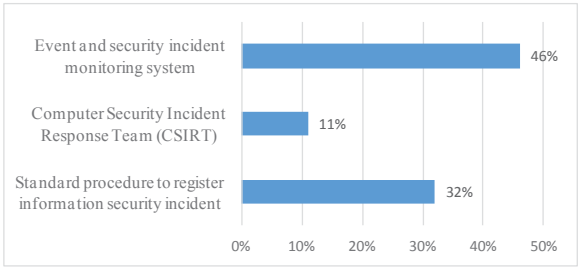
Fig. 16. *Formal third party contracts that established eletronic data exchange*



3.12 Information security incident management

Information security incident management was poorly evaluated by the interviewed. According to Figure 17, only 11% of the participants had a Computer Security Incident Response Team (CSIRT). Institutions had a standard procedure to register security incidents for 32% of the participants, and 46% had an incident and event monitoring system.

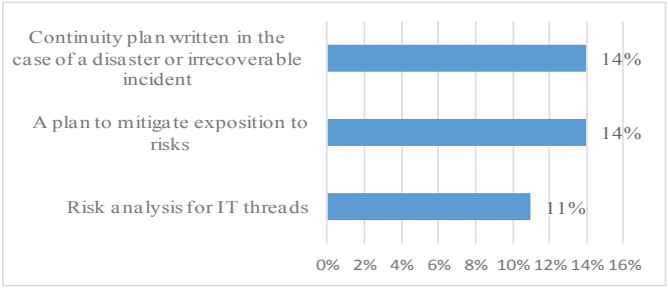
Fig. 17. *Information security incident management*



3.13 Information security aspects of business continuity management

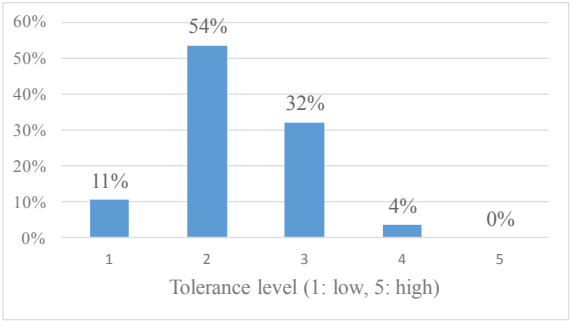
The information security aspects of business continuity management were poorly evaluated as well. Figure 18 shows that only 11% of the participants developed IT risk analysis. A small percentage (14%) of participants had a continuity plan written in the case of a disaster or irrecoverable incident that results in an inoperable IT environment. Only 14% had a plan to mitigate risk exposition.

Fig. 18. *Business continuity management*



The level of risk tolerance was poorly evaluated. In Figure 19, most of the interviewed, 54%, stated that the risk tolerance level was 2 (1:low, 5:high).

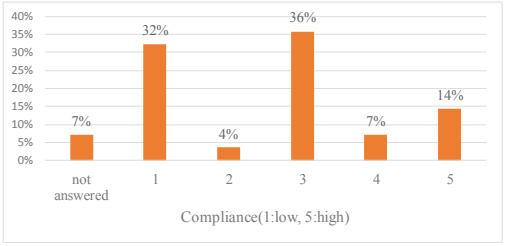
Fig. 19. *Tolerance to security risks*



3.14 Compliance

The security requirements were in high compliance to legislation, contracts, and security policy for only 14% of the participants. Figure 20 shows that 36% believed that the adherence was reasonable and indicated level 3. Nevertheless, 72% of the participants alleged that adherence was low to medium.

Fig. 20. *Compliance to legislation, contracts, and information security policy*



Vulnerability analysis verifies if the security requirements implemented are compliant to the information security policy. 50% of participants had already conducted a vulnerability analysis using a penetration test.

4 Status and staff calculation

Information security can be improved constantly if metrics are used to identify the real management state. We developed here two analytical models to calculate the security status and the staff size. Both used real data collected in the case study described in section 3.

4.1 Status calculation

The calculation of security status was based on the positive responses obtained for each domain of ISO 27001:2013. A positive response depended on the type of question used in the survey and is denoted as *positive_domain*, where:

- For questions whose answers were "yes or no", *positive_domain* is the percentage of equal answers to "yes"
- For questions whose answers were to inform "level 1-5", *positive_domain* is the percentage of responses between "3-5"
- For questions whose answers were to inform percentage, *positive_domain* is the percentage of responses for "50-100% and 100%"

Figure 21 presents the *positive_domain* calculations for all domains considered in section 3. The security status, denoted as *SecStatus* calculated the average of all *positive_domains* and is denoted by Equation (1). According to values presented in Figure 21 and Equation (1), the security status of the survey participants was 51%.

$$SecStatus = \Sigma(positive\_domain)/14 \quad (1)$$

It is important to note that the participants had good information security management for topics related to operational functions such as asset management, communication security, security operations, and physical security.

However, participants had insufficient information security management in the fields related to policy and information security procedures, human resources management, incident management, business continuity management, and compliance with legal and contractual requirements.

Considering that only 29% of the CIOs answered that they had a dedicated team to information security (Figure 2), these findings confirmed, only in this survey, that even without a dedicated information security team, operational activities were performed reasonably well with the existing team. However, the procedural and regulatory issues became impaired and pointed to the need for improvements in these themes.

Fig. 21. *Security status according to ISO 27001:2013 domains*

4.2 Staffing calculation

The staff number of the IT security team was based on several literature studies presented in section 2.2. The study results can be summarized in the following recommendations: 1) Allocate 1 IT security professional per 1,000 users; 2) Allocate 1 person in the IT security team per 5,000 interconnected devices; 3) Allocate 3% of IT staff to the security team; 4) Allocate 3.8 to 6.15 people to the execution of security activities considering FTE.

We developed below a model that considers all of these recommendations to define a multi-factor numerical value to calculate the IT security team size. The recommendations are represented as metrics, defined herein as M1, M2, M3, and M4, and the security team size is defined as *SecS*. The *metrics and SecS* are denoted in Equations (2) to (6) as:

$$M1 = nusu/1000 \quad (2)$$

$$M2 = ndis/5000 \quad (3)$$

$$M3 = nequi * 0.03 \quad (4)$$

M4 = 3.8 people (minimal situation), 6.15 people (ideal situation) (5)

$$SecS = round(\Sigma(M1,M2,M3,M4)/4)|Max=7 \quad (6)$$

Where:

nusu = number of employees in the institution
ndis = number of interconnected devices on the network
nequi = number of IT employees

Table 2 presents the calculation of IT staff size for each survey participant considering real data presented by them. The last column, *SecS*, corresponds to IT security team size calculated according to Equation 6. *SecS* calculated the averages of M1, M2, M3, and M4, and rounded the result to the next integer, maximum 7, considering the study of FTE.

Table 2: IT security team size calculation

ID	nusu	ndis	nequi	M1	M2	M3	M4	SecS
1	304	450	13	0.3	0.1	0.39	3.8	1
2	718	889		0.7	0.2	0	3.8	1
3	500	1000	15	0.5	0.2	0.45	3.8	1
4	600	1167	17	0.6	0.2	0.51	3.8	1
5	716	1200	15	0.7	0.2	0.45	3.8	1
6	1086		14	1.1	0.0	0.42	3.8	1
7	815	1427	21	0.8	0.3	0.63	3.8	1
8	842	2000	33	0.8	0.4	0.99	3.8	2
9	850	1956	40	0.9	0.4	1.2	3.8	2
10	719	1400	35	0.7	0.3	1.05	3.8	2
11	2000	1038	32	2.0	0.2	0.96	3.8	2
12	1082	2800	53	1.1	0.6	1.59	3.8	2
13	1700	2000	42	1.7	0.4	1.26	3.8	2
14	1400	2300	50	1.4	0.5	1.5	3.8	2
15	1602	2580	43	1.6	0.5	1.29	3.8	2
16	2009	4467	22	2.0	0.9	0.66	3.8	2
17	1800	1730	49	1.8	0.3	1.47	3.8	2
18	2967	4000	54	3.0	0.8	1.62	3.8	2
19	3000	4280	55	3.0	0.9	1.65	3.8	2
20	2200	8776	59	2.2	1.8	1.77	3.8	2
21	3000	4000	90	3.0	0.8	2.7	3.8	3
22	3553	5838	67	3.6	1.2	2.01	3.8	3
23	4005	8000	88	4.0	1.6	2.64	3.8	3
24	6647	10143	79	6.6	2.0	2.37	3.8	4
25	4950	10000	153	5.0	2.0	4.59	3.8	4
26	8075	12350	116	8.1	2.5	3.48	3.8	4
27	6000	6245	330	6.0	1.2	9.9	3.8	5
28	13511	15000	516	13.5	3.0	15.48	3.8	7

Two survey participants lacked some required metrics and are detached in Table 2. *SecS* was limited to security activities related to auditing, management, development, and implementation of security policies and processes as reported in the study [6] and as a result of Figure 21. The simulation of data provided in the survey using our model, synthesized in Equation 6, demonstrated that the calculation obtained for the security team size was feasible.

5 Conclusions

This paper carefully addresses information security demands and the amount of staff needed for accomplishing these tasks. From the survey with 28 participants, it was possible to characterize the strengths and weaknesses in information security governance.

IT managers can repeat this experience as a reference for analyzing their security situation to others and use the benchmark technique this work provides.

In the case study, the main difficulties encountered in information security management were related to security governance in aspects of policy, organization, human resource management, system maintenance, supplier relations, business continuity, incident management, and compliance.

Daily operational management, communications management, physical security, access control, and assets management were well rated in the case study. The security staff size proposed disconsidered operational functions, since other areas also took care of information security in the institution.

The study presented quantitative models to calculate security status and team size. The models were simulated with real data obtained in the survey.

The work produced feasible results facilitating its implementation. The calculated metrics can improve security information and help achieve more efficient management.

6 References

[1] ISO. International Standardization for Organization. http://www.iso.org.

[2] COBIT. Control Objectives for Information and related Technology. “Cobit 5 – A management guide“. Van Haren publishing. 2012.

[3] ITIL. “Information Technology Infrastructure Library“. Available at http://www.itil.org.uk/all.htm. Visited in 15/06/2014.

[4] ABNT NBR ISO/IEC 27001. “Tecnologia da informação – Técnicas de segurança – Sistemas de gestão da segurança da informação – Requisitos“. ABNT. 2013.

[5] Tipton, Harold & Krause, Micki. Information Security Management, pp 598-599. 2003.

[6] Computer economics. “IT Security staff levels are declining“. Available at http://www.computereconomics.com/article.cfm?id=1384. Visited in 27/11/2014. 2008.

[7] Pirani, Judith A. “High Stakes: Strategies for Optimal IT Security Staffing“. Educause – Center for Applied Research. 2004.

[8] Vostrom. “Rationalizing Information Security Staffing“. Available at http://vostrom.com. Visited in 27/11/2014. 2004.

[9] OISSG – Open Information System Security Group. « “Information Systems Security Assessment FrameWork (ISSAF) 2.1A “. 2006.

[10] Wisegate. “2013 IT Security Benchmark Report. Crowdsourced Survey Uncovers Key Security Program, Budget and Job Trand Data for CISOs and Security Leaders ». Wisegate Research Report. 2013.