A MULTI-CRITERIA EVALUATION OF INFORMATION SECURITY CONTROLS USING BOOLEAN FEATURES

Angel R. Otero[1], Carlos E. Otero[2] and Abrar Qureshi[2]

[1]Graduate School of Computer and Information Sciences, Nova Southeastern University, Fort Lauderdale, FL, USA
ao269@nova.edu
[2]Department of Mathematics & Computer Science, University of Virginia's College at Wise, Wise, VA, USA
cotero@mcs.uvawise.edu; aqureshi@uvawise.edu

ABSTRACT

For organizations, the protection of information is of utmost importance. Throughout the years, organizations have experienced numerous system losses which have had a direct impact on their most valuable asset, information. Organizations must therefore find ways to make sure that the appropriate and most effective information security controls are implemented in order to protect their critical or most sensitive classified information. Existing information security control selection methods have been employed in the past, including risk analysis and management, baseline manuals, or random approaches. However, these methods do not take into consideration organization specific constraints such as costs of implementation, scheduling, and availability of resources when determining the best set of controls. In addition, these existing methods may not ensure the inclusion of required/necessary controls or the exclusion of unnecessary controls. This paper proposes a novel approach for evaluating information security controls to help decision-makers select the most effective ones in resource-constrained environments. The proposed approach uses Desirability Functions to quantify the desirability of each information security control taking into account benefits and penalties (restrictions) associated with implementing the control. This provides Management with a measurement that is representative of the overall quality of each information security control based on organizational goals. Through a case study, the approach is proven successful in providing a way for measuring the quality of information security controls (based on multiple application-specific criteria) for specific organizations.

KEYWORDS

Information security; information security controls; risk analysis and management; baseline manuals; best practice frameworks; desirability functions

1. INTRODUCTION

For organizations, the protection of information is of utmost importance. Throughout the years, organizations have experienced numerous system losses which have had a direct impact on their most valuable asset, information. According to [1], losses related to information security will continue to happen and their effect will be devastated to organizations. In 2006, the CSI/FBI Computer Crime and Security Survey stated that total losses in the United States attributable to computer security breaches reached $52,494,290. Further, eight former employees of Bank of America, Wachovia, and other major banks were arrested for illegally stealing and selling account information of approximately 500,000 customers [2]. These alarming figures point to an inadequacy in today's information security practices and serves as motivation for finding new ways to help organizations improve their capabilities for securing valuable information.

DOI : 10.5121/ijnsa.2010.2401

In today's organizational culture, most information security challenges are addressed through the use of security tools and technologies, such as, encryption, firewalls, access management, etc. [3], [4]. Although tools and technologies are an integral part of organizations' information security plans [5], [6], it is argued that they alone are not sufficient to address information security problems [7]. To improve overall information security, organizations must evaluate (and thus implement) appropriate information security controls (ISC) that satisfy their specific security requirements [8], [9], [10]. However, due to a variety of organizational-specific constraints (e.g., cost, schedule, resources availability), organizations do not have the luxury of selecting and implementing all required ISC. Therefore, the selection, adoption, and implementation of ISC within organizations' business constraints become a non-trivial task.

This paper proposes a novel approach for evaluating and identifying the most appropriate ISC based on organization specific criteria. The proposed approach uses Desirability Functions to quantify the desirability of each ISC taking into account benefits and penalties (restrictions) associated with implementing the ISC. This provides Management with a measurement that is representative of the overall quality of each ISC based on organizational goals. The derived quality measurement can be used as the main metric for selecting ISC. The remainder of the paper is organized as follows. Section 2 provides a summary of previous work on ISC selection. Section 3 briefly describes the proposed solution approach. Section 4 provides detailed explanations of the Desirability Functions technique. Section 5 presents the results of a case study. Lastly, Section 6 provides summarized conclusions and highlights of the proposed approach.

2. BACKGROUND WORK

Various reasons have been put forth for explaining the lack of effectiveness in the evaluation, selection, and implementation process of ISC. Based on [11], the implementation of ISC in organizations may constitute a barrier to progress. For instance, participants from the ICIS 1993 conference panel indicated that the implementation of ISC may slow down production thereby turning the employees' work ineffective [12]. Employees may view ISC as interrupting their day-to-day tasks [13] and may, therefore, tend to ignore implementing them in order to be effective and efficient with their daily job tasks.

According to [14], organizations are required to identify and implement appropriate controls to ensure adequate information security. In [15], the authors place emphasis on the fact that "different organizations have different security needs, and thus different security requirements and objectives." In addition, [16] stress that there is no single information security solution that can fit all organizations. As a result, ISC must be carefully selected to fit the specific needs of the organization. Identification and implementation of the most effective ISC is a major step towards providing an adequate level of security in organizations [8].

2.1. Previous Approaches in the Selection of ISC in Organizations

Based on [8], the process of identifying (and selecting) the most effective ISC in organizations has been a challenge in the past, and plenty of attempts have been made to come up with the most effective way possible. Risk analysis and management (RAM) is just one example. RAM has been recognized in the literature as an effective approach to identify ISC [8]. RAM consists of performing business analyses as well as risk assessments, resulting in the identification of information security requirements [8]. RAM would then list the information security requirements as well as the proposed ISC to be implemented to mitigate the risks resulting from the analyses and assessments performed.

RAM, however, has been described as a subjective, bottom-up approach [17], not taking into account organizations' specific constraints. For example, through performing RAM, organizations may identify 50 information security risks. Nonetheless, Management may not be

able to select and implement all necessary ISC to address the previously identified 50 risks due to costs and scheduling constraints. Moreover, there may not be enough resources within the organization to implement these ISC. In this case, Management should lists all those risks identified and determine how critical each individual risk is to the organization, while considering cost versus benefit analyses. Management must, therefore, explore new ways to determine/measure the relevancy of these ISC considering the constraints just presented.

Baseline manuals or best practice frameworks is another approach widely used by organizations to introduce minimum security controls in organizations [8]. Per [14], best practice frameworks assist organizations in identifying appropriate ISC. Some best practices include: Control Objectives for Information and related Technology (COBIT), Information Technology Infrastructure Library (ITIL), and Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE). Additionally, [9] have mentioned other best practice frameworks which have assisted in the identification and selection of ISC. These are: International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) 177995 and ISO/IEC 27001, PROTECT, Capability Maturity Model (CMM), and Information Security Architecture (ISA).

The process of selecting the most effective ISC from these best practice frameworks can be challenging [17]. According to [17], best practice frameworks leave the choosing of controls to the user, while offering little guidance in terms of determining the best controls to provide adequate security for the particular business situation. Additionally, frameworks do not take into consideration organization specific constraints, such as, costs of implementation, scheduling, and resource constraints. Other less formal methods used in the past, such as, *ad hoc* or random approaches, could lead to the inclusion of unnecessary controls and/or exclusion of required/necessary controls [8]. Identifying and selecting ISC based on the above may result in organizations not being able to protect the overall confidentiality, integrity, and availability of their information [14]. In order to increase the effectiveness of the selection and prioritization process for ISC, new methods need to be developed that save time while considering major factors (e.g., constraints, restrictions, etc.) that undoubtedly affect the selection of ISC.

From the reviewed literature, it is evident that the selection of ISC is mostly driven by cost, scheduling, and resource availability. In other words, ISC at organizations will be selected by Management when the benefits of implementing them surpass the costs of establishing the control. Equally important, scheduling issues may affect whether ISC should be selected. Implementation of ISC may require specific scheduled times, not necessarily planned by the organization. Finally, availability of personnel often determines whether ISC can be selected or not. Effective information system security implementation requires the identification and adoption of the most appropriate and effective set of ISC [17] taking into account the issues presented above.

3. SOLUTION APPROACH

To properly evaluate the quality, importance, and priority of ISC in organizations, Management must follow a methodology that takes into consideration the quality attributes of the ISC that are considered relevant. The methodology must provide capabilities to determine the relative importance of each identified quality attribute. This would allow the methodology to provide an ISC selection/prioritization scheme that represent how well these ISC meet quality attributes and how important those quality attributes are for the specific organization. To achieve this, the methodology created in [18] is modified and customized to solve the problem of prioritizing ISC in organizations. First, a set of quality attributes are identified as evaluation criteria for all possible ISC. These attributes are defined in terms of different features, where each feature is determined to be either present or not. Once all features are identified, each individual ISC is evaluated against each feature using a simple binary (boolean) scale (i.e., 0 or 1). ISC that

satisfy the highest number of features would expose a higher level of quality (or priority) for that particular quality attribute. Once all ISC are evaluated and measurements computed for all features, the proposed approach uses Desirability Functions to fuse all measurements into one unified value that is representative of the overall quality of the ISC. This unified value is computed by using a set of Desirability Functions that take into consideration the priority of each quality attribute. Therefore, the resulting priority of each ISC is derived based on Management's goals and organization's specific needs. This results in an ISC evaluation/prioritization approach based on how well ISC meet quality attributes and how important those quality attributes are for the organization.

4. DESIRABILITY FUNCTIONS

Desirability Functions are a popular approach for simultaneous optimization of multiple responses [19], [20]. They have been used extensively in the literature for process optimization in industrial settings, where finding a set of operating conditions that optimize all responses for a particular system is desired [18], [21]. Through Desirability Functions, each system response y_i is converted into an individual function d_i that varies over the range $0 \leq d_i \leq 1$, where $d_i = 1$ when a goal is met, and $d_i = 0$ otherwise [20]. Once each response is transformed, the levels of each factor are typically chosen to maximize the overall desirability which is represented as the geometric mean of all m transformed responses [19]. Alternatively, when factors are uncontrollable, the overall desirability value can be used to characterize the system based on the multiple selected criteria.

Similar to the characterization of industrial processes, the evaluation of the quality and prioritization of each ISC in organizations can be approached by finding the set of criteria that provide the optimal benefit versus cost value for a particular organization. When formulated this way, Desirability Functions can be used to provide a unified measurement that characterizes the quality of ISC based on a set of predefined evaluation criteria. Once the desirability of all ISC is computed, Management can use this information to determine the relative priority of ISC and select the best ones simply by choosing the most desirable ones for a particular organization.

4.1. Computing Desirability

The first step in the Desirability Functions approach involves identifying all possible ISC that could be implemented in an organization. These ISC can be obtained from the best practice frameworks listed in Section 2. For instance, the ISO/IEC 177995 standard has over 127 ISC available according to the organizations' specific needs [14]. Once selected, the results of these ISC are captured in the ISC vector, as presented in (1).

$$X = \begin{bmatrix} n_1 \\ n_2 \\ \vdots \\ n_n \end{bmatrix} \tag{1}$$

Once the ISC vector is identified, each ISC can be evaluated against a set of quality attributes QA_1, QA_2,.., QA_n. The evaluation process takes place as follow. First, each quality attribute is defined in terms of m features, where $m > 1$. The evaluation scale for each feature is binary; that is, the feature is evaluated as being present/true (i.e., 1) or missing/false (i.e., 0). For example, ISC can be prioritized based on their Scope. In other words, ISC that provide security of information in many systems have a higher priority than ISC that address security of information in a minimal number of systems. In this case, the quality attribute *Scope* can be defined with the following features: *System 1, System 2, ..., System n*. Therefore, the highest priority ISC (based on the *Scope* quality attribute) would be one where *System 1 = 1, System 2 = 1,* and *System n = 1*. Similarly, the lowest priority ISC based on the *Scope* quality attribute is

one where *System 1 = 0, System 2 = 0,* and *System n = 0*. For quality attributes where the presence of features affects the security of information negatively (e.g., restrictions, penalties), the reverse is true. In these cases, ISC with all features present (i.e., 1) result in lower priority and ISC with all features missing (i.e., 0) result in higher priority. With this framework in place, a measurement of the importance of the j^{th} ISC based on the i^{th} quality attribute (e.g., *Scope*) can be computed using (2),

$$y_{ij} = \frac{\sum_{x=0}^{m} f_x}{m} \tag{2}$$

where m is the number of features identified for the i^{th} quality attribute. This computation normalizes the evaluation criteria to a scale of 0 – 100, where 0 represents the lowest score and 100 the highest (or backwards for restrictions or penalties). The overall assessment of the ISC set based on all quality attributes is captured using the quality assessment matrix Q presented in (3). As seen, each y_{ij} value of the matrix represents the score of the j^{th} ISC based on each individual i^{th} quality attribute. It is important to point out that the quality assessment matrix can be extended to evaluate ISC based on any quality attributes containing numerous features.

$$Q = \begin{array}{c} \begin{matrix} QA_1 & QA_2 & \cdots & QA_m \end{matrix} \\ \begin{bmatrix} y_{11} & y_{21} & \cdots & y_{m1} \\ y_{12} & y_{22} & \cdots & y_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ y_{1n} & y_{2n} & \cdots & y_{mn} \end{bmatrix} \end{array} \tag{3}$$

Finally, to assess the importance of each quality attribute, a weight vector W is created where r_i represents the importance of the QA_i quality attribute using the scale 0 – 10, where 0 represents lowest importance and 10 represents highest importance. The weight vector W is presented in (4).

$$W = \begin{bmatrix} r_1 \\ r_2 \\ \vdots \\ r_m \end{bmatrix} \tag{4}$$

Once the information from *X, Q,* and *W* is collected, desirability values for each ISC can be computed using the desirability matrix d presented in (5). As seen, each d_{ij} value of the matrix represents the desirability of the j^{th} ISC based on each individual i^{th} quality attribute.

$$d = \begin{bmatrix} d_{11} & d_{21} & \cdots & d_{m1} \\ d_{12} & d_{22} & \cdots & d_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ d_{1n} & d_{2n} & \cdots & d_{mn} \end{bmatrix} \tag{5}$$

Each individual desirability value d_{ij} for the ISC is computed according to Management based on the organization's specific needs and goals. For example, quality attributes that are represented positively by a higher y_{ij} value are transformed using the maximization function in (6) [20]. Alternatively, quality attributes that are represented negatively by a higher y_{ij} value are transformed using the minimization function in (7) [20],

$$d_{ij} = \begin{cases} 0 & y_{ij} \le L \\ \left(\dfrac{y_{ij} - L}{T - L} \right)^{r_i} & L \le y_{ij} \le T \\ 1 & y_{ij} > T \end{cases} \tag{6}$$

$$d_{ij} = \begin{cases} 1 & y_{ij} < T \\ \left(\dfrac{U - y_{ij}}{U - T} \right)^{r_i} & T \le y_{ij} \le U \\ 0 & y_{ij} > U \end{cases} \tag{7}$$

where L and U are the lower and upper limits, T is the target objective (e.g., 100 for maximization, 0 for minimization), and r_i is the desirability weight for the i^{th} quality attribute. It is important to note that (6) and (7) are the normal equations for the Desirability Function approach. However, through experimentation, it was found that the approach for ISC selection and prioritization performed better when $d_{ij} > 0$. Therefore, as heuristic, when d_{ij} is less than .0001, the d_{ij} value is set to .0001. A desirability weight of $r = 1$ results in a linear Desirability Function; however, when $r > 1$, curvature is exposed by the Desirability Function to emphasize on being close to the target objective (T). When $0 < r < 1$, being close to the target objective is less important. Once individual desirability values for each quality attribute are computed, the overall ISC desirability value can be computed using (8). As seen, each overall desirability value is computed as the geometric mean of all m individual desirability values for ISC $1, 2, \ldots, n$.

$$D = \begin{bmatrix} \left(\prod_{i=1}^{m} d_{i1} \right)^{1/m} \\ \left(\prod_{i=1}^{m} d_{i2} \right)^{1/m} \\ \vdots \\ \left(\prod_{i=1}^{m} d_{in} \right)^{1/m} \end{bmatrix} \tag{8}$$

After the overall desirability value is computed for all ISC, Management can use this value as a priority measurement derived from the predefined quality attributes and their relative importance for the particular organization.

5. CASE STUDY

This section presents the results of an ISC evaluation/prioritization case study using the proposed approach. The case study evaluates 10 ISC based on the following identified quality attributes, some of which have been defined within the ISO/IEC 177995 standard [9].

- *Restrictions* – there are restrictions that Management must take into account before selecting and implementing ISC. These may include whether the costs involved in the selection and implementation of ISC are high, whether resources are not available, and whether there are scheduling constraints associated with implementing the ISC. The presence of any of the above will negatively affect the specific quality attribute. That is, ISC with all features present will result in a lower priority; conversely, ISC with all

features missing will result in a higher priority. A high priority scenario will be one where the implementation cost of the specific ISC is considered adequate and/or manageable (e.g., within budget), resources are available to implement the particular ISC, and there are no restrictions in terms of scheduling the ISC (i.e., the ISC can be scheduled anytime during the year). Restrictions is defined as: Costs (C), Availability of Resources (AoR), and Scheduling (T).

- *Scope* – This quality attribute assesses the impact of the ISC on the organization. ISC that provide security of information in many systems have a higher priority than ISC that address security of information in a minimal number of systems. Scope is defined as: System 1 (S1), System 2 (S2), …, System n (Sn).

- *Organization's Objectives* – the number of information security objectives the ISC satisfies. The higher the number of objectives the ISC satisfies, the higher the desirability of the ISC. Organization's objectives is defined with the following features: Objective 1 (O1), Objective 2 (O2), …, Objective n (On).

- *Physical Access* – ISC will prevent and/or record unauthorized access to the organization's building facilities, including computer rooms where information processing takes place, the finance/accounting department, human resources department, etc. The higher the number of physical locations addressed by the ISC, the higher the desirability of the ISC. Physical access is defined as: Location 1 (L1), Location 2 (L2), …, Location n (Ln).

- *Access Controls* – implementation of an ISC for this quality attribute will promote appropriate levels of access controls to ensure protection of the organization's systems/applications against unauthorized activities. Organizations may implement network access controls (N), operating systems access controls (O), and application controls (A) based on their specific needs.

- *Human Resources* – implementation of an ISC supports reductions of risk of theft, fraud, or misuse of computer resources by promoting information security awareness (Aw), training (Tn), and education of employees (E) [22]. Depending on the particular situation, costs involved, and availability of personnel, organizations may select which of these to employ.

- *Communications and Operations Management* – ISC will ensure the correct and secure operation of information processing facilities, which includes addressing for adequate segregation of duties (SoD), change management (CM), and network security (NS). Organizations may select ISC to address all of these or just some depending on their particular needs.

- *Systems Acquisition, Development, and Maintenance* – ISC will support security related to the organization's in-house and/or off-the-shelf systems or applications (e.g., ensuring personnel with authorized access can move changes into production environments, etc.). The higher the number of systems or applications addressed by the ISC, the higher the desirability of the ISC. Systems Acquisition, Development, and Maintenance is defined as: Systems or Applications 1 (SoA1), Systems or Applications 2 (SoA2), …, and Systems or Applications n (SoAn).

- *Incident Management* – ensures that security-related incidents (e.g., attempts to change/manipulate financial data, etc.) identified within the organization's processing of information are communicated in a timely manner and that corrective action is taken for any exceptions identified. Incident management may apply to online processing

and/or batch processing. Incident Management is defined as Processing 1 (P1), Processing 2 (P2), …, and Processing n (Pn).

Using synthetic data for the identified quality attributes, a binary input evaluation (Table 1), and Desirability Functions parameters (Table 2), results were generated from the Desirability Functions and presented in Table 3. As seen in Table 2, all lower and upper boundaries are set to 0 and 100, respectively. Also, all quality attributes have been identified as having equal priority. This is accomplished by setting the weight $r = 1$ for all quality attributes. Finally, different target values have been identified for each quality attribute. This means that the threshold for achieving 100% desirability is customized for each quality attribute. For example, quality attributes where T = 70 are considered 100% desirable if they exhibit 70% (or more) of the features that define them.

Table 1. Binary Input Evaluation.

ISC	QA1 = Restrictions			QA2 = Scope			QA3 = Organization's Objectives			QA4 = Physical Access			QA5 = Access Controls			QA6 = Human Resources			QA7 = Communications and Operations Management			QA8 = Systems Acquisition, Development, and Maintenance			QA9 = Incident Management		
	C	AoR	T	S1	S2	Sn	O1	O2	On	L1	L2	Ln	N	O	A	Aw	Tn	E	SoD	CM	NS	SoA1	SoA2	SoAn	P1	P2	Pn
1	0	0	0	0	1	0	0	0	0	1	1	1	1	1	1	0	0	1	1	1	1	0	0	1	0	1	1
2	1	0	1	0	1	0	0	1	0	0	1	1	0	1	1	1	0	1	0	0	1	0	1	0	0	1	1
3	0	0	1	1	1	1	0	0	0	1	1	1	1	1	1	0	1	1	1	0	1	1	1	0	0	0	0
4	1	1	0	1	1	1	1	1	1	0	0	1	1	0	1	1	0	0	1	0	1	0	1	1	1	1	0
5	1	1	1	1	0	1	1	0	1	0	1	0	1	0	0	1	1	0	0	0	1	0	0	0	1	1	0
6	0	0	1	1	1	1	1	1	1	0	0	0	0	0	0	1	1	1	0	0	0	0	0	1	1	0	1
7	0	0	1	1	0	1	1	1	1	0	1	0	1	0	1	1	0	0	1	1	0	1	1	0	0	0	1
8	0	0	1	1	1	0	1	0	0	0	1	1	0	0	0	0	1	0	0	0	0	0	0	0	1	1	1
9	1	1	1	1	0	0	0	1	0	0	1	1	1	1	0	0	0	1	0	0	1	0	0	1	0	1	1
10	0	1	0	0	1	0	1	0	0	1	0	1	1	0	1	0	0	1	1	0	0	1	1	0	1	0	0

Table 2. Desirability Functions Parameters.

ISC	QA1 = Restrictions	QA2 = Scope	QA3 = Organization's Objectives	QA4 = Physical Access	QA5 = Access Controls	QA6 = Human Resources	QA7 = Communications and Operations Management	QA8 = Systems Acquisition, Development, and Maintenance	QA9 = Incident Management
L	0	0	0	0	0	0	0	0	0
U	100	100	100	100	100	100	100	100	100
T	33	40	100	70	70	70	70	70	70
r	1	1	1	1	1	1	1	1	1

Table 3. Desirability Functions Results.

ISC	QA1 = Restrictions			QA2 = Scope			QA3 = Organization's Objectives			QA4 = Physical Access			QA5 = Access Controls			QA6 = Human Resources			QA7 = Communications and Operations Management			QA8 = Systems Acquisition, Development, and Maintenance			QA9 = Incident Management			Desirability
	C	AoR	T	S1	S2	Sn	O1	O2	On	L1	L2	Ln	N	O	A	Aw	Tn	E	SoD	CM	NS	SoA1	SoA2	SoAn	P1	P2	Pn	
1	1.0000			0.8333			0.0010			1.0000			1.0000			0.4762			1.0000			0.4762			0.9524			38.36%
2	0.4975			0.8333			0.3333			0.9524			0.9524			0.9524			0.4762			0.4762			0.9524			66.60%
3	0.9950			1.0000			0.0010			1.0000			1.0000			0.9524			0.9524			0.9524			0.0014			22.04%
4	0.4975			1.0000			1.0000			0.4762			0.9524			0.4762			0.9524			0.9524			0.9524			76.79%
5	0.0001			1.0000			0.6667			0.4762			0.4762			0.9524			0.4762			0.0014			0.9524			12.82%
6	0.9950			1.0000			1.0000			0.0014			0.4762			1.0000			0.0014			0.4762			0.9524			19.66%
7	0.9950			1.0000			1.0000			0.4762			0.9524			0.4762			0.9524			0.9524			0.4762			76.79%
8	0.9950			1.0000			0.3333			0.9524			0.0014			0.4762			0.0014			0.0014			1.0000			9.12%
9	0.0001			0.8333			0.3333			0.9524			0.9524			0.4762			0.4762			0.4762			0.9524			23.95%
10	0.9950			0.8333			0.3333			0.9524			0.9524			0.4762			0.4762			0.9524			0.4762			66.60%

As evidenced, each ISC has been evaluated using the identified features for each quality attribute. The binary input scale is used to determine the presence of features. Using the proposed approach, the most desirable ISC (based on the quality attributes) is ISC 4 and ISC 7, followed by ISC 2 and ISC 10, and so on. It is important to notice that the evaluation of ISC using this approach is fully dependent on the particular scenario at hand. In this case study, the results are based on the parameters configured in Table 2. However, if changed to reflect more priority on different quality attributes, the results would vary from the ones presented in Table 3. In addition, different applications of the approach can contain numerous features, which make it fully customizable for practical applications. These are perhaps the most meaningful contributions from this research; that is, the ability to fully customize and prioritize organization's goals when selecting ISC. This all can be done easily through simple spreadsheet calculations. Similar to this case study, many different organizational-specific parameters can be specified for the Desirability Functions to properly prioritize/evaluate ISC in industry scenarios.

6. CONCLUSION

The research presented in this paper develops an innovative approach for evaluating the quality of ISC in organizations based on a multiple quality evaluation criteria. Specifically, it presents a methodology that uses Desirability Functions to create a unified measurement that represents how well ISC meet quality attributes and how important the quality attributes are for the organization. Through a case study, the approach is proven successful in providing a way for measuring the quality of ISC for specific organizations.

There are several important contributions from this research. First, the approach is simple and readily available for implementation using a simple spreadsheet. This can promote usage in practical scenarios, where highly complex methodologies for ISC selection are impractical. Second, the approach fuses multiple evaluation criteria and features to provide a holistic view of the overall ISC quality. Third, the approach is easily extended to include additional quality attributes not considered within this research. Finally, the approach provides a mechanism to evaluate the quality of ISC in various domains. By modifying the parameters of the Desirability Functions, quality of ISC can be evaluated by taking consideration of prioritized quality attributes that are necessary for different organizations. This can be beneficial for cases such as [23], where the approach can be used to assess and help define information systems security policies [23] and controls that are most effective. Overall, the approach presented in this research proved to be a feasible technique for efficiently evaluating the quality of ISC in organizations.

ACKNOWLEDGEMENTS

The authors would like to thank the reviewers whose constructive critique greatly improved the quality of the paper.

REFERENCES

[1] M. Schwartz, “Computer security: Planning to protect corporate assets,” Journal of Business Strategy, vol. 11(1), pp. 38-41, 1990.

[2] L. Yuan, “Companies face system attacks from inside, too,” Wall Street Journal, pp. B1 (2005, June 15).

[3] L. Volonino and S. R. Robinson, Principles and Practice of Information Security. Pearson Prentice Hall, Inc., New Jersey, 2004.

[4] E. Vaast, “Danger is in the eye of the beholders: Social representations of information systems security in healthcare,” Journal of Strategic Information Systems, vol. 16(1), pp. 130-152, 2007.

[5] S. Ransbotham and S. Mitra, "Choice and chance: A conceptual model of paths to information security compromise," Information Systems Research, vol. 20(1), pp. 121-139, 2009.

[6] G. Rotvold, "How to create a security culture in your organization," Information Management Journal, vol. 42(6), pp. 32-38, 2008.

[7] T. Herath and H. R. Rao, "Encouraging information security behaviors in organizations: Role of penalties, pressures, and perceived effectiveness," Decision Support Systems, vol. 47(2), pp. 154-165, 2009.

[8] L. Barnard and R. Von Solms, "A formalized approach to the effective selection and evaluation of information security controls," Computers & Security, vol. 19(2), pp. 185-194, 2000.

[9] A. Da Veiga and J. H. P. Eloff, "An information security governance framework," Information Systems Management, vol. 24(4), pp. 361-372, 2007.

[10] M. Karyda, E. Kiountouzis, and S. Kokolakis, "Information systems security policies: A contextual perspective," Computer Security, vol. 24(1), pp. 246-260, 2004.

[11] C. Wood, "An unappreciated reason why security policies fail," Computer Fraud and Security, vol. 10(1), pp. 13-14, 2000.

[12] K. Loch, S. Conger, and E. Oz, "Ownership, privacy and monitoring in the workplace: A debate on technology and ethics," Journal of Business Ethics, vol. 17, pp. 653-663, 1998.

[13] G. V. Post and A. Kagan, "Evaluating information security tradeoffs: Restricting access can interfere with user tasks," Computers & Security, vol. 26(3), pp. 229-237, 2007.

[14] R. Saint-Germain, "Information security management best practice based on ISO/IEC 17799," The Information Management Journal, vol. August 2005, pp. 60-66, 2005.

[15] R. Baskerville and M. Siponen, "An information security meta-policy for emergent organizations," Journal of Logistics Information Management, vol. 15(1), pp. 337-346, 2002.

[16] M. E. Whitman, A. M. Towsend, and R. J. Aalberts, "Information systems security and the need for policy," in G. Dhillon, Eds. Information security management: Global challenges in the new millennium (pp 9-18). Hershey, PA: Idea Group Publishing (2001).

[17] H. Van der Haar and R. Von Solms, "A model for deriving information security controls attribute profiles," Computers & Security, vol. 22(3), pp. 233-244, 2003.

[18] C. E. Otero, E. Dell, A. Qureshi, and L. D. Otero, "A quality-based requirement prioritization framework using binary inputs," In 4th Asia International Conference on Mathematical/Analytical Modeling & Computer Simulation, pp. 187-192, 2010.

[19] G. Derringer and R. Suich, "Simultaneous optimization of several response variables," Journal of Quality Technology, vol. 12(1), pp. 214-219, 1980.

[20] D. Montgomery, Design and Analysis of Experiments. John Wiley & Sons, Inc., New York, 2008.

[21] C. E. Otero, L. D. Otero, I. Weissberger, and A. Qureshi, "A multi-criteria decision making approach for resource allocation in software engineering," In 12th International Conference on Computer Modeling and Simulation, pp. 137-141, 2010.

[22] J. D'Arcy, A. Hovav, and D. Galletta,"User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach, " Information Systems Research, vol. 20(1), pp. 79-98, 2009.

[23] Wilkinson, K., "IT Security Incidents Prompt Nashville, Tenn., to Strengthen Policy, Hire IT Security Chief", http://www.govtech.com/gt/articles/768757?utm_source=rss&utm_medium=link, retrieved on August 24, 2010.

Authors

Angel R. Otero was born in 1974 in Bayamon, Puerto Rico. He received his B.S. in Accounting from The Pennsylvania State University and M.S. in Software Engineering from the Florida Institute of Technology. Mr. Otero is currently a Ph.D. student at Nova Southeastern University's Graduate School of Computer and Information Sciences. Mr. Otero is currently a Manager in the Florida/Puerto Rico Enterprise Risk Services practice of Deloitte & Touche, LLP, based in Puerto Rico. He has over 13 years of industry experience in the areas of public accounting/auditing, information technology consulting, and information systems auditing. Mr. Otero is a Certified Public Accountant, Certified Information Systems Auditor, Certified Information Technology Professional, and Certified Internal Controls Auditor. He is also a member of the American Institute of Certified Public Accountants, the Information Systems Audit and Control Association, the Puerto Rico Society of Certified Public Accountants, and The Institute for Internal Controls.

Dr. Carlos E. Otero was born in 1977 in Bayamon, Puerto Rico. He received his B.S. in Computer Science, M.S. in Software Engineering, M.S. in Systems Engineering, and Ph.D. in Computer Engineering from the Florida Institute of Technology, in Melbourne, FL. His primary research interests include performance evaluation and optimization of systems and processes in a wide variety of domains (including wireless systems, software engineering, and systems engineering). He is currently Assistant Professor in the department of Mathematics and Computer Science at the University of Virginia's College at Wise, Wise, VA. Previously, he was adjunct professor in the department of Electrical & Computer Engineering at Florida Institute of Technology. He has over 10 years of industry experience in satellite communications systems, command & control systems, wireless security systems, and unmanned aerial vehicle systems. Dr. Otero is an active professional member of the ACM and active senior member of the IEEE.

Dr. Abrar Qureshi received a BS degree in Mathematics from the University of the Punjab, a BS in Electrical Engineering from Central Philippines University, and a MS and Ph.D. in Computer Engineering from Florida Institute of Technology. He is currently Assistant Professor in the department of Mathematics and Computer Science at the University of Virginia's College at Wise, Wise, VA. Before joining UVa-Wise, he worked in Industry for more than thirteen years where he worked on various software engineering projects, software development, database design, system/software test and automation, and quality assurance. His research interests include software testing, quality assurance, and software security.