Audit financiar, XIV, No. 5(137)/**2016**, *564-574*
ISSN: 1583-5812; ISSN on-line: 1844-8801

Considerations on the selection and prioritization of information security solutions

Maria Cristina RĂDULESCU,
Bucharest University of Economic Studies,
E-mail: maria.radulescu@cig.ase.ro

Abstract

This paper provides a set of guidelines that can be used to prescribe a methodology or a detailed process for selecting and prioritizing security projects or solutions. It is based on the idea that costs of security solutions should be justified by their contribution to ensuring adequate protection of information resources in the organization which implements them. The article reviews general issues of security risks and costs, arguing the need for explicit consideration of information resources security requirements in order to validate decisions concerning security projects implementation. In such an approach, security requirements of information resources are used as a reference system to quantify the benefits and limitations of security solutions defined as alternative or complementary responses to certain security risks as their implementation faces budget constraints.

Keywords: *Information security; security solution; information resource; security risk; efficiency.*

JEL Classification: *M15, O33, M40, D81*

To cite this article:
Rădulescu, M.C. (2016), Considerations on the selection and prioritization of information security solutions, Audit Financiar, vol. XIV, no. 5(137)/2016, pp. 564-574,
DOI: 10.20869/AUDITF/2016/137/564

Permanent link to this document:
http://dx.doi.org/10.20869/AUDITF/2016/137/564

1. Introduction

As efficiency is a key factor in decision-making and security goals must be constantly reconciled with budget constraints, each security model should aim at maximizing benefits while minimizing costs (Scholtz, 2011). Possibilities of economic substantiation of information security policies are investigated in various papers which resort to quantitative techniques and models (Böhme, 2010; Gordon and Loeb, 2002; Gordon and Loeb, 2005; Pontes et al., 2011), most of which target the information system as a whole, without regard to its structural complexity, which determines various risks and security requirements.

As software applications supporting business processes in an organization are commonly used as a starting point for security risks identification and analysis, security solutions are technically oriented and specifically designed for a certain area of information infrastructure. Relative to the typological diversity of business information they must protect, security solutions can be seen as composite structures, spanning multiple data categories, with various security requirements. This paper defines both effectiveness and limitations of security solutions in terms of the protection they offer to an organization's information resources. Having considered that security solutions are not ends in themselves, but means that must ensure an adequate level of protection for information resources, the paper aims at providing a set of guidelines and criteria to validate decisions concerning security solutions from a perspective which complements the economic and financial view with corresponding indicators (annual loss expectancy, return on security investment, net present value etc.).

2. Research methodology

This article is the result of a qualitative research, aimed at approaching security solutions analysis and comparison in terms of their protective impact on information resources managed by an organization. The research is based on an extensive study of literature on security risk management and the efficiency of security solutions for risk mitigation, which enabled proper argumentation of the relevance of the approach proposed in this paper. The theoretical approach concerns the following aspects: conceptual delimitation of information resources and security solutions as key elements of the analysis model, adoption of risk management tools and techniques to be used for a reference system to assess security solutions impact, identification of conceptual correlations required to quantify this impact. The results of the present research may be integrated into a formal model to assist investment decisions concerning information security; such an approach facilitates the expansion of the research through a quantitative approach, aimed at analysing data security solutions implemented by companies in the business environment.

3. Information security costs and benefits

In a broad sense, information security covers both digital and non-digital data, and it is presently seen as a field that transcends organizational processes and subdomains. The imperative need to manage this complexity, on both technical and organizational levels, led to standards such as ISO27k *Information Security* (ISO - International Organization for Standardization) and NIST SP800 *Computer Security* (NIST - National Institute of Standards and Technology), or to best practice or reference models, such as COBIT- Control Objectives for Information and Related Technology or ITIL - Information Technology Infrastructure Library. Information security is also targeted by certain norms and regulations or influenced by them; Basel II and III in banking, or the Sarbanes-Oxley Act in the US are frequently referenced in literature. Such regulations or adoption of certain standards affect the security strategy and policies of a company and, subsequently, the level of security investments. Impact of regulations on security is analysed by Lee et al. (2016), relative to scenarios involving parallel and sequential implementation of security controls prescribed by standards and those decided by organizations.

That security is a distinct management area is confirmed by PricewaterhouseCoopers - PwC (2015) in an extensive study (10,000 decision-makers from 127 states) showing that 58% of organizations have a security strategy. Despite an increase of 38% in security incidents compared to 2014 PwC (2015) finds a decrease of 5% in financial losses due to security incidents, which certifies the utility of security strategies. On the other hand, given that 24% of companies reported an increase in their security budget, it is

imperative to consider the efficiency issues of security strategies. Their importance is emphasized by another global study by Ernst&Young - EY (2015), which indicated budget restrictions as the main obstacle (for 67% of companies) for an adequate level of information security. Due to an invariably limited budget, security models must be optimized by weighing potential and actual benefits against security costs (Scholtz, 2011).

Risk management is essential for security budget. The first question is "How much is enough?" (Hoo, 2002), then the security budget must be adequately allocated to security controls aimed at risk management. A judicious distribution requires realistic estimation of security incidents costs, including indirect losses due to temporary applications dysfunctionalities. There must also be considered all responses to security risks. For example, Zhao et al. (2009) compares the options for security risk transfer and indicates *outsourcing* as being preferable to security insurance. On the other hand, IT *outsourcing* raises the issue of hidden costs (Barthelemy, 2001), the identification and assessment of which is critical for the proper validation of *outsourcing* decisions.

Security risk management is not confined to the IT infrastructure; for example, Goettelmann et al. (2014) present a risk analysis model for business processes supported by *cloud-computing* solutions. In NIST (2012) security risk management is approached on technical, business processes and strategic levels; these correspond to distinct levels for risk identification and analysis as well as to decision levels for risk mitigation. Usually addressed on an operational or technical level, security risks are less approached from the perspective of strategic decisions concerning security policies and their financial support. For example, Gordon and Loeb (2006) or Hamill et al. (2005) presume information security budget as being known; Anderson and Choobineh (2008) propose a different approach, which explicitly addresses the issue of proper sizing of information security budget. On the strategic level, security risks are weighed against security costs, including opportunity costs (Gordon and Loeb, 2006); the actual information security budget essentially depends on the perception that decision makers have on risk, leading to certain levels of risk tolerance. The risk tolerance can vary greatly from an organization to another, and for the same organization, from one period to another, depending on the company's business goals and the economic context; as such, one may consider the approach proposed by Gordon et al. (2003) - postponing costly investments until a security incident warrants a reaction.

Economic substantiation of information security policies is investigated in various papers which resort to quantitative models and techniques. For example, Böhme (2010) deals with the relationship between security metrics and investment models, while Gordon and Loeb (2002) present an economic model for an optimal level of information security investments. Typically, efficiency of security investments is assessed using cost-benefit analyses, which involve estimates of losses avoided because of the investments. Gordon and Loeb (2005) provide a guide on cost-benefit analyses for IT security; it is directed at proper sizing of security investments, but it also deals with aspects such as the influence of risks on financial resources to support information security or strategies to minimize the impact of security incidents. Also, Pontes et al. (2011) address profitability of security investment in relation to risk management.

Brecht and Nowey (2012) provide a detailed analysis of cost and investment issues pertaining to information security by comparing significant contributions in literature on the subject. A potential problem of most models is the "black box" perception on an information system, while ignoring its structural complexity which determines various risks and security requirements. In the short term, this helps saving costs with data analysis and classification in terms of security requirements, as well as with security policy adaptation. In the long run, security model opacity could lead to inadequate budgets or improperly distributed budgets, oversizing some allocations and under-sizing others favouring security incidents that generate new costs. A more nuanced approach is provided by Gordon and Loeb (2002), who propose an economic model for the optimal level of security investments to ensure data integrity, confidentiality, availability, authenticity and non-repudiation; the authors use an adjusted version of the annual loss expectancy model, adapted to scenarios when only one of the attempts to undermine security goals will be successful. Security requirements corresponding to information resources managed by an organization are explicitly addressed by the present paper, which treats them as a stable and uniform reference for assessing the benefits and limits of

security projects, irrespective of their financial aspects, operational magnitude or timeframe.

4. A security approach to information resources

Although security goals can be used for both data and applications, this paper adopts a broader perspective and targets an abstraction level that is relevant to the business logic. Information resources are therefore approached as stable conceptual entities that transcend applications and business processes; in other words, the focus is the actual business information and corresponding typological and classification criteria which are also relevant from a security perspective.

As information entities with common properties are abstracted as generic types, the entire information system of an organization may be modelled on a purely conceptual level, as in the popular *Entity-Relationship* formalism by Chen (1976). Most frequently, however, the granularity level in such models is inadequate for the analysis and treatment of security risks, and therefore initial entities must be regrouped in information categories relevant to security risks assessments. For example, contracts, customers and receipts could be placed in the same *Sales* category; alternatively, one could define a category to group both suppliers and customers with their corresponding operations; another approach would be to separate contracts and financial transactions in distinct information categories. Information resources can vary considerably in terms of strategic and operational importance, in addition to which one may consider other differentiation criteria, such as policies enforced by different regulations (minimum period to store the data, conditions in which it can be destroyed or disposed of etc.). Therefore, data analysis and classification in terms of the importance it presents to the organization is a mandatory step in order to identify critical information resources and corresponding security risks.

Although information in the same category may be subject to scenarios involving multiple users and various applications or software environments with different security requirements, approaching business information in a systematic and consistent manner in the context of risk management allows for the definition of minimum thresholds for security requirements to match all scenarios that must to be addressed. Identifying the typology of information resources requires detailed analysis of the information system, as for each information category one must specify corresponding business processes, applications and types of users, with their security prerogatives and constraints.

The protection level that is adequate to each information category is the aggregated expression of security requirements concerning a specific set of security goals. Although these goals are impacted by standards like ISO27k or adherence to certain control or IT governance frameworks and, such as ISACA's COBIT, they are usually represented by the confidentiality-integrity-availability triad; also, they may be supplemented by additional criteria such as non-repudiation, authenticity, resilience etc. Even when the same quantitative and descriptive scale is applied for all security goals it is possible that security requirements for a specific category of information resources vary considerably, depending on the security goal; for example, Oberlaender (2011) outlines a set of scenarios that require different levels of security requirements for certain types of business information.

Although business information modelling issues are outside the scope of this paper, the presentation above is meant to provide a proper conceptual delimitation of information resources as key elements for security solutions analyses and comparisons.

5. Security solutions analysis from the perspective of information resources

The following section of the article expands on the generic components of an analysis model of security projects or solutions focused on information resources security requirements. Such a model is meant to validate decisions on selection or prioritization of solutions defined as alternative or complementary responses to certain security risks, when their implementation is subject to budget constraints. As such, the set of security solutions and their corresponding costs are presumed known and they are used as inputs for the analysis model. Furthermore, since the risk level is the most relevant criterion in prioritizing risk mitigation actions, the set of solutions to be compared should be limited to those defined as responses to risks of a certain level, assessed in advance using specific risk management tools and techniques.

5.1. Security solutions inventory

In this paper, the expression "*security solution*" designates a set of technical and organizational elements directed at information security risks mitigation. Depending on its complexity, each security solution implements security controls and mechanisms that may act on a single or several levels:

- *Logical:* user authentication and access authorization, monitoring, auditing, backup, encryption, antivirus, firewall, etc.;
- *Physical:* securing a certain perimeter, hardware management, etc.;
- Operational and administrative: training, employee screening, work procedures, help-desk, etc.

Such an approach to security solutions has a dual argument:

- Adequate security risk management determines complementarity and interdependency of security measures and controls;
- Financial constraints require selection of controls and prioritization of investments according to their efficiency.

In view of the statements listed above, each security solution corresponds to a specific mix of technical and operational components which are relevant to risk management. Security solutions may be defined at various granularity levels provided that each solution can be implemented independently and be subject to cost-benefit analyses; in other words, a particular solution may be designed as the simpler version of another security solution, the difference in granularity having direct consequences on cost levels. Given the budget constraints, the costs corresponding to a set of predefined security solutions are, in different proportions, both additive and exclusive; thus, it is necessary to identify the combination of solutions that enables an optimal response to security risks while complying with the budget limit.

From case to case, security solutions may target a wider or narrower set of information resources, while the same resources may be of interest to multiple security solutions. On the other hand, the security requirements of information resources are independent of solutions being analysed, as they are determined by the intrinsic nature of business information and its importance to the organization. Therefore, in order to quantify the overall impact of a security solution it is necessary to assess its contribution to ensuring the protection level predefined as optimal for each security goal corresponding to information resources targeted by that solution.

Even when having identical security requirements, information resources can be significantly different in terms of operational or strategic importance and therefore the criterion of the relative importance of each information category is essential for the quantitative assessments of security goals and security solutions contribution to achieving them. In a more pragmatic approach, which allows the simplification of such assessments, security solutions-information resources mappings may be defined using the subset of resources regarded as critical due to the effects of potential security incidents. This approach was used to specify the generic mappings in **Table 1**, which are limited to critical resources targeted by the security solutions.

5.2. Security solutions impact assessment

As security goals must be accompanied by clear criteria for specifying each level of security requirements of information resources, for the latter one can identify a certain level of compliance or non-compliance (compliance gap) with predefined security requirements; for example, NIST (2005) uses a compliance gap indicator concerning the information system as a whole. The present paper recommends a more nuanced approach, by isolating information resources security requirements; as such, a protection level higher than the one predefined as adequate is not considered necessary nor possible without entailing additional costs that are disproportionate to the expected benefits.

Compliance with security requirements is not an absolute goal, but is assessed by comparison to the level set as optimal for each security criterion. As a consequence, the effectiveness of a security solution can be perceived as an aggregate of individual values that quantify its impact in terms of the actual increase in compliance with security requirements of information resources targeted by that solution. When using the optimal level of security requirements as a reference (100%), the following metrics can be considered for each security solution:

- *The compliance gaps preceding security solutions implementation (Previous Gap - PG)*
- *The compliance gaps subsequent to security solutions implementation (Subsequent Gap - SG)*

Table 1. Example on security solutions - information resources mappings

Solutions/ Resources		Confidentiality			Integrity			Availability		
		Low	Medium	High	Low	Medium	High	Low	Medium	High
S1	R1		PG = 0.50 SG = 0.30 P = 0.20			PG = 0.70 SG = 0.50 P = 0.20				PG = 0.50 SG = (-0.25) P = 0.50 | OP = 0.25
	R2			PG = 0.75 SG = 0.50 P = 0.25		PG = 0.00 SG = (-0.50) P = 0.00 | OP = 0.50			PG = 0.50 SG = 0.00 P = 0.50	
S2	R2			PG = 0.75 SG = 0.00 P = 0.75		PG = 0.00 SG = 0.00 P = 0.00			PG = 0.50 SG = 0.50 P = 0.00	
S3	R1		PG = 0.50 SG = (-0.20) P = 0.50 | OP = 0.20			PG = 0.70 SG = 0.70 P = 0.00				PG = 0.50 SG = 0.30 P = 0.20
	R2			PG = 0.75 SG = 0.50 P = 0.25		PG = 0.00 SG = 0.00 P = 0.00			PG = 0.50 SG = 0.50 P = 0.00	
	R3	PG = 0.20 SG = 0.20 P = 0.00			PG = 0.00 SG = 0.00 P = 0.00					PG = 0.50 SG = 0.25 P = 0.25
S4	R2		PG = 0.50 SG = 0.5 P = 0.00			PG = 0.70 SG = 0.70 P = 0.00				PG = 0.50 SG = (-0.15) P = 0.50 | OP = 0.15
	R2			PG = 0.75 SG = 0.75 P = 0.00		PG = 0.00 SG = 0.00 P = 0.00			PG = 0.50 SG = 0.25 P = 0.25	

PG = Previous Gap [compliance gap preceding security solution implementation)

SG = Subsequent Gap [compliance gap subsequent to security solution implementation)

P = Protection effect OP = Overprotection effect

Source: Author's processing

The compliance gap preceding security solutions implementation is assessed by taking into account the current state of the information system, while the gap subsequent to implementation corresponds to a potential future state, the transition to which is triggered by the implementation of a specific security solution. Inherent difficulties of compliance gap assessments must be handled in the context of security risk management; for example, one must assess the likelihood of security incidents and the organization's capacity of neutralizing their consequences. Such estimates involve statistical data and quantitative models, but also the professional reasoning of experts in IT security, risk management and internal audit. The limits of quantitative models in complex scenarios where professional expertise is critical are analysed by Devos et al. (2013). Accurate compliance gap quantification depends on a consistent security risk management which involves monitoring of implemented solutions and evaluation of results, to be later used as inputs in a new risk management cycle.

Although an increase of the compliance gap (SG > PG) following security solutions implementation is generally unlikely, an exception is the case of replacement of pre-existing solutions which prove to be superior to potential substitution solutions that are being assessed, in terms of compliance with specific security goals. However, in the usual scenario, the analysed solutions partially or, ideally, completely, solve compliance issues concerning security requirements of information resources to which they apply. On the other hand, a detailed analysis, which opposes each security solution all information resources it must protect, may expose solutions with a partially void impact (they target a subset of security goals without any contribution to the decrease in the

compliance gap corresponding to others) or solutions that satisfy certain security requirements in a degree which is higher than that predefined as appropriate for certain information resources.

The negative value of compliance subsequent to security solution implementation (SG < 0) indicates an over-compliance with security requirements. Such an effect should be distinguished from that which allows achieving the predefined optimal level of compliance, since it corresponds to oversized investments or excessive controls that cannot be justified in terms of actual security benefits. Therefore, the impact of security solutions will be quantified separately for each of the effects they may produce:

- Protection, which translates as a complete elimination or a decrease in the compliance gap:

Protection effect (P) = Subsequent Compliance Gap - Previous Compliance Gap

- Overprotection, which involves the elimination of the initial compliance gap and an additional protection above the level defined as optimal for specific information security requirements:

Protection effect (P) = Previous Compliance Gap

Overprotection effect (OP) = (-Subsequent Compliance Gap)

5.3. The overall impact of security solutions

Given that a security solution applies to multiple information resources, its overall impact will be computed as the average of values that quantify its effect considering individual security requirements of information resources corresponding to that solution.

However, these values must be first separated into two data subsets, depending on the nature of the effect; therefore, we distinguish between the average protection effect and, if available, the average overprotection effect. The average protection effect is a measure of the effectiveness of a security solution, in terms of its contribution to ensuring an adequate protection level for information resources; on the other hand, a higher or lower level of the average overprotection effect is expected to entail costs that cannot be accounted for in terms of actual security needs of information resources.

The identification and quantification of the overprotection effect produced by security solutions are guided by the idea that only a protection level deemed necessary is acceptable from a cost perspective. On the other hand, given that security solutions are collectively aimed at several categories of information resources, providing an adequate level of protection for certain resources may result in overprotection of others, without this leading to an increase in costs of security solutions implementation. A direct and immediate relationship between the overprotection effect and costs may be difficult if not impossible to determine, given the difference of perspectives used for their assessment: information resources security requirements in contrast with economic value of assets and services required for securing information resources managed by the organization. In such circumstances, the arithmetic computation of a portion of costs attributable to overprotection has no economic justification, as overprotection is only an assumption, not a certainty of an increase in security solutions costs. As a result, the overprotection effect will not influence the treatment of costs, as inputs required to assess the effectiveness of security solutions.

Table 2. Metrics of the exemplified security solutions

Solution	Costs	Average Protection Effect	Average Overprotection Effect	Cost Efficiency	Average Subsequent Compliance Gap
S1	15,000	0.275	0.375	0.183	0.217
S2	5,000	0.250	0.000	0.500	0.167
S3	35,000	0.133	0.200	0.038	0.272
S4	17,500	0.125	0.150	0.071	0.367

Source: Author's processing

5.4. The efficiency of security solutions

The subject of security solutions efficiency is covered extensively in various papers that analyse specific indicators and issues raised by their computation - for example, Pontes et al. (2011). Leaving aside other economic and financial data (monetary value of the software applications and equipment, estimated trends of productivity or financial results etc.), NIST (2005) uses an efficiency indicator expressed as the ratio of the compliance gap to the cost of a security project. The assumption is that security solutions will achieve their purpose, namely the elimination of compliance gaps; the higher the compliance gap and the lower the costs, the more efficient the security solution.

Although this paper approaches efficiency of security solutions in a similar manner (a certain number of effect "units" to a cost "unit"), explicit consideration of information resources security requirements helps with increasing the relevance of such indicators. In other words, for better risk mitigation on a limited budget, the costs of each security solution must be justified by its actual utility, considering the expected and necessary effect and disregarding a possible overprotection of resources. Therefore, the efficiency of a security solution will be expressed as a ratio of its average protection effect to the costs entailed by its implementation. Since they raise the cost size issue, efficiency indicators are relevant only to the extent that the analysed security solutions have comparable levels of implementation costs. This scenario should be, however, implicit, as projects and solutions which differ significantly in terms of their impact on the information system question the relevance and usefulness of the comparative analysis of security solutions. Efficiency indicators of generic solutions used for exemplification are available in **Table 2***;* to simplify their use, the actual values have been multiplied by 10,000.

5.5. Security solutions selection and prioritization

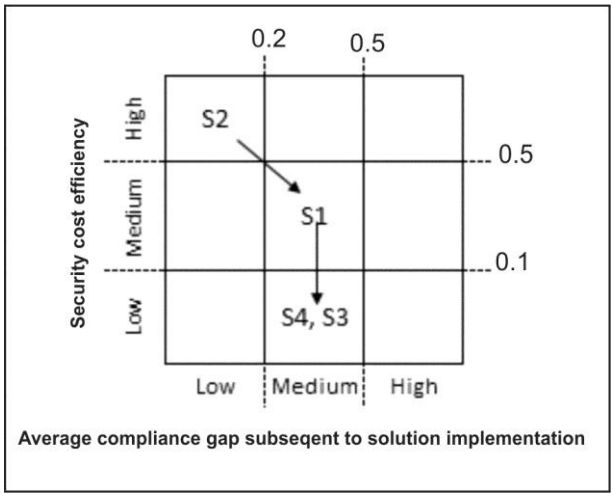
Although efficiency can be used as a criterion for security projects selection, this indicator only takes into account the positive impact of solutions, and not their limitations relative to security requirements of information resources they must protect. The extent to which a solution has achieved its purpose is the aggregate expression of compliance gap values resulting from its application (SG) and it is quantified as their average. For the generic solutions considered for exemplification, the indicators of average compliance gap subsequent to implementation are presented in **Table 2**. A particular treatment is required for cases of overprotection of information resources. While this may be a prerequisite for an increase in costs that cannot be justified in terms of actual security requirements of information resources, it is certain that the level of achieved protection enables the full elimination of the compliance gap preceding the implementation of security solutions. Therefore, when computing the average compliance gap subsequent to the implementation of a security solution, 0 must be used as input for each overprotection occurrence.

In the absence of a conceptual correlation leading to a relevant indicator which involves both criteria, the efficiency and the average compliance gap subsequent to security solutions implementation will be combined in a matrix that allows delineation of generic contexts which qualify security solutions as being more or less advantageous relative to certain combinations of values. In **Figure 1**, the quantitative and descriptive categories commonly used for risk management (low, medium, high) were applied for each of the two criteria; the corresponding value scales are predefined in terms of risk tolerance and are independent of security solutions that are being analysed. Obviously, the solutions selection starts from the extremity of high efficiency and low compliance gap and continues with cells in its close proximity. The actual approach of selecting one or more solutions raises, however, a number of issues that can be mapped to the following scenarios:

- *Multiple security solutions positioned in the same section of the matrix.* Efficiency, compliance gap subsequent to implementation, cost, or average overprotection effect can be used as differentiating criteria in a predefined order, which depends on the importance attached to them. For example, if no strict budget limitations apply, one may favour the compliance gap due to the security risks it entails.
- *Non-exclusive security solutions, to be implemented in parallel (concurrently) while meeting budget constraints.* Starting from the extremity corresponding to the optimal combination and, if necessary, continuing with adjacent cells, there must be identified the combination of solutions that complies with the budget limit.

- *Non-exclusive security solutions, to be implemented sequentially.* In this case it is assumed that all solutions must be implemented, though not simultaneously; therefore, the highest priority will be given to the most advantageous solutions in terms of their effects. The prioritization starts from the extremity corresponding to the optimal combination, but the direction to advance depends on the importance of the criteria expressing expected effects of security solutions (high efficiency or low compliance gap subsequent to solution implementation).

Figure 1. Security solution selection and prioritization matrix



Source: Author's processing

When targeting a common set of resources, non-exclusive security solutions raise the question of analysis consistency. Thus, assessing compliance with security requirements of information resources individually, for each solution that is being analysed, does not allow for identification of possible over-compliance resulting from accumulation of protection effects of each security solution selected for implementation. In case of an integrated approach, the post-conditions of implementing a solution become pre-conditions for the subsequent solution to be implemented, so the compliance gap relative to the security requirements of resources targeted by multiple security solutions is not identical for each of them and does not remain that which was initially estimated, as it is updated after each selection of a solution, according to the prioritization criteria described above. Selecting one of the solutions for implementation requires redefinition of security solutions - information resources mappings by adjusting the set of solutions and reconsidering the initial compliance gap for shared resources (it is equal to the estimated value of the compliance gap subsequent to the implementation of the latest selected solution). Despite its complexity, this approach is more adequate for real-world implementation scenarios as it allows identifying overprotection effects on information resources and, subsequently, the risk of unnecessary costs that cannot be exposed and estimated unless explicitly considering the dynamics that a specific prioritization logic enforces on compliance gaps relative to predefined security requirements.

5.6. The limits of the proposed approach

The main limit of the approach proposed for analysing and comparing security solutions stems from the theoretical construction and therefore its usefulness and applicability should be tested on real organizations in the business environment. The actual implementation of guidelines in the article presents a series of specific difficulties, the first of which concerns consistent definition, using an adequate abstraction level, of information resources and security solutions; they also raise the question of appropriate granularity and treatment of possible overlaps and dependencies. In addition, the analysis and classification of information resources, followed by the assessment of compliance with security requirements are rather laborious endeavours. Though common in the context of security risk, management compliance gap assessments are complicated by the detailed approach, as they must be performed for each of the security goals corresponding to information resources.

Conclusions

Although it does not prescribe a detailed process for security solutions selection or prioritization, this paper provides a set of guidelines that may be used for this purpose and which are based on the assumption that costs of each solution must be accounted for in

terms of its contribution to ensuring an adequate level of protection for information resources to which it applies. Putting aside the fact that estimating compliance gaps relative to security requirements raises inherent difficulties and is dependent on a coherent management of security risks, information resources security requirements are used as a non-monetary reference system, in order to quantify the efficiency and limits of security solutions. From this perspective, the guidelines and criteria proposed for security solutions analysis and comparison have the advantage of being generic and uniformly applicable to any organizational context, regardless of how information security is addressed. The presented approach complements those regarding the economic and financial dimension of information security as the results produced by solutions selection and prioritization may be used to validate analyses concerning the financial impact of security solutions.

REFERENCES

1. Anderson, E.E. and Choobineh, J. (2008), Enterprise Information Security Strategies, *Computers & Security*, vol. 27, no. 1/2, pp. 22-29, DOI:10.1016/j.cose.2008.03.002.
2. Barthélemy, J. (2001), The Hidden Costs of IT Outsourcing, *Sloan Management Review,* vol. 42, no. 3, pp. 60-69.
3. Böhme, R. (2010), Security Metrics and Security Investment Models. In: *Advances in Information and Computer Security*. *Proceedings of IWSEC 2010*, LNCS vol. 6434, pp. 10-24, Belin/Heidelberg: Springer-Verlag.
4. Brecht, M. and Nowey, T. (2012), A Closer Look at Information Security Costs, *11th Annual Workshop on the Economics of Information Security*, WEIS 2012, Berlin. [online] Available at: http://www.econinfosec.org/archive/weis2012/papers/Brecht_WEIS2012.pdf [Accessed on April 2, 2016].
5. Chen, P. (1976), The Entity-Relationship Model - Toward a Unified View of Data, ACM Transactions on Database Systems, vol. 1, no. 1, pp. 9-36, DOI:10.1145/320434.320440.
6. Devos, J., Munteanu, A. and Fotache, D. (2013), How Much Matter Probabilities in Information Security Quantitative Risk Assessment?, In: *International Business Information Management Conference (22nd IBIMA) - Creating Global Competitive Economies: 2020 Vision Planning & Implementation*, Noiembrie 2013, Roma, pp. 45-57.
7. EY - Ernst & Young (2015), *Creating Trust in the Digital World. EY's Global Information Security Survey 2015*. [online] Available at: http://www.ey.com/GL/en/Services/Advisory/ey-global-information-security-survey-2015-1 [Accessed on April 2, 2016].
8. Goettelmann, E., Dahman, K., Gateau, B., Dubois, E. and Godart, C. (2014), A Security Risk Assessment Model for Business Process Deployment in the Cloud, *IEEE International Conference on Services Computing*, Iunie 2014, Anchorage, AK - SUA, pp. 307-314.
9. Gordon, L.A. and Loeb, M.P. (2002), The Economics of Information Security Investment, *ACM Transactions on Information and System Security*, vol. 5, no. 4, pp. 438-457.
10. Gordon, L.A., Loeb, M.P. and Lucyshyn, W. (2003), Information Security Expenditures and Real Options: A Wait-and-See Approach, *Computer Security Journal*, vol. 9, no. 2, pp. 1-7.
11. Gordon, L.A. and Loeb, M.P. (2005), *Managing Cybersecurity Resources: A Cost-Benefit Analysis*, New York: McGraw-Hill Education.
12. Gordon, L.A. and Loeb, M,P. (2006), Budgeting Process for Information Security Expenditures, *Communications of the ACM 2006*, vol. 49, no. 1, pp. 121–125, DOI: 10.1145/1107458.1107465.
13. Hamill, J.T, Dekro, R.F. and Kloeber, J.M. (2005), Evaluating Information Assurance Strategies. *Decision Support Systems*, vol. 39, no. 3, pp. 463–484, doi:10.1016/j.dss.2003.11.004.
14. Hoo, K.J.S. (2002), How Much is Enough? A Risk-Management Approach to Computer Security. In:

Workshop on Economics and Information Security (WEIS), University of California, Berkeley.

15. Lee, C.H., Geng, X. and Raghunathan, S. (2016), Mandatory Standards and Organizational Information Security, *Information Systems Research,* vol. 27, no. 1, pp.70-86, DOI:10.1287/isre.2015.0607.
16. Oberlaender, M.S. (2011), Data classification - A New Approach to Data Centric Security, (*IN)SECURE Magazine*, no. 31, Septembrie 2011, pp. 35-42.
17. NIST (2005), National Institute of Standards and Technology - Special Publication 800-65, Version 1.0, *Integrating IT Security into the Capital Planning and Investment Control Process.* [online] Available at: http://csrc.nist.gov/publications/nistpubs/800-65/SP-800-65-Final.pdf, [Accessed on April 2, 2016].
18. NIST (2012), National Institute of Standards and Technology - Special Publication 800-30, Revision 1*, Guide for Conducting Risk Assessments* [online] Available at: http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf, [Accessed on April 2, 2016].
19. Pontes, E., Guelfi, A.E., Silva, A.A.A. and Kofuji, S.T. (2011), A Comprehensive Risk Management Framework for Approaching the Return on Security Investment (ROSI), In: Savino, M. (Ed), *Risk Management in Environment, Production and Economy*, pp. 149-170, Intech, DOI: 10.5772/25911.
20. PwC – PricewaterhouseCoopers (2015), *The Global State of Information Security Survey*, [online]. Available at: http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html [Accessed on April 2, 2016].
21. Scholtz, T. (2011), Articulating the Business Value of Information Security. Technical report, Gartner Inc. [online] Available at: https://www.forrester.com/report/Articulating+The+Business+Value+Of+Information+Security/-/E-RES54908, [Accessed on April 2, 2016].
22. Zhao, X., Xue, L. and Whinston, A.B. (2009), Managing Interdependent Information Security Risks: A Study of Cyberinsurance, Managed Security Service and Risk Pooling. In: *Proceedings of the International Conference on Information Systems ICIS 2009*, Phoenix – Arizona. Paper 49. [online] Available at: http://aisel.aisnet.org/icis2009/49, [Accessed on April 2, 2016].