How to Assess Confidentiality Requirements of Corporate Assets?

Gabriela Cervantes, Stefan Fenz

How to assess confidentiality requirements of corporate assets?

Gabriela Varona Cervantes and Stefan Fenz

University Carlos III of Madrid, Madrid, Spain and Vienna University of Technology and SBA Research, Vienna, Austria

gvarona@pa.uc3m.es and stefan.fenz@tuwien.ac.at

Confidentiality is an important property that organizations relying on information technology have to preserve. The purpose of this work is to provide a structured approach for identifying confidentiality requirements. A key step in the information security risk management process is the determination of the impact level arisen from a loss of confidentiality, integrity or availability. We deal here with impact level determination regarding confidentiality by proposing a method to calculate impact levels based on the different kind of consequences typically arisen from threats. The proposed approach assesses the impact arisen from confidentiality losses on different areas separately and uses a parameterized model that allows organizations to adjust it according to their specific needs. A validation of the developed approach has been conducted in a small software development company.

1 Introduction

Nowadays Information Technology (IT) plays a crucial role in society. Organizations depend on it to successfully carry out their business missions and functions. In our interconnected and digitized world, confidentiality becomes an important asset to preserve for companies and individuals. The National Institute of Standards and Technology (NIST) defines confidentiality as "preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information."

Companies typically have information that should kept secret in order to maintain their business' competitive advantage. Confidentiality requirements must be incorporated in the business processes of a company, along with the implementation of the corresponding security measurements. The 2013 edition of the biennial information security breaches survey carried out by Infosecurity Europe in UK (Department for business innovation and skills, United Kingdom, 2013), has confirmed the upward trend in the number of security breaches affecting UK businesses. Affected companies experienced on average roughly 50% more breaches than a year ago. The number of organizations critically depending on externally hosted services has slightly increased since the last survey. Increasing numbers of companies are now storing confi-

dential or highly confidential data on the cloud, which makes confidentiality compliance more complex. 10% of respondent companies had their worst security incident related with the theft or unauthorized disclosure of confidential information, the majority of which had a serious impact for the organization.

In information security risk management (ISRM), IT managers have to identify and evaluate possible risks before deciding what security measures to implement. In this process, a balance has to be found between the impact of potential breaches and the operational and economic costs of protective measures. Regarding confidentiality, it is important to accurately define confidentiality requirements on data, resources and business processes. While no restrictions can cause confidential information leaks, setting everything as confidential will complicate the processes and result in higher economic costs for the company. Therefore, the research question of this paper is: How can confidentiality requirements be determined for corporate assets?

Our work approaches confidentiality determination by proposing a structured method for companies to determine their resources' confidentiality. In this paper we present our developed approach on confidentiality determination and validate it in the context of a small software development company.

2 Related work

Related work includes business process-based approaches (cf. (Accorsi et al., 2011a), (Accorsi et al., 2011b), (Accorsi et al., 2012), (Fenz et al., 2009), (Lehmann et al., 2012), (Lehmann et al., 2013), and (Lohmann et al., 2009)) and confidentiality determination methods implemented as part of different risk assessment methods (e.g., NIST (Barker et al., 2008a), Magerit (Spanish Ministry for Public Administrations, 2006), and Mehari (CLUSIF, 2010)). When dealing with confidentiality requirements in business processes one of the first decisions to make is the level to which each asset should be protected. This is part of the risk assessment phase of the ISRM process, which aims at identifying and evaluating risks affecting confidentiality, integrity and availability. Standards, methods and tools supporting security categorization and ISRM in general have been developed (e.g. (NIST, 2012; ISO/IEC, 2013; Spanish Ministry for Public Administrations, 2006; CLUSIF, 2010).

The National Institute of Standards and Technology (NIST) defines security categorization as the first step in the risk management process. Security categories used by NIST SP 800-60 are defined in the Federal Information Processing Standard Publication 199 (FIPS 199) (NIST, 2004):

Potential impacts	Definitions
Low	The potential impact is **low** if—The loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals (e.g., minor damage to organizational assets).
Moderate	The potential impact is **moderate** if—The loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational

	operations, organizational assets, or individuals (e.g., significant financial loss).
High	The potential impact is **high** if—The loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals (e.g., severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries).

Table 1. Potential impact levels by FIPS 199

In Magerit's (Spanish Ministry for Public Administrations, 2006) terminology, confidentiality, availability and integrity, together with authenticity are dimensions of an asset that together determine its value. Furthermore, the "valuation of an asset in a certain dimension is the measurement of the prejudice the organization may suffer if the asset is damaged in that dimension", i.e. the impact level. For valuation of assets a scale of 10 values is used. Criteria to value the assets consider adverse consequences in the following aspects: the security of persons, personal information, obligations arising from the law, capacity for following up offences, commercial and financial interests, interruption of the service, public order, corporate policy, and other intangible values. As a result from the valuation process, assets are assigned one of four confidentiality labels: secret, confidential, restricted or unclassified. Magerit's risk analysis process takes into account dependencies between assets when calculating the security impact.

Mehari (CLUSIF, 2010) uses a four-value scale to measure the impact level should a security breach occur:

Level 4 - Vital: existence and survival of the entity is in danger.
Level 3 - Very Serious: The impact is considered very serious at the level of the entity, although its future would not be at risk.
Level 2 - Serious: Malfunctions at this level would have a clear impact on the entity's operations, results or image, but are globally manageable.
Level 1 - Not significant: At this level, any resulting damage would have no significant impact on the results or image of the entity.

3 Confidentiality impact level determination

Confidentiality determination refers to how restricted access to a certain resource must be in order to preserve its confidentiality. It can be expressed as a meaningful label or category. How to combine this categorization with other risk information and translate it to security measures is subject of another part of the risk management process. As mentioned earlier, the confidentiality label that must be assigned to an asset depends directly on the impact if the asset's confidentiality is compromised. This impact should be assessed independently of the implemented security measures and not with respect to any particular threat. Instead, the overall impact for the organization in case the asset is publicly available should be considered.

Consider for instance a company that keeps a file containing the details of a planned advertising campaign of which only the marketing team and the managers are

aware. The file disclosure by other staff members would probably have a negligible impact for the company, while its disclosure by competitors could reduce the effectiveness of the campaign and negatively affect the company. The confidentiality of such a file should be then determined by the higher potential impact resulting from any possible situation.

In general, adverse impact is related to a degradation of the following:

- Laws and regulations compliance
- Commercial and financial interests
- Company's reputation
- Privacy and security of individuals

Note that they are not independent from each other and are interrelated in a cause-effect manner. Thus, a compromise to the privacy of individuals may affect the company's reputation and directly lead to a noncompliance with the law, which in turn may cause the company to be fined and affect financial interests. Nevertheless this relation may sometimes be difficult to determine and so the approach we propose evaluates each factor independently.

Furthermore, organizations may find damage to some of the above mentioned factors to have a greater impact than others. For instance, a company acting as a trusted third party managing the electronic transactions between absent participants will find a minimum damage to its reputation to have a stronger impact on it than, for instance, the noncompliance to a minor regulation.

3.1 Impact level determination

To determine the overall impact level derived from the loss of confidentiality of a certain resource x, we propose the following formula:

$$I(x) = \alpha * \mathrm{A}_1(\mathrm{x}) + \beta * \mathrm{A}_2(\mathrm{x}) + \gamma * \mathrm{A}_3(\mathrm{x}) + \delta * \mathrm{A}_4(\mathrm{x})$$

where each of the A_i represent the level of damage to one of the mentioned areas (in this order): laws and regulations, commercial and financial interests, company's reputation and privacy and security of individuals. The coefficients allow adjusting the relevance each factor has with respect to the others.

Each of the consequences should be assessed in a scale from 0 to 4, being

0 – No damage to the organization
1 – Minimum damage with no significant impact on the organization
2 – Damage with clear impact on the organization
3 – Serious damage to the organization (future of the organization is not at risk)
4 – Maximum damage to the organization (bankruptcy, etc.)

Coefficients should range from 0 to 1, all of them summing up to 1. Aspects having stronger impact on the company's mission and business activity will be accompanied by higher coefficients. Note that organizations are free to add to the formula

additional terms representing factors they might find missed. It is not advisable to neglect any of the factors, i.e. assigning a value very close to 0 to any of the accompanying coefficients, as that would cause to ignore potential impacts affecting the particular factor. Coefficients should be used to tune the final result by adding information of the specific company context to the model. According to our estimations, it is not recommended to have any coefficient being more than twice the value of any other one. We recommend equally distributing the coefficients (i.e., 0.25 at each coefficient) and only adjust if there is clear evidence to do so.

Notice that the coefficients (α, β, γ, δ) are part of the general model built by the company to evaluate potential impact, while the damage on each factor (A_i) should be determined for each resource for which the potential damage wants to be calculated.

Here are some questions that can help in the determination of each of the Ai factors regarding the disclosure of a specific asset x. Notice that in case a certain fact affects more than one aspect, damage to each of them should be estimated independently.

Laws and regulations compliance

Is the disclosure likely to lead to an important/serious breach of legal or regulatory obligations? Consider not only external laws affecting the organization's activity but also internal regulations the company or the group to which it belongs can be subject to.

Commercial and financial interests

Does it facilitate significant improper gain or advantage for individuals or other organizations? Is x of high/medium interest to a competitor? Would the disclosure result in significant monetary or productivity losses?

Company's reputation

Is it likely to adversely affect relations with other organizations, the public, or other countries? To what extent? Is it likely to result in widespread adverse publicity? Could it lead to loss of public confidence in the organization? Could it lead to loss of current or potential employees trust? Could it lead to a serious breach of contractual undertakings to maintain the security of information provided by third parties?

Privacy and security of individuals

Does x contain sensitive information such as financial account number or medical records that can be linked to individuals? Is it likely to lead to the life of an individual or group of individuals being threatened?

Recall that this whole process should be carried out in the specific context of the organization in question. The same financial loss (in terms of absolute monetary units) won't have the same impact in a big and in a small company. Also, some aspects will be more critical to some kinds of companies. For instance, the impact a hospital would face if its customers' (i.e. patients) records are disclosed are higher than the impact faced by a dancing company giving up its customers' data. For this reason it is important that impact determination process is guided by managers and

staff involved in the company's activity and with some experience in the sector. It may be the case that the consequences of a confidentiality breach are rated differently by different stakeholders within the company. Therefore the proposed method requires a consolidation phase for the impact ratings (0-4). In this phase the organization has to identify the reasons for the deviations and has to harmonize the impact ratings. Furthermore, confidentiality categories might vary as part of the regular lifecycle of a process. For instance, the disclosure of an advertising campaign could have a considerable impact while is still being planned, but once it has been implemented the impact will be minimal, if not zero.

3.2 Validation - field test

To validate the approach, we conducted a field test in a 4-year-old software development company in Austria. The company develops information security software and has therefore a high interest in protecting the confidentiality of the products' source code. Because of its business activities, the company relies on its reputation and trustworthiness and because it is a young company, it is critical for them to maintain a quality service and gain its customers loyalty.

For validation purposes, the members of the management team were informed about the developed confidentiality determination method and asked to determine the required parameters. The management team discussed the weighting of the impact categories and decided to focus on the financial interest and reputation category (i.e. these categories were weighted higher than the remaining ones). The following weights were applied:

Laws and regulations: 0.2
Commercial and financial interests: 0.3
Reputation: 0.3
Privacy and security for individuals: 0.2

Therefore, the general formula used by the company to assess the impact level derived from the loss of confidentiality is:

$$I(x) = 0.2 * \mathrm{A}_1(\mathrm{x}) + 0.3 * \mathrm{A}_2(\mathrm{x}) + 0.3 * \mathrm{A}_3(\mathrm{x}) + 0.2 * \mathrm{A}_4(\mathrm{x})$$

After the category weighting we asked the management board to estimate the damage derived from the disclosure of the source code (0: no damage, …, 4: maxiumum damage to the organization):

Laws and regulations (A_1): 3
Commercial and financial interests (A_2): 4
Reputation (A_3): 4
Privacy and security for individuals (A_4): 1

Thus, the overall impact level derived from the disclosure of the source code is 3.2. Based on their experience, the calculated impact level has been approved by the man-

agement board. Within this field test we conducted 14 calculations regarding different assets to check if the calculation results comply with managements' opinion. 9 calculations provided obvious results (like the source code confidentiality calculation shown above). 5 calculations provided results which were not obvious to the management team (e.g., disclosure of personal data on invoices or e-mails). In these cases the method helped to think in a structured way about the confidentiality impact and plan appropriate countermeasures.

4 Conclusions and further work

Impact level determination is a complex and context-dependent process and a crucial step in security risk management processes. When approaching confidentiality, impact level estimations are more complex as the kinds of possible damage involved are of different nature and thus affect in different ways.

Approaching our original research question: "How can confidentiality requirements be determined for corporate assets?" we proposed here a method of impact level determination regarding confidentiality. The peculiarity of the method is that it estimates negative impact on different areas separately. That is, damage to laws and regulations, finance, or reputation are assessed independently and then combined to calculate the overall impact to the organization. The model also allows organization to give more relevance to some aspects than to others thus making the process more flexible and customizable.

Although this method leads to more accurate results in the context of each organization, it requires a lot of effort from qualified and experienced personnel. In further research we aim at automating the proposed method (e.g., by analyzing business processes and their interaction with the corporate assets).

5 References

Accorsi R. and Wonnemann C. (2011a) "InDico: Information flow analysis of business processes for confidentiality requirements" in 6th International Workshop, Security and Trust Management in Athens, Greece 2010. Springer Berlin Heidelberg, pp. 194-209

Accorsi R. and Wonnemann C. (2011b) "Strong non-leak guarantees for workflow models" in Proceedings of the 2011 ACM Symposium on Applied Computing in New York, USA, pp. 308-314

Accorsi R. and Lehmann A. (2012) "Automatic information flow analysis of business process models" in Business Process Management in Tallin, Estonia, 2012, Springer Berlin Heidelberg, pp. 172-187

Barker W., Stine K., Kissel R., Fahlsing J. and Gulick J. (2008a) "Volume I: Guide for mapping types of information and information systems to security categories" in NIST Special Publication 800-60 Volume I Revision 1, NIST, Gaithersburg, MD 20899-8930

Barker W., Stine K., Kissel R., Fahlsing J. and Lee A. (2008b), "Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories" in NIST Special Publication 800-60 Volume II Revision 1, Gaithersburg, MD 20899-8930

Club for the Security of Information in France (CLUSIF) (2010), "Method for Harmonized Analysis of Risk (Mehari)"

Department for business innovation and skills, United Kingdom (2013), "Information security breaches survey. Technical report"

Fenz, S., Ekelhart, A. and Neubauer, T. (2009), "Business process-based resource importance determination" in Business Process Management Conference in Ulm, Germany 2009, Springer, pp. 113-127

ISO/IEC (2013) "ISO/IEC 27001:2013, Information technology - Security techniques - Information security risk management"

Lehmann A. and Fahland D. (2012) "Information flow security for business process models - just one click away" Lohmann N. and Moser S. (Eds.) in Proceedings of the Demo Track of the 10th International Conference on Business Process Management 2012 in Tallinn, Estonia, 2012

Lehmann A. and Lohmann N. (2013), "Modeling wizard for confidential business processes" in Business Process Management Workshops in Tallin, Estonia, 2012, Springer Berlin Heidelberg, pp. 675-688

Lohmann N., Verbeek E. and Dijkman R. (2009) "Petri net transformations for business processes–a survey" in Jensen K. (Ed.), Transactions on Petri nets and other models of concurrency II. Springer, pp. 46-63.

McCallister E., Grance T. and Scarfone K.(2010) "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)" in NIST Special Publication 800-122, NIST Gaithersburg, MD 20899-8930

National Institute of Standards and Technology (2004) "Standards for Security Categorization of Federal Information and Information Systems" in Federal Information Processing Standards Publication 199, NIST, Gaithersburg, MD 20899-8930

National Institute of Standards and Technology (2012) "Guide for conducting risk assessment" in NIST Special Publication 800-30 Revision 1, NIST, Gaithersburg, MD 20899-8930

Spanish Ministry for Public Administrations (2006), "Methodology for Information Systems Risk Analysis and Management (MAGERIT) v2"