Considering technical and financial impact in the selection of security countermeasures against Advanced Persistent Threats

Gustavo Daniel Gonzalez Granadillo, Joaquin Garcia-Alfaro, Hervé Debar, Christophe Ponchel, Laura Rodriguez-Martin

Considering technical and financial impact in the selection of security countermeasures against Advanced Persistent Threats (APTs)

Gustavo Gonzalez Granadillo
Joaquin Garcia-Alfaro
Hervé Debar
Institut Mines Telecom, Telecom SudParis
CNRS UMR 5157 SAMOVAR, Evry, France
{first_name.last_name}@telecom-sudparis.eu

Christophe Ponchel
Laura Rodriguez Martin
Airbus Defence & Space CyberSecurity
Elancourt, France
{first_name.last_name}@airbus.com

***Abstract*—This paper presents a model to evaluate and select security countermeasures from a pool of candidates. The model performs industrial evaluation and simulations of the financial and technical impact associated to security countermeasures. The financial impact approach uses the Return On Response Investment (RORI) index to compare the expected impact of the attack when no response is enacted against the impact after applying security countermeasures. The technical impact approach evaluates the protection level against a threat, in terms of confidentiality, integrity, and availability. We provide a use case on malware attacks that shows the applicability of our model in selecting the best countermeasure against an Advanced Persistent Threat.**

I. Introduction

Cost sensitive metrics are widely proposed as a viable approach to find an optimal balance between intrusion damages and response costs. The main goal of such metrics is to provide the assessment of the potential impact that security actions may cause on the organization in a financial perspective. However, such security actions, while highly effective (in financial terms), might lead to operational negative side-effects (e.g., technical constraints) on their implementation.

In this paper, we propose a dual approach to evaluate security countermeasures in order to select the most appropriate response without sacrificing the system functionalities. The approach includes industrial evaluation and simulations of the financial and technical impact associated to a given security countermeasure.

The rest of the paper is structured as follows: Section II introduces the Advance Persistent Threats (APTs). Section III presents a comparison of the most used financial and information security metrics. Section IV details the financial countermeasure impact approach. Section V details the technical countermeasure impact approach. Section VI presents a case study on an Advanced Persistent Threat which shows the applicability of our approaches. Finally, conclusions and perspectives for future work are presented in Section VIII.

II. Advanced Persistent Threat (APT)

Over the last ten years, we have assisted to the advent of advanced, persistent and threatening computing attacks (abbreviated in the literature as APTs). APTs are complex cyber attacks executed in multiple stages over period of times that could count for months or even years to reach the final stage [1], [2]. APTs are not entirely new. These attacks use well-known strategies in order to target complex environments. They follow the logical evolution of traditional network and system attacks. What is substantially new about APTs is the vast number of current infrastructures they can eventually affect. Indeed, traditional critical infrastructures such as banking and energy are nowadays being upgraded with novel computing, communication and interconnection capabilities. This opens new areas that can be successfully misused by APTs, including assets from private companies and government networks. The associated costs, especially in terms of loss of business opportunities and the expense of fixing the incidents caused by APTs, shall be reduced.

APT attacks are generally executed throughout six stages [2]:

1) **Reconnaissance:** Gathering information about the target (via network scan, network mapping, employee profiling, search zero-day exploits).
2) **Delivery:** Spread information (via crafted emails, malware, malicious URL, phishing emails).
3) **Exploitation:** The malicious code is downloaded, installed and activated. Examples of exploitation can be: deliver spear phishing email, exploit employee user machine, collect user credentials, scan internal network.
4) **Operation:** Persistent presence in the organization network over long periods of time, that involves actions such as locate targeted data, target most privilege users, elevate access privileges, access sensitive data.
5) **Data Collection:** Operators use privileged users credentials to access targeted data. This stage involves selecting intermediary staging servers, moving, packing, encrypting, and compressing sensitive data.
6) **Exfiltration:** The information is transferred over encrypted channels to multiple external servers that act as drop points. This stage implies selecting drop servers, establishing large Control and Command (C&C) channels, initiating external connections, and exfiltrating data.

As we have seen, APTs are innovative in the way they syn-

thesize all the factors around a particular target, successfully gathering everything needed to prepare a long-term attack. The response to this threat shall also change. The vulnerabilities they aim to exploit will always exist. Mitigation of APTs is no longer a matter of taking actions, but rather how to manage them once APTs are discovered. This management will not only need to address technical aspects, but also financial and strategical aspects. The approach presented in the following sections aims to prepare some of the necessary building blocks to address the challenge.

III. Financial and Information Security Metrics

The economic approach for information security is closely related to the concepts of investment and return. This latter is commonly referred to as the amount of losses that are avoided due to a security investment; losses that were expected to occur had these investments not been applied [3]. In order to evaluate information security investments, financial models have been proposed, e.g., the Net Present Value (NPV) [4], the Internal Rate of Return (IRR) [5], and the Return On Investment (ROI) [6] and all its variants (e.g., Return On Attack [7] Return On Security Investment [8], Return On Response Investment [3]).

The remaining of this section discusses the characteristics of the different financial models based on five criteria: accuracy, time value of money, payback period, collateral damage, and corner cases such as the strategy of applying no operation (NOOP).

Accuracy: Estimating soft benefits parameters (e.g., fewer errors, reduced processing time, etc.) to calculate the Net Present Value or the Internal Rate of Return of a given project is extremely difficult [5]. A great level of subjectivity is considered while estimating parameters such as benefits and importance of the investment in the ROI model. In addition, it is very difficult to be accurate in predicting the attacker's behavior, an important parameter to calculate the ROA. Similarly, the ROSI and RORI metrics rely on parameters such as the costs and benefits of a security solution. In general, the costs of countermeasures are rather easily defined, in contrast with their benefits, since it requires prediction of an event that has not yet occurred.

Time value of money: While the ROI metric presents a percentage of return of an investment over a defined period of time, the IRR model does not inform about the absolute value of such investment. The NPV is the only approach informing about the absolute value of a project. The ROA, ROI, ROSI and RORI models face a problem in the case of long-term investments because they do not consider the time value of money. NPV has advantages within pre-investment analysis while all variants of the ROI metric are best for the ongoing assessment of investment profitability [9].

Payback period: The payback period is calculated by cumulatively summing the net cash flows of a project. When the sign of the cumulative sum of the net cash flows changes from negative to positive the project has paid back the initial investment [5]. The NPV and IRR models depend directly on the time period of the evaluation (results change if the time period of the analysis is reduced or extended). Since the time value of money is not considered in metrics such as ROA, ROI, ROSI and RORI, they are not useful for comparing projects that run over different periods of time.

Collateral damage: None of the cost-sensitive metrics described in this section, except for the Return On Response Investment, consider collateral damage as a parameter in their calculation. Collateral damages depend on both response mechanism and the current state of the target system. By modifying configurations, the response affects users of the target system, and thus resulting in collateral damages. Although they provoke mostly negative costs, response collateral damages are unlikely to be avoided when reacting against an intrusion attempt [11].

No operation: : A reasonable strategy when the mitigation cost is greater than the benefits it provides to the system, is to accept the risk. Acceptance is the choice of executing no operation (-NOOP- for short) against a security incident. From the previously described cost sensitive metrics, none of them, except for the RORI, are useful in evaluating NOOP. The ROA focuses on the attack behavior and therefore assumes that some gain and costs are associated to the incident. The ROSI considers the cost of the countermeasure in both, the numerator and denominator of the equation, leading to an indetermination in case of NOOP. RORI equals zero when evaluating the NOOP option, meaning that no gain is expected if no action is taken to mitigate a given attack.

IV. Financial Impact

Based on the limitations of the previously discussed models, we propose an improvement of the Return On Response Investment (RORI) index to quantitatively analyze the financial impact of an attack and the countermeasures selected for its mitigation. The improved RORI index is computed using Equation 1.

$$RORI = \frac{(ALE \times RM - ARC)}{ARC + AIV} \times 100 \qquad (1)$$

Where:

- ALE is the Annual Loss Expectancy and refers to the impact cost suffered in the absence of security measures. ALE is expressed in currency per year and will depend directly on the attack's severity and likelihood.
- RM refers to the Risk Mitigation level associated to a particular solution. RM ranges between zero and one hundred percent. In the absence of countermeasures, RM equals zero percent.
- ARC is the Annual Response Cost that is incurred by implementing a new security action. It corresponds to the sum of the operation cost (including setup and deployment costs) and the collateral damage costs (the cost added by the security measure) of the previous RORI index. ARC is always positive and is expressed in currency per year.
- AIV is the Annual Infrastructure Value (including cost of equipment, services for regular operations, etc.) that is expected from the system, regardless of the implemented countermeasures. AIV is always strictly positive and expressed in currency per year.

The quantification of the parameters composing the RORI model is a task that requires expert knowledge, statistical data,

simulation and risk assessment tools. A complete methodology of this quantification can be found in [12].

V. Technical Impact

In order to perform the technical impact analysis, we propose to evaluate a protection level against a threat, related to confidentiality, integrity, and availability, that considers technical and business services as assets. The cyber protection level is an evolution of the safety integrity level (SIL) [13]. This latter is determined based on a number of quantitative and qualitative factors such as development process and safety life cycle management.

The cyber protection level uses a risk assessment methodology to identify assets, threats, vulnerabilities, likelihood, countermeasures, and consequences. Although most organizations follow a particular methodology to deploy a risk analysis, current approaches do not consider the effectiveness of a protection function and rarely propose calculation methods for the protection level. Based on this, we propose to evaluate the technical impact of a security incident using parameters such as Effectiveness (EF), Risk Mitigation (RM) and Coverage (COV). Equation 2 shows the calculation of the Effectiveness factor of a countermeasure in mitigating a given threat.

$$EF \mid threat = \frac{RM \mid threat}{COV \mid threat} \tag{2}$$

Where:

- $RM \mid threat$ results from the delta between the risk level at time T1 (the risk of the model including countermeasures) and the risk level at time T0 (the risk for the model in supervision), as shown in Equation 3.
- $COV \mid threat$ results from dividing the number of incidents that a specific countermeasure covers (Ninc) by the total number of incidents that have been attached to a threat (NINC) as shown in Equation 4.

$$RM \mid threat = R_{T1} - R_{T0} \tag{3}$$

$$COV \mid threat = \frac{Ninc}{NINC} \tag{4}$$

From Equation 3, R_{Tn} is calculated as shown Equation 5.

$$R_{Tn} = P_x \times D_{real} \tag{5}$$

Where:

- P_x corresponds to the probability for the incident x to occur per year.
- D_{real} corresponds to the real danger for a threat, which is calculated by the difference between the level of danger for a specific service i (i.e., $D(threat, S_i)$), and the level of protection given by the product j, considered in the countermeasure $P(threat, P_j)$, as shown in Equation 6.

$$D_{real} = D(threat, S_i)(1 - P(threat, P_j) \tag{6}$$

The danger of a threat against a service S_i is given considering the service value in confidentiality (C), integrity (I) and availability (A), and the strength of the impact on the same criteria (i.e. C, I, A) due to the threat objective, as shown in Equation 7.

$$D(threat, S_i) = (S_C, S_I, S_A) \times (T_C, T_I, T_A) \tag{7}$$

The level of protection given by the product j for a specific threat is shown in Equation 8; where the $COV \mid threat$ has been discussed in Equation 4, and $EF \mid Pj$ represents the effectiveness of the product j for the countermeasure.

$$P(threat, P_j) = COV \mid threat \times EF \mid P_j \tag{8}$$

The Full Service Protection Level (FSPL) represents the sum of all individual Service Protection Level (SPL). Adding or removing protection items on services results into degradation or improvement of security at the service level. For each service, a list of couples (threat, protection flag) is provided. This gives the list of threats that endanger the observed service. When the protection flag is set to true, related threats are supposed to be mitigated by some of the protection means described in the model.

The FSPL is the average coverage against identified threats. It refers to all modeled services as shown in Equation 9.

$$FSPL = \frac{\sum_i COV(S_i) \times Cr(S_i)}{\sum_i Cr(S_i)} \tag{9}$$

Where:

- $Cr(S_i)$ is the criticality of the service i according to the significance configured in the model by an operator with respect to security expert knowledge and operational usage of the service. Service criticality is given as the maximum of service C, I, A values.
- $COV(S_i)$ is the average coverage of a specific service i against the threats it may be the target of, as shown in Equation 10.

$$COV(S_i) = \frac{\sum_{j=1}^{N} COV(S_i, threat_j)}{N_{threat}} \tag{10}$$

Where N_{threat} is the total number of threats.

Note that in the absence of threats, $COV(S_i)$ is 100.

VI. Case Study: Advanced Persistent Threat

A. General Description

Assuming that a malware file has been found in a host belonging to the marketing network of a banking institute, and it is suspected that it could gather and attempt to send confidential information. The company needs to start investigating how far the attacker has come, and update its network security policy in order to mitigate the attack impact and prevent from future incidents. The company is interested in assessing if those changes are technically effective and if they

are worth being made in terms of investment in the long run: are countermeasures profitable versus the attack cost?

The initial compromise assumes APT attackers have a solid knowledge of the company and they rely on several techniques to install a backdoor. This will let attackers get into the network as many times as they want. In this scenario it has been considered three different ways to install malicious software programs. (1) by attaching a piece of malware in a file and using phishing techniques; (2) by assuming the malware can be in an employee's USB drive; (3) throughout employees' mobile phones.

Once the malware is present, attackers have gained access to one or several machines inside the target's corporate network. They escalate privileges in order to facilitate lateral movement. The last step is data theft and leakage. Attackers are able to exfiltrate information from the compromised company.

B. Financial Analysis

As previously mentioned, this attack is considered as a three-step attack named as malware installation, presence and execution. The first step is divided into malware installation by USB drive, malware attached to an email, and mobile phone installation attempts. Vectors of infection are different and will be detected/prevented by different security products. The second step assumes the malware has already infected machines. Finally, the third step has been divided into data theft (capability to discover the compromised information) and data leakage (sending information out from the company network).

The Annual Infrastructure Value (AIV) includes the equipment costs, personnel costs, services costs and others and is estimated as 850,000€ by the company's experts.

The Annual Loss Expectancy (ALE) refers to the impact cost obtained in the absence of security measures. Therefore, if the attack is revealed, financial impact may be very high as reputation and trust will decrease. A significant part of customers will leave the bank and potentiality for new customers will decrease. ALE is estimated in 1,000,000€ (1M€) by the company's experts.

Countermeasure Candidates: The following list of security countermeasure has been selected to mitigate the effects of an advanced persistent threat. Each countermeasure will modify the original banking data model and has an associated cost (ARC) and mitigation effect (RM) on the system.

C.1 **No Operation (NOOP):** Accepting the risk without performing any modifications. The cost and risk mitigation level are equal to zero.

C.2 **Update Security Policies:** Updating policies and rules of every perimeter security equipment.

C.3 **McAfee Security for Email Server:** Investing on professional security software to detect malicious mailing and prevent them to reach target inboxes.

C.4 **Symantec Endpoint Encryption:** Reinforcing the security on equipments with sensitive data and protecting them with data encryption in order to avoid data theft.

C.5 **McAfee EPO & Agents:**Reinforcing the surveillance of all equipments that belong to the organization to detect malware presence.

C.6 **Cyber Insurance:** Assuming the risk and considering to invest in cyber-insurance

Table I summarizes the information regarding benefits, costs and the RORI values of each security countermeasure.

TABLE I. RORI EVALUATION FOR AN APT

Countermeasure	ARC	RM	RORI
C.1. NOOP	0.00€	0.00%	0.00%
C.2. Update Security Policies	80,000€	16.15%	8.76%
C.3. McAfee Security for Email Server	40,000€	15.30%	12.70%
C.4. Symantec Endpoint Encryption	110,000€	14.45%	3.59%
C.5. McAfee EPO & Agents	100,000€	29.70%	20.74%
C.6. Cyber Insurance	37,000€	0.00%	-4.17%

From the financial perspectives, the countermeasure that provides the highest benefit to the organization is C.5, which suggest to reinforce the surveillance of the organization's equipments to improve malware detection. The next section presents the results of the technical evaluation of all countermeasures.

C. Technical Analysis

This section evaluates the technical capabilities of all security countermeasures through the analysis of the full service protection level (FSPL) detailed in Section V. It should be emphasized that the FSPL for the model in supervision without countermeasures has been assessed in 68%. Hereinafter this value will be compared with the one provided by each countermeasure candidate.

The APT occurrence was split into six types of incidents: data leakage, data theft, malware attached to email, malware installation from USB drive, malware installation in mobile device, and malware presence. Each identified countermeasure covers either zero, or only one incident, except C.5 that covers 2 incidents. The coverage (COV) is therefore rounded to 0%, 17% (1/6) or 33% (2/6).

The product effectiveness ($EF \mid P_j$ as described above) defines the protection capability against different attack types. In this example, for simplification purposes, it is assumed that the product effectiveness value comes from expert knowledge. As per each countermeasure simulation, we only introduce one kind of product with a full deployment, the EF parameter will be assimilated to $EF \mid P_j$.

Please note that the FSPL is a general value that applies to all services of the model, whereas, the risk mitigation applies for a single service and a threat. Table II summarizes this information.

From the technical perspective, C.5 is the countermeasure with the highest Full Service Protection Level (FSPL) value. Countermeasure C5 is focused in reinforcing the surveillance of all equipment that belong to the organization in order to detect malware presence. This countermeasure takes into account malware detection deploying antimalware agents. C5 considers including the commercial product McAfee EPO and anti-virus agents. This implies inserting two new products in the security product section. Such products will be added to the incident category section as detection/prevention means. In addition, from the model point of view, a new server will be

TABLE II. RORI EVALUATION FOR AN APT

CM	Incident Category	Equipment	EF	COV	FSPL
C.1.	any	none	0.00%	0.00%	68.00%
C.2.	data leakage	netask FW/IPS upgrade policy	95.00%	17.00%	70.00%
C.3.	malware attached to email	McAfee Security for Email Server	90.00%	17.00%	69.00%
C.4.	data theft by malware	Symantec Endpoint Encryption	85.00%	17.00%	69.00%
C.5.	malware presence and installation from USB drive	McAfee EPO & Agents	90.00%	33.00%	71.00%
C.6.	any	Insurance	100.00%	0.00%	68.00%

added as equipment and agents will be inserted into the hosts as applications.

As a result, the implementation of countermeasure C5 will have a positive impact on the overall level of service protection, going from 68% (actual FSPL) to 71% (potential FSPL).

VII. RELATED WORK

Cost sensitive metrics are widely proposed as a viable approach to find an optimal balance between intrusion damages and response costs, and to guarantee the choice of the most appropriate response without sacrificing the system functionalities. The Return On Response Investement (RORI) has been first introduced by Kheir et al. [3] as a service dependency model for cost sensitive response based on a financial comparison of the response alternatives. RORI is an adaptation of the ROSI [8] index that provides a qualitative comparison of response candidates against an intrusion. The parameters that constitute this index are derived from the ROSI parameters by drawing an analogy between costs for intrusion prevention and response.

The deployment of the RORI index into real case scenarios has presented the following shortcomings:

- the absolute value of the cost parameters is difficult to estimate, which generates accuracy and magnitude issues;
- the model is not originally defined when no solution is enacted (NOOP);
- the model is not normalized with the size and complexity of the infrastructure;
- the model can not be deployed to evaluate multiple countermeasures simultaneously;

Based on the previous shortcomings, we propose an improvement of the RORI model that considers not only the countermeasure cost and its associated risk mitigation, but also the infrastructure value and the expected losses that may occur as a consequence of an intrusion or attack. The improved RORI handles the choice of applying no countermeasure to compare with the results obtained by the implementation of security solutions (individuals and/or combined countermeasures), and provides a response that is relative to the size of the infrastructure.

In addition, The service protection level is an evolution of the safety integrity level (SIL), which is defined as a relative level of risk reduction provided by a safety function. The process is generally used to identify assets, threats, vulnerabilities, likelihood, countermeasures, and consequences. This is usually obtained from a risk analysis, following any of the international standards (e.g., NIST [14], ISO [15]), or any of the risk management methodologies (e.g., MEHARI [16] and EBIOS [17]) as well as expert knowledge.

Although most organizations follow a particular methodology to deploy a risk analysis, current approaches present the following shortcomings:

- they rarely propose calculation methods for the protection level;
- none of them can be applied on an operational environment with "living" protection means (i.e., potentially unavailable for a period of time);
- they do not consider the different instances that must be deployed in the network to cover the threat everywhere;
- the effectiveness of a protection function is hardly considered in the analysis.

Taking into account current shortcomings in risk analysis methodologies, we propose to evaluate a protection level against a threat, related to confidentiality, integrity, and availability, that considers technical and business services as assets.

VIII. CONCLUSION AND FUTURE WORK

We propose in this paper an approach to evaluate and select security countermeasures based on industrial evaluation and simulations of the financial and technical impact associated to a group of countermeasures. The financial impact considers the Return On Response Investment (RORI) as a metric that evaluates parameters such as the attack impact (i.e., Annual Loss Expectancy), the countermeasure impact (i.e., Annual Response Cost, Risk Mitigation), and the infrastructure size (i.e., Annual Infrastructure Value). The technical impact considers the countermeasures technical capabilities based on the analysis of the full service protection level (FSPL).

The combination of these two aspects (i.e., financial and technical impact) provides an important decision support for the selection of security countermeasures against complex threats (e.g., APTs). However, as information and communication systems also involve human intervention, equally important is the compatibility of the countermeasures with the security culture of the organization and their usability.

Our approach has been deployed in a case study that considers a complex cyber attack (i.e., Advanced Persistent Threat) executed in multiple stages over long period of times. An analysis of the threat is led by experts along with a state-of-the-art set of potential countermeasures. Cost of the attack, countermeasures, and annual expenses in security are evaluated as well. Proposed countermeasures take into account different points of view keeping the focus in the ways an APT can be remediated.

Once the experts' report is provided, simulation tools are used to get risk mitigation and RORI values applied to the APT threat with the data model representing the banking infrastructure and business services. The resulting evaluation helps network and system administrators to select security countermeasures based on their financial and technical impact assessment.

Future work will concentrate in improving the effectiveness evaluation by introducing the product effectiveness per incident type (currently the product effectiveness is the same whatever the incident). Then, accuracy will be improved by assessing the global effectiveness of a countermeasure in regards with a threat, making it possible to evaluate cases when different products are used as part of a single countermeasure. Formalizing the product effectiveness measurement will (and must) be addressed as well.

Technical impact associated to security countermeasures shall be evaluated in terms of architectural weaknesses. Such weaknesses may affect both information and operational technologies (i.e., IT and OT related weaknesses). Therefore, they must also be addressed in terms of functional security. While the technical impact criteria concerning security aspects for IT traditionally give higher priority to confidentiality over integrity and availability, the counterpart concerning functional aspects for OT shall give higher priority to integrity and availability rather than confidentiality. In this paper, we addressed the technical impact assessment based on traditional IT security aspects. We are actually extending the approach to properly balance the technical analysis in a holistic manner, to address the analysis in terms of both IT and OT.

ACKNOWLEDGMENT

The research in this paper has received funding from the Information Technology for European Advancements (ITEA2) within the context of the ADAX Project (Attack Detection and Countermeasure Simulation) and the PANOPTESEC project. Authors acknowledge support from the EC Framework Program, under the PANOPTESEC project (GA 610416), as well as the Spanish Ministry of Science and Innovation (project TIN2011-27076-C03-02 CO-PRIVACY).

REFERENCES

[1] Websense: Advanced Persistent Threats and other Advances Attacks: Threat analysis and defense strategies for SMB, mid-size and enterprise organizations, White Paper, (2011)

[2] Giura, P., Wang, W.: A Context-Based Detection Framework for Advanced Persistent Threats, Int. Conference on Cyber Security, (2012)

[3] Kheir, N., Cuppens-Boulahia, N., Cuppens, F., Debar, H.: A Service Dependency Model for Cost-Sensitive Intrusion Response, 15th European Symposium on Research in Computer Security, pp. 626–642, (2010)

[4] Puangsri, P.: Quantified Return On Information Security Investment - A Model for Cost-Benefit Analysis, Master Thesis, Delft University of Technology, (2009)

[5] Jeffrey, M.: Return on Investment Analysis for e-Business Projects, Internet Encyclopedia, H. Bidgoli Editor, vol. 3, pp. 211–236, (2004)

[6] Schmidt, M.: Return on Investment (ROI): Meaning and Use, Encyclopedia of Business Terms and Methods, Available at: http://www.solutionmatrix.com/return-on-investment.html, (2011)

[7] Cremonini, M., Martini, P.: Evaluating Information Security Investment from Attackers Perspective: the Return-On-Attack (ROA), 4th Workshop on the Economics on Information Security, (2005)

[8] Sonnenreich, W., Albanese, J., Stout, B.: Return On Security Investment (ROSI) A Practical Quantitative Model, Journal of Research and Practice in Information Technology, vol. 38, number 1, (2006)

[9] Locher, C.: Methodologies for Evaluating Information Security Investments - What Basel II Can Change in the Financial Industry, ECIS Proceedings, Paper 122, (2005)

[10] Gordon, L., Loeb, M.: Return on Information Security Investments: Myths vs. Realities, Strategic Finance, vol 84(5), (2002)

[11] Kheir, N.: Response policies and countermeasures: Management of service dependencies and intrusion and reaction impacts PhD Thesis, Ecole Nationale Supérieure des Télécommunications de Bretagne, (2010)

[12] G. Gonzalez Granadillo and M. Belhaouane, H. Debar, and G. Jacob, *RORI-based countermeasure selection using the OrBAC formalism*, Int. Journal of Information Security, Vol. 13(1), pp. 63-79, 2014.

[13] A. Ingrey and P. Lereverent and A. Hildebrant, *Safety Integrity Level*, Manual PEPPERL+FUCHS, 2007.

[14] National Institute of Standards and Technologies, *Guide for Conducting Risk Assessment*, 2012.

[15] International Standard ISO/IEC 27005, *InformationTechnology - Security Techniques - Information Security Risk Management*, available at http://www.iso27001security.com/html/27005.html, 2008.

[16] Clusif, *MEHARI 2010 - Risk Analysis and Treatment Guide*, available at http://mehari.info/, 2010.

[17] ANSSI, *EBIOS 2010 - Expression of Needs and Identification of Security Objectives*, available at http://www.ssi.gouv.fr/IMG/pdf/EBIOS-1-GuideMethodologique-2010-01-25.pdf, 2010.