Security Triage: A Report of a Lean Security Requirements Methodology for Cost-Effective Security Analysis

Matteo Giacalone*, Rocco Mammoliti*, Fabio Massacci†, Federica Paci†, Rodolfo Perugino*, Claudio Selli*
*Security and Safety, Poste Italiane SpA, Roma, Italy - {giacal69,mammoliti.rocco,peruginor,c.selli}@posteitaliane.it
†DISI, University of Trento, Trento, Italy - {name.lastname}@unitn.it

***Abstract*—Poste Italiane is a large corporation offering integrated services in banking and savings, postal services, and mobile communication. Every year, it receives thousands of change requests for its ICT services. Applying to each and every request a security assessment "by the book" is simply not possible. We report the experience by Poste Italiane of a lean methodology to identify security requirements that can be inserted in the production cycle of a normal company. The process is based on surveying the overall IT architectures (*Security Survey*) and then a lean dynamic process (*Security Triage*) to evaluate individual change requests, so that important changes get the attention they need, minor changes can be quickly implemented, and compliance and security obligations are met.**

I. How to Secure Evolving ICT Systems?

For Poste Italiane - the largest Italian employer offering integrated services in finance, logistics, and mobile communication with a turnaround of around 24 billion Euro - balancing security and change means identifying security requirements for over 150 change requests/month and over 2000/year.

A simple solution is to just follow existing methodologies and standards like ISO 27005 [1], USA's NIST 800-30 [2], CoBIT [3] Germany's BSI [4], France's EBIOS [5], Spain's Magerit [6], UK's IAS [7], etc. One can also use academic methods (e.g. Misuse Case [8], SI* [9], CORAS [10], SQUARE, [11], SREP [12], etc.).

Both industry and academic approaches alike look simple and straightforward on paper. Yet, they very rarely report the *actual effort* needed to perform a security analysis "by the book" in an industrial setting. The earliest publication mentioning the actual effort for the identification of security requirements [13] reported that "The CommerceNet requirements analysis [Re-engineering the web server for taking electronic payments] was conducted by 4 analysts, the authors, and various stakeholders, for approximately 30 hours a week over a period of four months".

With 2000+ requests per year, applying to each request a methodology "by the book" as in [13] would require around 400 people working full time for the whole year long, just to identify the requirements!

In this report we present the results of a year long project at Poste Italiane where a lean, innovative security requirements methodology has been experimented *in vivo* and successfully deployed at a large scale.

II. Overview of the Solution

Our objective is to streamline the security requirements identification process so that it can process thousands of requests per year. Our solution combines two key ideas from architecture and medicine.

The first notion is that of a *Security Triage* [14]. In medicine, the Triage is the process where "medical personnel systematically categorize victims of a disaster into three groups: those who will die whether treated or not; those who will resume normal lives whether treated or not, and those for whom medical treatment may make a significant difference. Each group requires a different strategy. The first group receives palliative care, the second group waits for treatment, and the third requires some ranking in light of available resources. As new victims appear, personnel must repeat the categorization". Similarly, in our methodology, the Security Triage is performed directly by the proposer of the change request, the "Owner" of the business service, along the guidelines of the Security Team. The Service Owner classifies change requests based on their relevance as described in Section V. Requests with a "red code" are subject to a full fledged analysis "by the book", while the requests with "white code" will proceed directly to implementation of baseline security requirements.

Still, we must be sure that a Security Triage is not just a politically correct term for a sloppy security assessment. The second instrument, the *Enterprise (security) Survey* is our solution to the problem. In architecture, a land surveyor builds a detailed map of an area by observations, measurements in the field, research of legal instruments, and data analysis in order to establish property boundaries, identify buildings and support planning (of new buildings). The Survey provides the identification of the components of the IT architecture, the breakdown of those into compliance and security perimeters against which a Triage (for the new component) can be successfully performed. A survey is *not* just an architectural diagram, no more than a map is the only result of a land survey. Attaching business values, identifying owners, drawing legal boundaries, etc. are all essential parts.

III. Security Analysis "by the book"

The default application of an *Information Security Risk Management Process* (ISRM) follows the ISO 27001 standards (see [1] for details):

978-1-4799-6336-2/14/$31.00 © 2014 IEEE

EmpiRE 2014, Karlskrona, Sweden

TABLE I
EXAMPLE EFFORT FOR ISRM ANALYSIS

Level	Questions	Time	Unit
Process/People	300	3hrs	Process
Information	16	1hrs	Data
Applications	250	3hs	Application
Software components	200	2hrs	Type of Asset
Infrastructure	200	2hrs	Type of Asset
Facilities	100	1hrs	Facility

Traditional ISRM asks almost 1000 questions, for more than a full day of work, without mentioning the time necessary for actually finding the answer to each question.

Asset and Process Identification describes the overall architecture of process impacted by the change;

Business Impact Analysis targets the information used by each service and the impacts of compromising its confidentiality, integrity, and availability;

Risk Assessment at the level of *Process, People, Application, Infrastructure, Facilities Analysis* identifies gaps and current risk levels (Table I);

Security Requirements Identification produces a menu of security measures that can be implemented;

Risk Treatment, or acceptance of residual risks, is decided by the Service Owner on the basis of the analysis and the business consideration and implemented by the ICT Department.

Filling the questionnaire from Table I takes 2 working days and with 2000 requests per year it is more than 10 persons working full time for a year just to fill the paperwork, let alone doing any mitigation.

IV. ICT SECURITY SURVEY

The high level purpose of the *ICT Security Survey* process is to provide a comprehensive characterization of the ICT and business services of the company.

The first step is called "Census" and is an ongoing refinement of the enterprise architecture. It brings together the Business View and the IT View of the systems. In land surveying this is the measurements of the fields and the drawing of the maps.

Each "logical" component (services, macro-products, products, applications) is then categorized as belonging to a number of *Perimeters* that determine the baseline in terms of security requirements that must be implemented. We called this part of the process "Mapping". In land surveying this would correspond to draw boundaries and identifying ownership of tracts of land measured in the first phase. Each perimeter would be a layer in the physical map (e.g. rainfall, ownership, vegetation etc.). Overall there are more than 20 different perimeters that can be cross-combined in a variety of ways.

A further classification is then performed to assess the relevance of each asset for the company:

Level C1: services that do not manage personal data and not associated with security perimeters;

Level C2: services that handle personal data but not bound to security and compliance perimeters;

Level C3: services that manage personal data and bound to security and compliance perimeters;

Level C4: services that manage personal and sensitive data or with medium economic relevance;

Level C5: services that are fundamental from a business perspective and that are bound to relevant security and compliance perimeters.

V. SECURITY TRIAGE

When a change request is placed, the Service Owner identifies the service related to the change request and the compliance and security perimeters (if changed from the service already described in the survey's catalog). After this initial analysis, the *Business Impact Analysis* (BIA) is performed:

Economic Operating Loss is appreciated by Service Owner as the actual monetary amount that a breach to the service will imply;

Loss of Reputation as could be perceived by suppliers, end users, and national regulators in case of breaches of the service's security;

Loss of Competitiveness includes the possibility for competitors to exploit the security breach to gain market share or even directly exploit the leaked information for direct purposes; and

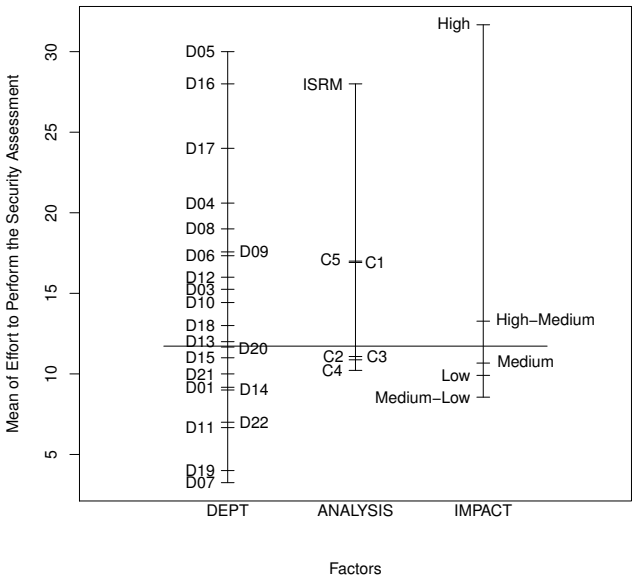
Legal Liabilities include fines or criminal prosecution related to security breaches.

For each category a Service Owner is faced by 16 questions grouped by impact type: *loss to confidentiality, loss to integrity and loss to availability*. Answer to each category have been streamlined to "make sense" for a Service Owner (as opposed to a Security Expert). For example, for the economic losses, a Service Owner should appreciate whether a loss to availability for a certain number of hours might lead to minor or major economic loss. Another example: for the legal liability category, she might be asked whether a violation to integrity might lead to an administrative offense with monetary fine or a criminal offense with minimum jail terms. Typical notions used by security expert such as session compromise, forward compromise, root control etc. are difficult to grasp. They would be investigated for the change requests that have the highest level C5.

This information is combined with the information from the Survey to obtain a final value for the request.

VI. EMPIRICAL EVALUATION

The process of surveying and triage has been first piloted in 2012, with a product in the e-financial sector in March 2012. In June 2012 over 1600 new change requests have been identified as possible activities to be included in the pilot phase. By the end 2012 other two major pilots for internal processes for financial procurement and supply chain management concluded. In 2013 the procedure has been applied to a much larger scale and it is now in full swing.



ISRM analysis takes almost twice more effort than Security Triage-based analysis (C1…C5). As a control, notice effort is distributed across all departments and high impact cases take a significant effort as expected. (Each dash is mean effort per category)

Fig. 1. Plot Design of Effort by Category

We measured the effort (number of days) required to identify security requirements following the ISRM process with the effort required by the Security Survey and Triage process. In particular, we wanted to test the following hypothesis:

H_1: *Identify requirements by ISRM takes more effort than by Security Survey and Triage (C1-C5).*

Figure 1 shows the distribution of the mean of the effort required for a security assessment. This variable has been measured uniformly across the various requests and makes *relative* comparisons possible. The first vertical line shows the mean of the effort grouped by departments placing a change request. The second vertical line shows the mean of the effort required to identify security requirements following the ISRM process and the effort required for security requirement elicitation by Security Survey and Triage grouped by the level of relevance of the change requests. The third vertical line represents the mean of the effort required to identify security requirements grouped by the impact that change requests had on the business. ISRM analysis takes almost twice more effort than Security Survey and Triage process (C1…C5). This is also attested by the results of Mann-Whitney test that shows the difference in effort is statistically significant (p-value = 0.00453). Thus hypothesis H_1 is upheld. We can thus conclude that the combination of Security Survey and Security Triage is more effective than the "by the book" approach.

It is important to note that *both* components are necessary for the approach to work in practice. Having only a Triage without the Survey just generate a poor people risk assessment that does not guarantee meeting compliance obligations. Having the Survey without the Triage means that the Survey quickly becomes obsolete and security assessments lag behind.

VII. Conclusions

In this paper we have reported a lean innovative approach for the identification of security requirements stemming from a year long project conducted by Poste Italiane. The process is based on an global mapping analysis of the overall ICT landscape (*Security Survey*) and then a lean dynamic process (*Security Triage*) to quickly identify the level of relevance of a request for security assessment and the corresponding security requirements. We have also provided some data the show the approach significantly reduces the time to identify security requirements at the pace of change.

The Security Survey and Triage process should be embedded in a company's production cycle as mandatory step to prioritize security initiatives based on the relevance of the assets and of the business objectives of the company.

Acknowledgment

This work has been partly supported by the EU under grant agreements n.256980 (NESSOS) and n.285223 (SECONOMICS), by the SESAR JU WPE under contract 12-120610-C12 (EMFASE) and by MIUR-PON under project PON03PE_00032_2_02 within the framework of the Technological District on Cyber Security.

References

[1] ISO/IEC, *27005:2011–Information Technology–Security Techniques–Information Security Management Systems–Requirements*, 2011.
[2] G. Stoneburner, A. Goguen, and A. Feringa, *Risk management guide for information technology systems*. NIST, 2002.
[3] ISACA, *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*, 2012.
[4] BSI, *Standard 100-2, The IT-Grundschutz Methodology*, 2011.
[5] ANSSI, *EBIOS 2010 - Expression of Needs and Identification of Security Objectives*, 2010.
[6] F. L. Crespo, M. A. Amutio Gomez, J. Candau, and J. A. M. Manas, *Magerit v2 –Methodology for Information Systems Risk Analysis and Management - Book I - The Method*, 2006.
[7] CESB, *HMG Information Assurance Standard 1*, 2009.
[8] G. Sindre and A. Opdahl, "Eliciting security requirements with misuse cases," *REJ*, vol. 10, no. 1, pp. 34–44, 2005, cited By (since 1996) 217.
[9] P. Giorgini, F. Massacci, J. Mylopoulos, and N. Zannone, "Requirements engineering for trust management: model, methodology, and reasoning," *IJIS*, vol. 5, no. 4, pp. 257–274, 2006.
[10] M. S. Lund, B. Solhaug, and K. Stolen, "A guided tour of the coras method," in *Model-Driven Risk Analysis*. Springer, 2011, pp. 23–43.
[11] N. R. Mead and T. Stehney, "Security quality requirements engineering (square) methodology," *SIGSOFT*, vol. 30, no. 4, pp. 1–7, May 2005.
[12] D. Mellado, E. Fernández-Medina, and M. Piattini, "Towards security requirements management for software product lines: A security domain requirements engineering process," *CSI*, vol. 30, no. 6, pp. 361–371, 2008.
[13] A. I. Anton and C. Potts, "The use of goals to surface requirements for evolving systems," in *Proc. of ICSE '98*, 1998, pp. 157–166.
[14] A. Davis, "The art of requirements triage," *Computer*, vol. 36, no. 3, pp. 42–49, 2003.