A Collaborative System Offering Security Management Services for SMEs/mEs

Theodoros Ntouskas, Dimitrios Papanikas, and Nineta Polemi

Department of Informatics, University of Piraeus,
Karaoli & Dimitriou 80, 185 34 Piraeus, Greece
{tdouskas,papanik,dpolemi}@unipi.gr

Abstract. Although small, medium and micro enterprises (SMEs, mEs) play a decisive role in the European digital economy, they have been identified as one of the weakest links in information security. Identifying these security weaknesses and needs we parameterize our open collaborative environment STORM in order to offer a cost-efficient tool to the SMEs and mEs for self-managing their security.

Keywords: Collaboration, Security management, Vulnerability assessment, Risk Management, SMEs, mEs.

1 Introduction

Small, medium and micro enterprises (SMEs, mEs) play a decisive role in the European digital economy. Despite the increasing demand for their services as suppliers and sub-contractors in value chains of larger companies, they also have been identified as one of the weakest links in information security. Unable to comply with stricter security demands to the business value chains as established by large businesses and their customers, SMEs and mEs may find themselves losing business opportunities.

These enterprises (SMEs, mEs) cannot easily foster a more secure attitude in their business activities (causing them security problems and bridges) due to their peculiar characteristics [1]:

- Minimal resources on budget or time prevent SMEs and mEs to evaluate and ensure security and privacy as a continuing activity;
- Lack of trained and security educated personnel dedicated to the task of security and privacy;
- Education is considered as extra cost with no tangible benefit;
- Dependency on external security expertise, strong tendency to rely for their security / privacy strategy on external support, making sourcing decisions primarily on the basis of cost and vicinity;
- Lack of formal security policy and strategy, a plan determining the level of security needed as well as a policy outlining how to operate and maintain security is not a highly prioritized issue for management;

H. Jahankhani et al. (Eds.): ICGS3/e-Democracy 2011, LNICST 99, pp. 220–228, 2012.

- Lack of attention by their managers to address legislative or regulatory requirements, even if there is a penalty for not doing so;
- Lack of far-sightedness by the business managers thinking of themselves as of "no interest" from a global perspective ("We're too small - who would want to attack us?");
- Risk-agnostic of their ICT security risks involved, as well as the resulting business risks (e.g. operational loss, breach of statutory obligations, customer loss, and damage to reputation) and the extended risk to e-business as a whole.

Being the backbone of the economy and chief provider of jobs in many EU Member States, this may create severe damage to the innovativeness and competitiveness of European economy. Therefore, enhancing information security practices of SMEs and mEs has become an urgent need.

Existing well-defined and widely adopted security methodologies, standards and tools, are inadequate to meet the SMEs/mEs' basic characteristics. This paper contributes towards the urgent need to improve the current security and privacy level of these enterprises by adjusting an open, collaborative and trustful information security management system, STORM [2] considering the SMEs/mEs characteristics. In particular, the risk management methodology, STORM RM, is improved (originally presented by the authors in [3]) with a new step for practical vulnerability assessment (in order to achieve accurate vulnerability evaluations) and its main steps are customized targeting the SMEs/mEs characteristics. Also the enhanced STORM RM methodology [3] is implemented as a user friendly STORM service enabling the non security qualified SMEs/mEs personnel to use it in order to self-manage their security.

The rest of the paper is organized as follows: Section 2, assesses existing security management standards, methodologies and tools against SMEs and mEs security needs. Section 3, describes the STORM-RM enhanced methodology and service along with its basic modules, that are customized in order to help SMEs and mEs solve their particular security problems. Finally, Section 4 draws conclusions and future research directions.

2 Assessment of Security Management Approaches

Managing information security requires a continuous and systematic process of identifying, analyzing, mitigating, reporting and monitoring technical, operational and other types of security risks. This section assesses and outlines the weaknesses of the existing information security approaches when applied to SME/mEs.

A bundle of Security Management standards have been developed in order to help organizations to develop Information Security Management such as Cobit [4], ITIL [5], ISO-17799 [6] and ISO-27001 [7]. These standards define security requirements that cover many areas of the security lifecycle such as, ICT, operational, legal and organizational security requirements. Also, security standards have been developed to support the implementation of the required security

controls, such as the ISO 27002 [8], Nist SP 800-53 [9]. Typically, setting up an Information Security Management System requires economic and human resources that are usually not available within the environment of SMEs/mEs who tend to consider security as a burden, rather than an asset in terms of profit. Although there exist automated tools to support security management lifecycle (such as ISO17799 Toolkit [10] or NetSPoC - Network Security Policy Compiler [11]), they are either too expensive for SMEs/mEs or in case of free tools, support capabilities for non-experts do not exist.

Existing RA/RM methodologies are targeted to bigger organizations and are too complex for mEs and SMEs since they do not possess the appropriate resources and expertise. The limitations of existing RA/RM methodologies can be summarized as follows:

- they are too complicated for the SMEs/mEs information systems requiring external, expensive, support. Simplifications and automated steps of the methodologies and the tools are still required to meet the SME/mEs characteristics;
- they are not supported by free of charge automated tools. Commercial tools supporting such methodologies are expensive and thus not likely to be used by micro and small enterprises;
- there is a lack of collaborative, multi-attribute, group-decision making approaches. More sophisticated approaches that enable collaboration, both within and between enterprises are required, especially for small and medium businesses with distributed IT systems.

Vulnerability assessment (VA) is yet another problem for the SME/mEs. Several initiatives have been launched releasing a set of methodologies and frameworks for VA. Some of these efforts emphasize on application security testing [12], [13] aiming at assessing and improving the security web applications while others mainly focus on network security testing by describing applied techniques and tools [14], [15], [16].

Also, open research communities have created open environments [17], [18], [19] that have been pre-configured to function as VA platforms. These platforms contain a set of open source/freeware tools that focus on testing information and communication systems. The main identified weaknesses of the existing VA approaches can be summarized as follows:

- there is a lack of VA methodologies, which would support the self implementation of a technical vulnerability assessment,
- although free of charge VA platforms and tools are in place, it is highly unlikely that SMEs and mEs will be able to trace, configure and utilize these tools, due to their lack of expertise and time availability. In addition, such open platforms do not usually come with instructions about how these environments have been configured or installation guidelines of the embedded tools.

There is an urgent need to develop targeted security management methodologies and tools addressing the SMEs/mEs characteristics and overcome the above mentioned obstacles.

3 STORM Security Management Service for SMEs/mEs

This section presents the targeted risk management service, STORM-RM, for the SMEs/mEs and its integration in the STORM environment.

STORM is an innovative, collaborative, cost effective and user friendly security consultancy environment (developed by the authors [2]) based on widely used collaborative web 2.0 technologies and can be used by different type of organizations in order to collaboratively manage their security, offering a pool of interactive services.

In order for SMEs/mEs to use STORM, the STORM Identity & Access Management system (STORM-IAM)[2] is customized in order to control the access to STORM services by SMEs and mEs users. Based on the STORM-IAM procedures and authentication mechanism, SMEs and mEs users will have access to the collaborative services, in order to cooperate and exchange information and ideas, work together in building open working groups, providing diverse opinions, thoughts and contributions and sharing information, experience and expertise. Notable components of these services are the Open and Private Forums and the Chat Rooms that support public and private discussions as well as the Open Knowledge area that acts as a knowledge source of security related information (e.g. security standards, specifications, reports, vulnerability assessment (VA) methodologies and frameworks, legal and regulatory directives and recommendations, open source and freeware tools and platforms, cases studies).

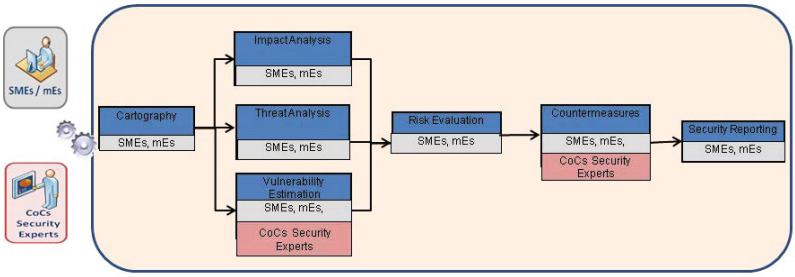

Fig. 1. STORM-RM Service for SMEs/mEs

Furthermore, the STORM Risk Management methodology (STORM-RM) (first presented in [3]) is enhanced, parameterized and implemented as a modular service (each step of the methodology is integrated independently and can be separately accessed depending on the users role/privileges reported in the STORM

IAM).The STORM-RM service (Fig. 1) consists of the following modules enabling SMEs/mEs to: capture all assets of their IT system (Cartography); identify their security critical asset(s) (Impact analysis); reveal their threats (Threat Analysis); estimate their vulnerabilities (Vulnerability Estimation) / risk levels (Risk Evaluation) of their assets and select the appropriate Countermeasures for their organization. The final collected outcome of the above modular steps is embedded in the Security Reporting.

Taking into account the specific characteristics (e.g. minimal resources / expertise) of the SMEs and mEs, STORM system is proposed to be hosted by an appropriate service provider (SP), e.g. the Chambers of Commerce (CoC). The CoCs are natural candidates to become STORM SPs since their fundamental responsibility is to serve the interests of their members (SMEs and mEs mostly). The CoCs mainly identify and underscore their members' needs by promoting, stimulating and supporting any initiative that aims at creating and developing innovative business services for them (and security is definitely a business driver). Their existing security team will embrace the STORM-RM service (Fig.1) which will be offered at low cost to their SMEs/mEs members.

In the following section, the STORM-RM enhanced methodology and the implemented service (in Fig.1) will be described.

3.1 STORM Risk Management Service (STORM-RM) for SMEs/mEs

STORM-RM service integrates and implements the STORM-RM methodology [3], which is based on Analytic Hierarchy Process, AHP [20] and is customized in order to address the specific characteristics of the SMEs and mEs. All the steps of STORM-RM methodology are implemented in an automated, self explanatory, user friendly manner by making use of interactive screens, online forms and help menus. The distinctive steps of the STORM-RM methodology are implemented as independent modules of the STORM-RM service (see Fig. 1). The autonomous modules of the STORM-RM service are:

Module 1 - Cartography: This module is implemented using online forms and consists of four (4) phases. In the *first phase*, all assets of ICS (e.g. servers, rooters, applications, users etc.) are reported and categorized in four main groups (hardware, software, services and participants). In the *second phase*, each service is associated with its interactive hardware, software and participant(s), in order to report the interdependencies and interconnection of assets. In the *third phase*, installed security controls (e.g. back-ups/ access control policies) (if any) are reported. The appropriateness of these controls are assessed against the ISO-27001 [7] proposed controls as well as their implementation maturity (e.g. fully, partly or not implemented). In the *fourth phase*, weights (opinion priorities) of all participants (administrators, managers, end users) are calculated, according to their role in the organization and the services that they use. To summarize the output of this module will be: all assets categorized in four groups (hardware, software, services, participants) with technical and operational characteristics;

all assets interconnections; all already installed controls and their assessment in terms of appropriateness and maturity; opinion weights of the organization participants (these weights will be used in the impact and risk analysis).

Module 2 - Impact Analysis: Distinct online questionnaires, stored in the STORM Content Management System (CMS), evaluating the security importance (taking into consideration the consequences of security loss i.e. loss of availability, integrity, confidentiality) for each asset are assigned automatically by the STORM tool to different groups of participants depending on their organizational role (administrators, managers, end users) and their access rights provided by the STORM-IAM. The group impact level is calculated by the STORM-RM automated multi-criteria algorithm [3], taking into account the weight of each participant of the organization. The output of this module is a list with all the assets, A_i, and their Impact security levels, I(A_i) , with possible values: Very Low = VL, Medium= M, High = H, Very High = VH.

Module 3 - Threat Analysis: In this module, the stored list in the STORM CMS with all possible threats categorized accordingly (e.g. physical, technical etc.) and correlated with different type of assets (e.g. server, application, router etc.) is used as follows: Each participant prioritizes the listed threats, corresponding to an asset, using online forms and then these priorities are taken into account in order to calculate the final group threat level for each asset. The threat priorities are calculated by the automated STORM-RM algorithm which in return estimates the Threat value, T(A_i), of each asset, A_i. The results of this module are depicted with interactive screens that help participants to view which threats are more possible to occur for every asset of the organization.

Module 4 - Vulnerability Estimation: In this module the Vulnerability Assessment (VA) and the estimation of the Final Vulnerability level (FV) for each asset A_i are calculated using four (4) distinct phases. *Vulnerability Identification:* During this phase, every threat is connected with corresponding vulnerabilities and each asset A_i is examined in terms of the vulnerabilities revealed from their correlated threats. *Theoretical Vulnerability Level:* Every user u_j compares, in this step, the vulnerabilities assigned to each asset A_i in order to calculate its Theoretical Vulnerability level, $TV_{u_j}(A_i)$ which in turn are collected within the STORM group decision tree [18] in order to calculate the Group Theoretical Vulnerability level (the resulting level from all u_j' s for a specific A_i), TV(A_i). *Practical Vulnerability (PV) Level:* Taking into consideration the list of assets and their Impacts levels, A_i, I(A_i), from Module 2, PV assessment is executed only for the assets with very high Impact level, i.e. I(A_i)=VH. Depending on the asset type (e.g. hardware, software etc.), STORM-RM suggests the appropriate open source, online, vulnerability assessment (VA) tool(s), stored in the STORM-CMS, to be used by the users; these VA tools are stored in the STORM-CMS. Security consultants of the service provider assess the results, which are exported by security testing tools, and estimate the Practical Vulnerability, PV (A_i), level of each tested asset A_i. *Final Vulnerability Level:* In this final phase, the Final Vulnerability Level, FV(A_i), is calculated for each asset A_i with Impact level I(A_i)= VH, as the maximum between the Theoretical

Vulnerability Level, TV(A_i), and the Practical Vulnerability Level, PV(A_i); for these assets A_i with Impact level I(A_i) < VH, the Final Vulnerability Level, FV(A_i), equals with the Theoretical Vulnerability Level, TV(A_i), as described in the following formula:

$$FV(Ai) = \begin{cases} \max(TV(A_i), PV(A_i)) & if I(A_i) = VH \\ TV(A_i) & if I(A_i) < VH. \end{cases} \quad (1)$$

Module 5 - Risk Evaluation: After collecting all values for Impact, I(A_i), Threat, T(A_i), and Final Vulnerability, FV(A_i), levels, the risk value, R(A_i), of each asset, A_i, is calculated here as the product:

$$R(A_i) = I(A_i) * T(A_i) * FV(A_i) \quad (2)$$

SMEs/mEs participants have the capability to see through online forms the results of STORM-RM risk analysis for all assets and decide which is the risk threshold (e.g. if R(A_i) > 6 then A_i is security critical) in order to continue with the next module of the security countermeasures' selection.

Module 6 - Countermeasures: There is a list of different type countermeasures (e.g. technical, physical etc.) that are appropriate for different type of asset (e.g. servers, rooters, application) stored in the STORM -CMS. SMEs/mEs participants are able to view all choices and select (using on-line forms) the appropriate countermeasures that wish to implement, taking into account different criteria (e.g. economical, business, legal, technical, performance) from their own business perspective. Each user of the above groups gives priorities through online judgments for all the recommended countermeasures of each asset. The final selection of countermeasures is the result of the automated AHP algorithm that STORM-RM uses [3], according to the participants' priorities. The outcome of this module is a list of the selected appropriate countermeasures that is implemented in order to minimize the identified risks.

Module 7 - Security Reporting: All security reports (produced in each module) can be generated as online growing documents in various representation formats and with personalized content (e.g. risk reports for all assets with characteristics, threats and risks interconnected with a particular service).

4 Conclutions and Future Work

SMEs and mEs have to take a more strategic comprehensive view of information security. They should treat it as a factor that guarantees and enhances their viability in a competitive, turbulent and diverse globalized e-market. In this context, STORM system, via the provision of a bundle of innovative security and privacy services offers these enterprises several benefits, such as increasing their competitiveness by strengthening their ICT security and data privacy level of their electronic services in a demonstrative way; respecting the regulations and standards and thus offering them competitive advantage in the area of trustful e-business in a cost-efficient, economic and collaborative way. In addition,

STORM-RM service improves their business processes by providing a simplified, integrated and comprehensive framework for the identification, assessment and treatment of security and privacy risks improving their ICT-based business processes.

Future work includes the integration of theoretical and practical vulnerability assessment on an upper level. Also STORM RM service will be implemented at the S-PORT system [21] and will be tested by three Greek commercial Ports (Piraeus Port Authority S.A., Thessaloniki Port Authority S.A, Municipal Port Fund Mykonos).

Acknowledgements. This work has been performed in the framework of the GSRT/SYNERGASIA/S-Port project (09SYN-72-650) (http://s-port.unipi.gr).

References

1. Reynolds, D., Rabey, K., Polemi, N.: Analysing mes needs and expectations in the area of information security. ENISA report (2008), http://www.enisa.europa.eu/act/sr/reports/micro-enterprises/files/wg-micro-report
2. Ntouskas, T., Pentafronimos, G., Papastergiou, S.: STORM - Collaborative Security Management Environment. In: Ardagna, C.A., Zhou, J. (eds.) WISTP 2011. LNCS, vol. 6633, pp. 320–335. Springer, Heidelberg (2011)
3. Ntouskas, T., Polemi, N.: STORM-RM: A collaborative and multicriteria risk management methodology. Int. J. Multicriteria Decision Making 2(2), 159–177 (2012)
4. COBIT4.1: It governance control framework. IT Governance Institute (2007), http://www.isaca.org
5. Clinch, J.: Itil v3 and information security, ogc white paper (May 2009), http://www.best-managementpractice.com
6. ISO/IEC:17799: Information technology - security techniques - code of practice for information security management (2005), http://www.iso.org
7. ISO/IEC:27001: Information technology - security techniques - information security management systems - requirements (2005), http://www.iso.org
8. ISO/IEC:27002: Information technology - security techniques - code of practice for information security management (2005), http://www.iso.org
9. NIST SP800-53: Recommended Security Controls for Federal Information Systems and Organization. NIST Special Publication 800-53, http://csrc.nist.gov/publications/PubsSPs.html
10. ISO17799: Toolkit, http://www.iso17799-made-easy.com/
11. NetSPoC: Network Security Policy Compiler, http://netspoc.berlios.de/
12. Agarwwal, A., Bellucci, D., Coronel, A., DiPaola, S., Fedon, G., Goodman, A., Heinrich, C., Horvath, K., Ingrosso, G., Liverani, R.S., Kuza, A., Luptak, P., Mavituna, F., Mella, M., Meucci, M., Morana, M., Parata, A., Su, C., Sureddy, H.S., Roxberry, M., Stock, A.: Owasp testing guide v3.0 (2008), http://www.mare-system.de/whitepaper
13. Stock, A.V.D., Lowery, D., Rook, D., Cruz, D., Keary, E., Williams, J., Chapman, J., Morana, M.M., Prego, P.: Owasp code review guide v1.1 (2008), https://www.owasp.org

14. NIST SP800-42: Guideline on Network Security Testing - Recommendations of the National Institute of Standards and Technology. NIST, http://www.iwar.org.uk/comsec/resources/netsec-testing/sp800-42.pdf
15. NIST SP800-115: Technical guide to information security testing and assessment. NIST, http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf
16. Orrey, K., Lawson, L.J.: Penetration testing framework(ptf) v0.21, http://www.vulnerabilityassessment.co.uk
17. Backtrack, http://www.backtrack-linux.org/
18. Net Tools 5.0, http://www.mabsoft.com/nettools.htm
19. Samurai Web Testing Framework, http://samurai.inguardians.com/
20. Saaty, T.L.: Decision making with the analytic hierarchy process. Int. J. Service Sciences 1, 83–98 (2008)
21. S-PORT: S-port project, http://s-port.unipi.gr/