Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 160 (2019) 181–188

Procedia Computer Science

www.elsevier.com/locate/procedia

The 10th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2019)
November 4-7, 2019, Coimbra, Portugal

A Conceptual Model for a Metric Based Framework for the Monitoring of Information Security Tasks' Efficiency

Ferda Özdemir Sönmez[a],*

[a] *Informatics Institute Middle East Technical University, Üniversiteler Mahallesi, Dumlupınar Bulvarı No:1 06800 Çankaya, Ankara, Turkey*

Abstract

Information Security Governance Systems are not adequate to measure the effectiveness and efficiency of security tasks for the enterprises. Although some of the systems offer ways for measurement, they still need the definition of measurement objectives and metrics. This study proposes a conceptual framework mode which has human and tool/process related metrics. This system also allows the collection of evidence data for security-related tasks and ways to motivate the security staff to provide a more productive environment. This system may be applied to any size of enterprise independent of its business domain or functions as long as the aim is to improve the effectiveness and efficiency of security-related tasks.

Keywords: Information Security Governance; Security; Efficiency; Metric; Productivity;

1. Introduction

Although there are numerous information security governance (ISG) frameworks, which focus on different aspects of information security, none of them has a specific focus for the efficiency of information security tasks. ISG's have many benefits as long as they work efficiently for an organization. Otherwise, the difficulties that they bring may exceed the benefits that they provide. The downside of these ISG's do not offer a way to measure the efficiency and effectiveness of adopting those in an organization. This deficiency has been identified by ISO and a

* Corresponding author. Tel.: +90-532-694-3503 ; fax: +90-312-210-5401.
E-mail address: ferda.ozdemir@metu.edu.tr

10.1016/j.procs.2019.09.459

specific standard, ISO/IEC 27004:2016 Information technology – Security techniques – Information security management – Monitoring, measurement, analysis, and evaluation, aiming to measure the effectiveness and efficiency of applying ISO 27K standards has been prepared.

Security related tasks can be very complicated from time to time. Existing information security governance systems are not adequate to measure and improve the efficiency of complex security tasks. A framework is needed, which deals with the measuring of the efficiency and provides ways to increase this efficiency. In order to depict the importance of having a framework dealing with the efficiency of complicated enterprise security tasks, an example task, data visualization is selected. Data visualization is a task commonly used as a part of various information security or cybersecurity examinations. Data visualization is not an independent task; on the contrary, visualization is the last process following numerous other tasks. It requires using various data collection, design, and analysis techniques. Multiple software and hardware technologies have to be involved in this process. Using the correct tools, systems, and procedures in a productive manner is vital. There are various problems in terms of identifying and sharing critical information. Education related to security visualization tools and techniques would increase the efficiency of the users. Other human originating factors affecting productivity include enterprise culture and habits and system-based factors.

Being lack of proper tools and processes in the enterprise causes lower efficiency or not effectively doing tasks. Low number of metrics, abounding or lacking the measurement data or wrong measurement techniques are some enterprise related factors would result in lower productivity for the security related tasks essentially. Specifically, for data analysis and data visualization tasks, being not familiar to the current status of data available to be visualized or to be analyzed is also a problem. Another enterprise originated factor is not encouraging or gifting actions of knowledge sharing within the team and the enterprise. Not learning or encouraging the use of newly emerged tools and technologies are other human originated factors.

The rest of the paper is constructed as follows. Section two is the state-of-the-art section. Section three has the problem definition and research questions. In section four, there is a description of the proposed solution, Enterprise Security Productivity Center. Finally, section five is devoted to the discussion and the concluding remarks.

2. State of Art

Rebello et al. [1] provided a comparative summary of nine ISG frameworks including ISACA [2], NIST [3], ISO [4], A practical guide to implement and control Information Security Governance [5], Information security policy: An organizational level process model [6], Information Security Governance by Solms [7], IT Governance Institute [8], and the ISG by Software Engineering Institute [9]. Performance measurement capability is one of the evaluation criteria. Based on Rebello et al.'s comparison, all the ISG frameworks did not contain adequate performance measurement features with two exceptions, ISO standards [4], and the ISG by IT Governance Institute [8].

ISO/IEC 27004:2016 [10], Information technology – Security techniques – Information security management – Monitoring, measurement, analysis, and evaluation is developed to provide a way for the measurement of the effectiveness of information security governance system. This standard aims to evaluate the effectiveness and efficiency of the IOS-IEC 27K standards. The author did not encounter an implementation of this standard focusing on other information security governance systems. By measuring the effectiveness of ISG, ISO/IEC 27004:06 also aims to improve the risk assessment and security management investments.

Measuring the effectiveness of ISG also would help the top-level management who in general track return on investment, ROI and don't know much about security. ISO/IEC 27004:2016 requires determination of measurement objects, having the measures in three levels: base measures, derived measures, and the indicators. The standard later relies on the comparison of measurement results with the decision criteria. In order to conduct a measurement based on ISO/IEC 27004:2016, the user of the standard requires to decide the data associated to the measurement object and select a way to collect that specific data. The standard contains information related to analysis and reporting of measurement values. Issues associated with the presenting and communicating the measurement results with the stakeholders are also included in the standard [11].

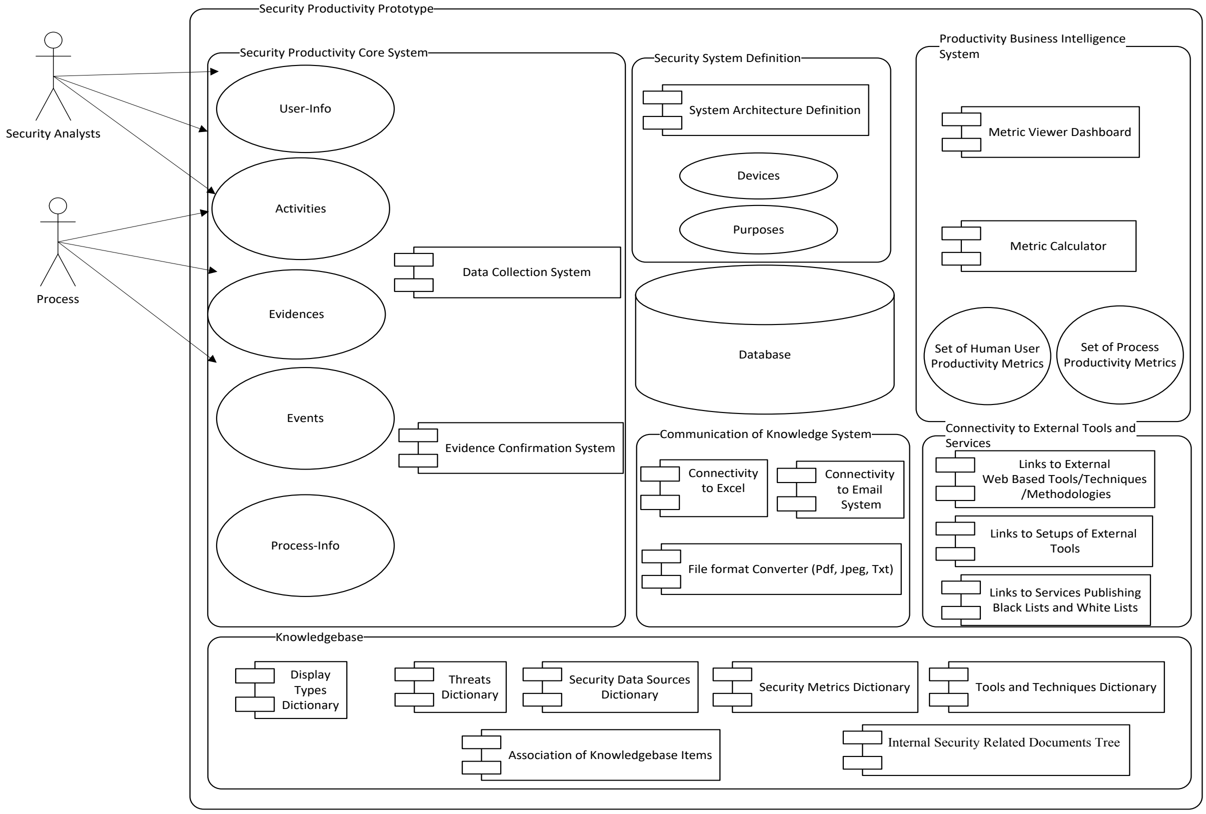
Security Productivity Prototype
Security Analysts
Process
Security Productivity Core System
User-Info
Activities
Evidences
Events
Process-Info
Data Collection System
Evidence Confirmation System
Security System Definition
System Architecture Definition
Devices
Purposes
Database
Productivity Business Intelligence System
Metric Viewer Dashboard
Metric Calculator
Set of Human User Productivity Metrics
Set of Process Productivity Metrics
Communication of Knowledge System
Connectivity to Excel
Connectivity to Email System
File format Converter (Pdf, Jpeg, Txt)
Connectivity to External Tools and Services
Links to External Web Based Tools/Techniques /Methodologies
Links to Setups of External Tools
Links to Services Publishing Black Lists and White Lists
Knowledgebase
Display Types Dictionary
Threats Dictionary
Security Data Sources Dictionary
Security Metrics Dictionary
Tools and Techniques Dictionary
Association of Knowledgebase Items
Internal Security Related Documents Tree

Fig. 1. Enterprise Security Productivity System

3. Problem Definition and Research Questions

Knowing the fact that existing other ISG frameworks are not adequate for the measuring of effectiveness and ISO/IEC 27004:2016 requires determination of measurement objectives, corresponding data and data collection techniques, there is a need for a metric-based framework aiming the measurement of the effectiveness of security processes and tasks. This framework should assist the users of the ISO/IEC 27004 standard during implementation.

The research questions identified at this step by the author are "what are possible generic measurement objectives which may apply to most organizations?". This question aims to find out the measurement objectives independent of ISG framework or implementation details. The second question is: "what are the corresponding metrics?". The third and last question is: "how to collect data to achieve the measurement tasks?"

4. Proposed Solution- Enterprise Security Productivity Center

The proposed solution is a conceptual framework aiming to provide an organization of a set of metrics which correspond to measurable objectives and the metrics related research questions. It also has some functional offerings aiming to improve the efficiency of complex security tasks and the listed problems in the previous sections. These offerings include ways to collect data to achieve measurement tasks which correspond to the third research question.

The goals of the proposed Enterprise Security Productivity Center are as follows:

- Measuring and displaying the productivity of human users and security tools and devices in a dashboard form.
- Forming an enterprise security knowledgebase which will eventually aid in reaching the information and providing a space to store and share enterprise know-how.
- Storing and sharing of earlier findings of security related tasks
- Providing a mechanism to evaluate these findings internally
- Improve and encourage communication and knowledge sharing
- Causing an even distribution of tasks among human beings
- Monitoring the productivity of both humans and processes
- Forcing the security team on making continuous improvement in security structure, program, and processes besides daily activities
- Encourage the team to be innovative and to use and learn new tools and techniques

Enterprise Security Productivity Center, EntSecProd, is a conceptual model. To achieve the listed purposes, the top-level architecture of EntSecProd including various modules is shown in Figure 1.

"Security Productivity Core System" module contains a mechanism to harvest and store security analysis outputs of employees'. These outputs should be associated with users, activities, and events. This module is also responsible to process the measurement information. The outputs are considered as pieces of evidence of the security-related tasks done by both human beings and the processes. These pieces of evidence should be confirmed by other employees by a confirmation mechanism. The confirmation rules can be specific to and defined by the organization. A simple rule can be such that evidence should be seen and agreed by at least two employees to be considered as confirmed. Once evidence is confirmed, it may be used for further analyses, and in the reports. The number of evidences captured will eventually affect the productivity score of both the human staff and corresponding processes and tools.

"Productivity Business Intelligence" module provides a means to acquire company intelligence competitively and a dashboard specifically designed to monitor the productivity of the team and tools/devices/methodologies. In order to achieve this target, metrics to measure the productivity of the security team and tools/devices/methodologies are defined. A preliminary list of enterprise security metrics aiming to measure the productivity of the security team and security tools/devices/methodologies are listed in Table 1, and Table 2. As well as visualizing these metrics in dashboard form in EntSecProd, these metrics can be used to increase the metric lists in the existing ISG frameworks.

Table 1- Enterprise Security Productivity Security Team Metrics

Measurement Focus	Metric Name
Process	• Days from last .... security audit/analysis • Days to .... security audit/analysis • Number of planned/unplanned night time work for security team members • Number of planned/unplanned weekend work for security team members
Performance	• Most active team members • Least active team members • Number of days in a month where active security analysis results exist for the team member
Outcomes	• Number of security analysis reports by team members • Number of security analysis made by team members in a time period • Number of visual pieces of evidence that are found by the team members • Number of new installations for the analyses purposes
Quality	• Education level • Years of experience • Number of piece of evidences/outputs that are confirmed as useful by management
Trends	• Increase in the number of outcomes in a month • Number of newly learned tools and techniques
Conformance to Standards	• Number of information security certificates that are related to security standards for security team members • Number of educations given/taken by the security team member related to security standards
Probabilities	• Number of educations that team members are attended in a time period (which may affect their future level of productivity)

Table 2- Enterprise Security Productivity Security Tools and Processes Metrics

Measurement Focus	Metric Name
Process	• Number of file types supported by the security tool • Number of file format types supported by the security tool • Number of automated reports provided by the security tool • Number of data displays provided by the security tool
Performance	• Total amount of file size investigated using a certain tool/methodology in a time period • Duration to automatically analyze 1000 lines of records in a specific type of log file • Installation/set up duration • Average learning duration for security tool/methodology
Outcomes	• Number of network alerts • Number of restricted network requests • Ratio of scanned and processed web pages • Number of application vulnerabilities
Quality	• Having advanced user interaction properties such as patterns searching capturing and saving analysis results for later use • Having multiple displays in one view allowing more efficient comparison • Is the security tool use latest external security data automatically, such as white lists, spam lists.
Trends	• Duration passed by the emergence of tool/methodology • Number of updates made in the last year for the tool/methodology
Conformance to Standards	• Is the tool/methodology supported by or related to a universally accepted security standard • Does a universally accepted standard suggest the tool?
Probabilities	• Integration capabilities of the system with other devices such as having web service interfaces, allowing database access connectivity with ERP systems, connectivity to an email system

Before continuing with other modules, it is necessary to explain how the proposed metrics are identified or in other words designed. The author decided to use a well-known taxonomy of metric types while preparing the preliminary productivity metrics list. Brotby [12] provided several taxonomies for security metric types. One of these categorization systems is based on “what the metric measures”. This categorization is preferred among others which deal with "how the metric data is collected", and "when the measurement for the metrics are made". This categorization has the following items: process, performance, outcomes, quality, trends, conformance to standards, and probabilities. These categories have various reflections on the productivity of the tools and the human staff. These reflections resulted in offerings all of which have direct or indirect impact on the productivity of the human staff and the tools while achieving security-related tasks.

The process criteria is considered as working habits, such as daily or night work time, frequency of overtime work for the human staff, and capabilities such as file types supported for a tool. The performance criteria is considered as the number of security analysis results submitted in a month, the average rank of the work submitted, and security related working hours for human staff. The performance metric for a tool will vary. A few examples are the total amount of file size investigated using a certain tool/methodology in a time period, or duration to automatically analyzing a fixed amount of code or log file. Installing or setting up some tools may require higher effort. Average learning duration is also considered a measurement which will affect the performance of using a tool. Outcomes are related to submissions or analysis results provided by both human staff and the tools. Quality factors which affect the productivity of staff while doing security tasks include items like education level, years of experience, and the number of confirmed submissions of previous work for a staff member. The quality of a tool which will affect productivity is considered as the set of predefined features such as connectivity alternatives, and the number of compliance reports provided. The trends for staff are thought of the amount of change in the number of outcomes in a time period and number of newly learned tools and techniques. The trend related metrics of a tool is considered to be related to the amount of maintenance effort spent on that tool by the tool vendor. For example, the trend for a tool which has not been updated for years shows that this tool may cause problems which may affect productivity in the short or long term. Duration passed by the emergence of tool/methodology, and the number of updates made in the last year for the tool/methodology are in this category. Conformance to the standards is thought to be related to the number of security certifications owned by a staff member. Conformance to standards for a tool points out the standards obeyed or supported by a tool. The idea is if the tool is supported by a universal standard it's being already tested by experts and by a community, which will also affect its usability, and thus, the overall productivity of the security tasks. The number of educations that team members are attended in a time period which may affect their future level of productivity is placed under the probabilities category for a staff. Integration capabilities of the system with other tools such as having web service interfaces, allowing database access, connectivity with ERP systems, connectivity to email systems are among the probabilities which may enhance the productivity for a tool.

"Security System Definition" module includes a standard way to define IT Infrastructure architecture definition. This part also includes the definition of currently used devices and tools together with the definition of the staff in charge of each tool and device. From time to time finding out installation details and people in charge of a security protection system takes days in a large organization which will eventually decrease the productivity of the security team. Clear definition of purposes of the tools and devices will also help to understand and use the system better. For example, one security device a firewall can be used for various purposes such as protecting all of the organization, protecting a department, part of an organization, and protecting a specific system.

Another example is a honeypot which can be installed for various purposes such as threat detection or educational tasks. The standard definition of devices, tools, and other infrastructure elements should include the definition of data sources which may be resulted related to them. During this definition, adding basic information related to security data sources, such as expected size in a time period, the average frequency of investigation will also be beneficial during the planning phases of security tasks.

"Knowledgebase" module includes several dictionaries including the threat dictionary, display types dictionary, security data sources dictionary, common security metrics dictionary, and tools and techniques dictionary. These dictionaries may include basic knowledge which may be useful when designing new analysis techniques. For example, some display types are more proper to visualize some data types, definitions of threats will increase the effectiveness and understandability of the analyses results. Including tools, methodologies, and how to use guides will decrease the learning time, the definition of security metrics and association of metrics to data sources and tools will allow saving the enterprise knowledgebase in a reusable form. The "Knowledgebase" module also contains a document tree which includes other essential security-related documents, such as policies, standards, and methodologies.

"Communication of Knowledge" module provides ways to better share the security-related information stored in all other parts of the EntSecProd. This module should include connectivity features to excel to export the data, connectivity to an email system to speed up sharing the knowledge process, and ways to enable conversion of data and evidence to various formats such as JPG, TXT, and PDF to speed up report creation.

"Connectivity to External Tools and Services" include a mechanism to route to newly emerged technologies, data, and tools. This will allow the central definition of links to external tools, methodology definitions, repositories in an enterprise which will provide easy reach to external knowledge, and increase the know-how of the enterprise and encourage self-learning of security staff. This mechanism includes a part with static links to pages with services publishing blacklists and white lists, a part including links to set up pages for commercial or freeware applications, such as links to trial versions, or links to open source versions, and a part including links to available web-based security-related applications.

5. Discussion and Concluding Remarks

To recap, in this study, a framework intending to provide a platform for the measuring of efficiency of the security tasks for human users and the security tools and devices has been described. Having a set of metrics associated with the productivity of human users and tools and devices would also enable easy implementation of Information Security Governance Systems which aim measurement of performances through the use of measurement objectives and metrics. Although other ISG frameworks allow some level of measurement, ISO/IEC 27004:2016 is the one single example of this group in the author's knowledge.

Having an enterprise security knowledgebase, the proposed system aims to increase both the effectiveness and the efficiency of the security analyses tasks. The assets and corresponding risks change from enterprise to enterprise. The countermeasures to prevent, diminish, and transfer these risks will change in parallel to assets and risks. The objective of this study is not to make risk analysis or to suggest new technologies to improve or harden existing infrastructures. The aim is to present novel metric alternatives associated with the effectiveness and the efficiency.

The main downside of this study is staying in a conceptual state. Implementation of the proposed enterprise security productivity system would require time and budget which are far above the limits of this study. Another difficulty, related to this system is evaluation because this system would require the contribution of an organization who is willing to use share its data and resources for a period of time. Besides the requirement of a huge resource and time, this may also cause privacy issues.

Although the system lacks an actual implementation and subsequent validation effort, the author believes that its own unique and novel perspective, structure and metrics would enhance both existing information security governance systems regarding their capabilities of measuring efficiency and effectiveness and may cause the formation of new ones.

Its novelty does not merely due to the measurement objectives and the proposed metrics. Its structure relies on rather than simply collecting data and showing it in a dashboard form but instead has a base to increase the productivity by providing better collaboration, by easing access to data and by creating a competitive environment in terms of security analyses tasks.

References

[1] Oscar R, Mellado D, Sanchez LE, Fernández-Medina E. Comparative Analysis of Information Security Governance Frameworks: A Public Sector Approach. In Proceedings of the 11th European Conference on EGovernment; 2011; Ljubljana, Slov. p. 482-490.

[2] ISACA. ISACA. [Online].; 2019. Available from: HYPERLINK "www.isaca.org" www.isaca.org .

[3] Bowen P, Hash J, Wilson M. Information security handbook: a guide for managers. Standard. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY; 2007.

[4] Disterer G. Iso/iec 27000, 27001 and 27002 for information security management. Journal of Information Security. 2013; 4(2).

[5] de Oliveira Alves GA, da Costa Carmo LFR, de Almeida ACRD. Enterprise Security Governance; A practical guide to implement and control Information Security Governance. IEEE/IFIP Business Driven IT Management. 2006;: p. 71-80.

[6] Knapp KJ, Morris Jr. RF, Marshall TE, Byrd TA. Information security policy: An organizational-level process model. Computers & Security. 2009; 28(7).

[7] Solms VR. nformation security management (2): guidelines to the management of information technology security (GMITS). Information Management & Computer Security. 1998;: p. 221-223

[8] ITGI. Information Security Governance: Guidance for Boards of Directors and ExecutiveManagement 2nd Edition. Rolling Meadows, USA:; 2006.

[9] Westby JR, Allen JH. Governing for Enterprise Security (GES) Implementation Guide. Pittsburgh, USA:; 2007.

[10] ISO. Information technology—Security techniques - Information Security Management- Monitoring, measurement, analysis and evaluation. Standard. ISO; 2016. Report No.: ISO/IEC 27004:2016 (E).

[11] Kosutic D. Free webinar: ISO 27001 and ISO 27004: How to measure the effectiveness of information security? [Online].; 2019 [cited 2019 7 13. Available from: HYPERLINK "https://advisera.com/27001academy/webinar/iso-27001-iso-27004-measure-effectiveness-information-security-free-webinar" https://advisera.com/27001academy/webinar/iso-27001-iso-27004-measure-effectiveness-information-security-free-webinar .

[12] Brotby KW. Information Security Management Metrics A Definitive Guide to Effective Security Monitoring and Measurement: Auerbach Publications; 2009.