Winter 12-13-2015

Development of an Artifact for Benchmarking Information Security Policy

Dae Youp Kang
Korea University

Anat Hovav
Korea University

Development of an Artifact for Benchmarking Information Security Policy

Dae Youp Kang
Business School, Korea University, Seoul, South Korea {kangd@korea.ac.kr}

Anat Hovav
Business School, Korea University, Seoul, South Korea {anatzh@korea.ac.kr}

ABSTRACT

Benchmarking of information security policies has two challenges: lack of communication between organizations and no two organizations are identical. In this paper, we attempt to propose an artifact for a benchmarking method of information security policy (BMISP), which can resolve the above challenges. We employ design science methodology, activity theory and international standards to design the artifact as a proof of concept. We illustrate the applicability of the artifact using our pilot data.

INTRODUCTION

Endeavors to find an adequate balance between information security policy (ISSP) and investments in security have been discussed in the literature. Examples include: marginal returns to security investments (Hausken 2006), the optimal amount to invest in protecting a given set of information (Gordon et al. 2002), and the relationship between information security investment, stock market and IT value (Chai et al. 2011; Otim et al. 2012). Based on these actions, practitioners and scholars have suggested a number of methods for efficient investments such as return on security investments (ROSI), risk assessment, cost benefit analysis (CBA), and market-value analysis. According to CSI report of 2011, 68% of companies use ROSI to justify security investments, 12% use net present value (NPV) and 15% use internal rate of return (IRR) (Berger 2011).

However, these methods have fundamental challenges. Losses of information security are difficult to quantify since some are intangible (Hovav and D'Arcy 2003). Moreover, some incidents may cause zero damage while one incident can cause millions of dollars in damage

(Hovav 2014; Wang et al , 2008). In addition, the objectives of some cyber-attacks are not for profits. Thus, the attacks are unclear and create a domino effect. The consequences from these types of attacks are difficult to calculate because it is complex to predict all possible vulnerabilities and due to lack of historical data (De Bruijn et al. 2010). On the other hand, a benchmark provides details on which controls should be considered following the recommended practices or industry standards. Benchmarking provides balanced investments calculation through the process of seeking out and studying practices used in other organizations (Whitman et al. 2013). Through benchmarking, the organization may employ collective intelligence based on previous experience in its industry. However, benchmarking has two major challenges. Firstly, organizations are reluctant to share data regarding information security that is sensitive to the operation, reputation and company's value (Whitman et al. 2013). Another challenge with benchmarking is that no two organizations are identical. Even if two organizations offer products or services in the same market, their size, composition, management, organizational culture and technologies are not the same.

In this paper, we attempt to propose an artifact for the benchmarking method of information security policy (BMISP), which can resolve the challenges discussed above. In order to overcome the first issue, we propose a universal artifact that indicates industry average of information security policy based on information security management system (ISMS) standards such as ISO 27001 and ISO 27004. The artifact consists of standardized information security measurements. Thus, organizations can communicate without disclosing details regarding their information security policy. Secondly, we employ design science methodology and activity theory in order to overcome the contextual challenge. The issue can be resolved if the artifact is capable of transferring knowledge from one circumstance in which it was produced to another situation (MacLean et al. 2002; Van Aken 2005). To do this, we employ activity theory as an overarching theory to develop the artifact. Activity theory

provides a theoretical framework to develop an artifact based on interaction activities between artifact, object, subject, instrument, community and rule. Following the guideline of activity theory, the knowledge that is acquired from various ISSP, government requirements and organizational traits can be standardized. In addition, we employed design science methodologies to validate the artifact.

To summarize, we followed design science research guidelines proposed by Hevner et al., Peffers et al., and Vijay et al. (Hevner et al. 2004; Peffers et al. 2007; Vaishnavi et al. 2008).

(1) Develop a visualized artifact that standardizes information security policies for benchmarking.
(2) Incorporate an activity theory approach that improves the management of information security policy and compliance.
(3) Carry out an artifact evaluation using a three-step approach:
    a. Initiate a request for comment (RFC) process
    b. Employ an empirical testing to show the value of the artifact
    c. Develop a prototype system and demonstrate it to information security analysis in an organizational level

In this paper, we illustrate the development of the BMISP. We include related literature, conceptual artifact, procedures to compose the measurements, and measurements validation process. In the remainder of this paper, we will first examine the existing literature on information security policy and activity theory. Next, we explore elements of BMISP such as measures, constructs and concept in international standards. We then present an example of an artifact based on the findings in literature and international standards. We conclude with the future study with further validation process of the BMISP and potential topics.

BACKGROUND AND THEORETICAL FRAMEWORK

The Principle of Information Security

Information security refers to the adoption of measures to prevent the unauthorized use, misuse, modification, or denial of use of information, knowledge, facts, data or

capabilities (Code ; Talbot et al. 2011; Whitman et al. 2013). In this sense, the purpose of information security protection is to identify the information that requires protection (Alberts et al. 2002), classify information assets according to their sensitivity, apply security management principles (Whitman 2003), and comply with relevant policies, law and legal requirements (Talbot et al. 2011; Whitman et al. 2013).

Talbot et al. (2011) and Whitman et al. (2013) proposed principles of information security. These principles are extended from CNSS (Committee on National Security System) model and McCumber (2004) cube to encompass the constantly changing information security environment. The Talbot et al. and Whitman et al. models used different terms to describe the same concepts with the exception of CIA (confidentiality, integrity, and availability), which is used in all models. We use terms from Whitman et al (2013) and compromise the definitions of terms with Talbot et al (Table 1).

Table 1 Principles of information security

Whitman et al. (2013)	Talbot et al. (2011)	McCumber (2004)	Definition
Confidentiality	Confidentiality	Confidentiality	The information asset is maintained in a secure manner by employing adequate privileges and controlled access.
Integrity	Integrity	Integrity	The quality or state of information asset being whole, complete and uncorrupted without altered interference.
Availability	Availability and Utility	Availability	The information asset will be available without interference or obstruction and in a useable format.
Privacy	Control and possession	-	No one other than authorized custodians or recipients can access all information asset or parts. The information asset should be used and stored according to the organization's intended will.
Identification, Authentication and Authorization (IAA)	Authenticity	-	The access to information asset should be under proof of data delivery (authentication), proper methods to confirm user's identity (identification), and granting proper authority to access, update or delete of the information asset.
Accountability	-	-	The accountability exists when a method controls assurance that information asset related activities are codified and traceable.

Activity Theory

The development of an artifact requires systematic approaches (Hevner et al. 2004; Purao et al. 2008). The systematic process may require a process of elicitation, depicter, and analysis. This involves determining the internal elements, structures, and relationships of the

artifact (Pressman 2005; Zowghi et al. 2005). In this paper, we employ activity theory to guide the requirements gathering process (Engeström 2000; Engeström et al. 1999). Activity theory provides a lens to comprehend and analyze social phenomena finding a pattern, and theorizes across interactions between groups of organizations, individuals and computers.

Activity theory argues that an individual produces an instrument when the individual interacts with the surrounding social environment. The instrument enhances social interaction by creating a transferring process that other people can access the instrument (Vygotsky 1980). In activity theory, the activity is considered a structure consisting of various sub-activities that are related to the core activities (Engeström et al. 1999). As explanations of the activity, the theory suggests six elements – object, subject, community, artifact, division of labor and rule.

(1) **Object** refers to a certain goal of the activity systems; the object is what the activity is directed at and can be considered the ultimate reason behind various behaviors of individuals, groups, or organizations (Kaptelinin 2005).

(2) **Subject** is the actor that is an active element of the activities. The actor can be either an individual or group (Kaptelinin et al. 1995).

(3) **Community** refers to all other actors that are involved in the activities (Engestrom 2000).

(4) **Instrument** refers to the tool used by the actors in the system that acts as a mediator of accumulation and transmission of social knowledge (Kaptelinin et al. 1995).

(5) **Division of labor** is the classification of activities among actors in the system (Kaptelinin 2005).

(6) **Rule** refers to conventions, social norms and guidelines that regulate the activities in the system (Engestrom 2000; Kaptelinin et al. 1995).

In this research, we employ a third-generation activity theory. The theory argues the use of multiple interacting activity systems to investigate complex social activities (Engeström 2014). The theory allows has an aggregated view of activity interactions not only for a single activity system but also for multiple activity systems, which depict overall interactions of the activity systems for a shared object (Engeström 2001).

Benchmarking of ISSP is a complex activity since the organization should consider various interactions between other organizations, standards, governmental regulations, and organizational structures. The principle component (e.g., subject) of benchmarking changes depending on the circumstances, and the implemented policies; the benchmarking process is influenced by social (e.g., community) and technical (e.g., instrumental)) factors whose relationships undergo environmental changes. By applying activity theory, we may investigate the interactions of benchmarking along the dimensions of subject, activity, instrument, community, rule, and division of labor in a systematic way. In our study, we capture all of these key-benchmarking elements in our artifact and standardize them to validate the relevancy of BMISP.

BMISP development

We sought to develop BMISP that standardizes the key principles of information security based on the guidance of international standards for ISMS. In this section, we apply the concepts introduced in the preceding section to facilitate the BMISP development process.

To define the scope of BMISP, we firstly establish a visual artifact named information security hexagon (ISH) that indicates degrees of information security based on the principles of information security. In ISH, the degree of each principle represents average degree that is measured by the organization's ISSP (Figure 1). Secondly, we visually extend the ISH with detail measurements (Figure 2).

Meta-model Development

We determine a meta-model for BMISP informed by activity theory and international standards. Table 2 exemplifies the definitions, implications of activity theory for BMISP, and BMISP measurement for three constructs. The concept of activity theory provides structural relationships between ISH and objectives of ISSP. The international standards, ISO 27000 series, provide a detail guidance to establish rigorous and reliable measurement constructs for BMISP. In figure 3, we demonstrate the meta-model of BMISP and example based on an illustration of activity theory.

Figure 1 Illustration of ISH

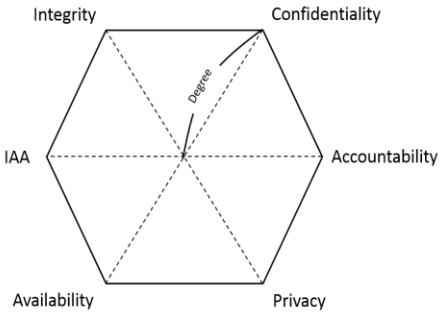
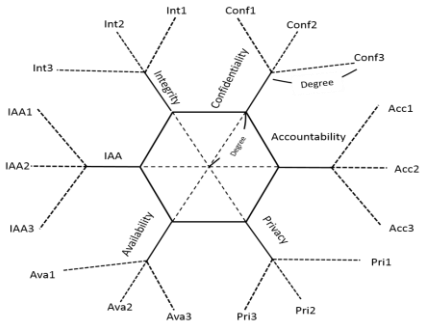
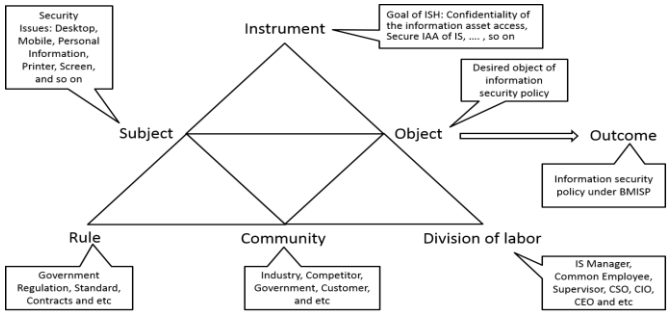


Figure 2 ISH with detail measurements



Employing the same approach and methodology of ISO 9000 series for quality assurance standards, ISO has assigned the 27000 numbering range for a series of information security standards for ISMS. The series consists of fifteen standards regarding vocabulary, requirements, controls, guidance, measurement, and risk management. In this research, we use components of ISMS control requirements and measurements that are depicted in ISO 27001 and ISO 27004. ISO 27001 depicts requirements for establishing, implementing, maintaining and continuity of ISMS. ISO 27004 provides guidance for development and use of measures for ISMS. In addition, we employ ISO 15939, which guides the quantitative research methodology for our measurements in BMISP.

Figure 3 Examples of BMISP and activity theory



BMISP Component Development

As the last step in the development of the BMISP, we propose components of BMISP based on aforementioned methodologies. We use the ISO 27001 naming convention for the BMISP components. However, we redefine the meaning of each component according to the purpose of this research. The components of the BMISP consist of three aspects: measurement and indicator specifications, recommended decision and interpretation, and stakeholders and responsibilities.

Table 2 Meta-model description of BMISP informed by activity theory

Activity theory concept		Description
Object	Definition in BMISP	Desired object of information security policy to mitigate and prevent incidents of information security.
	BMISP implication	The object provides general purpose of BMISP and its measurement constructs.
	ISO derived BMISP measurement construct	● Measurement construct identification [ISO 27004] ○ Measurement construct name ○ Purpose of measurement construct ○ Objective of control and process [ISO 27001] ● Object of measurement and attribute [ISO 27004] ○ Object of measurement ○ Attribute
Subject	Definition in BMISP	Incidents and issues that are related with information security. For instance, endpoints issues, security breaches, hacking, information leakage.
	BMISP implication	The subject that BMISP is applied.
	ISO derived BMISP measurement construct	● Measurement construct identification [ISO 27004] ○ Control and process [ISO 27001]
Community	Definition in BMISP	Relevant stakeholders who are related with information security concerns such as third-party, IS/IT developer community, partners, customers, government, and agencies.
	BMISP implication	BMISP should consider interactive incidents of information security between the stakeholders.
	ISO derived BMISP measurement construct	● Stakeholders [ISO 27004] ○ Client for measurement

Measurement and indicator specifications: The required measurements for determining the degree of ISH are defined below:

Measurement construction identification identifies the purpose of measurement construct, objective of control, and list of controls. The component explains the reasons of the measurement and specific objectives to achieve through the measurement. Based on the objectives, the component contains respective control and process under the measurement.

Object of measurement and attribute identify the entity that is characterized through the measurement and attribute. The attributes are property or characteristic of the object that can be quantified to measure. For instance, object of measurements can be information security policies, configurations of ISMS software, and organizational resources for information security.

Base and derived measure specification define measures in terms of an attribute and the method for quantifying it. Derived measure is defined as a function of two or more values of base measure.

Indicator specification provides the state or level of ISSP. Indicator specification also includes methods for visual presentation and algorithms to combine the measures.

Recommended decision and interpretation: Methodologies of decision criteria and interpretation of measurements are determined using the following components.

Decision criteria specification includes threshold, targets, or patterns that are used for determining the need for action, re-engineering, and further investigation.

Measurement result provides a general guidance based on the description of how the indicator and measurement should be interpreted. Reporting formats are included in this component. The measurement results may provide guidance to determine whether to increase or ease the restrictions of information security policy.

Stakeholders and responsibilities: Methodologies of communication and responsibilities of actors are determined using the following components. The actors can be internal or external to an organization. The relevant rule, policy, and government regulations are also specified.

Stakeholders specify internal management or other interested parties who are relevant to the ISSP. Reviewers, owners of information, data collectors and communicators are examples of the stakeholders.

Frequency and period determine periods of data collection and periodic revision rules of the organization for examining BMISP. The frequency and revision rules may differ by ISMS specifications and organization's interests.

CASE STUDY: BMISP FOR SYSSP OF EDRM

The following case study illustrates the above methodology. The case study includes detail components, explanations and examples of BMISP. We choose a system-specific security policy (SysSP) as a type of ISSP. Specifically we employ an enterprise digital right management (EDRM) policy. EDRM refers to the use of digital rights management (DRM) technology in the enterprise. EDRM includes various access control technologies for secure usage of information assets such as software, documents, data, hardware or content. EDRM is frequently employed to manage information assets in persistently protected way throughout the information asset's lifecycle (Morin et al. 2012). Enterprises have adopted EDRM to comply with relevant regulations and policies because EDRM enables the originator of the asset to establish rules of persistent controls and permissions (Jeon et al. 2015).

Data Collection

We use implemented SysSP data provided by an ISMS software integrator (Company X). We used SysSP from a total of seven programs: Secure Node (FSN), Secure Printer (FSP), ePrint (FEP), Secure Exchange (FSE), Mobile Gate (FMG), Secure Screen (FSS), and

Personal Identity Information Management (PIIM). FSN provides encryption and authority settings of all files and data that are saved on a PC. FSP and FEP trace and track printing activities. FSE controls and tracks data sharing processes with external users. FMG controls the usage of mobile devices for work. FSS protects sensitive information displayed on the computer screens. PIMM protects personal identifiable information using masking methods and encrypting technologies. We extract 69 tables and 223 attributes. Our prototype data set contains 978 data points.

Table 3 Summary of BMISP for confidentiality of EDRM SysSP policy

ISH Indi-cator	Derived measure	ISO 27001 Corres-pondence	Base measure (BM)
Confidentiality	Digital Information asset classification	A.8.2.1	BM1. Number of digital Information asset classifications BM2. Distance between classifications
	Application of general Information asset security policies	A.7.3.1	BM3. Expiration duration of Information asset encryption policy BM4. Expiration duration of print policy BM5. Expiration duration of information exchange policy BM6. Expiration duration of computer screen policy BM7. Type of default authority for Information asset exchange policy
	Automatic encryption	A.8.1.1 A.10.1.1	BM8. Number of automatic encryption file types BM9. Number of allowed macro programs

BMISP Application

To provide proof-of-concept of BMISP, we chose one section of the ISH, confidentiality (Table 4). To demonstrate application of BMISP, we focus on digital information asset classification. First, we extract a list of information asset classifications and types of authorized accounts for each classification. Subsequently, we draw staked charts that present different level of authorities by account types. The degree of digital information asset classification can be illustrated through the shape of charts. The convex shape of the charts shifts to the right side as the level of the classification decreases. The degree of BM1 and BM2 will increase as an organization has more number of classifications and less distance between the convex shapes.

Figure 1 Information asset classification and authority distribution

CONCLUSIONS

The study introduces a new approach in the development of information security policy benchmarking, leveraging systemic approaches based on third-generation activity theory. Activity theory and international standards are used to identify BMISP components. The utilization of activity theory proposes the conformance of BMISP to business goals and objectives of information security. The ISO 27000 series provides a general guidance to determine the components of BMISP in a rigorous manner.

Since this research paper is an analogy of methodology of BMISP, we did not include the actual testing portion and development of the prototype. These will be done based on the proposed BMISP structures by conducting RFC, implementation of the prototype, and an empirical case study. We will develop detailed data language based on markup language for visualization and communication of the BMISP. Subsequently, we will conduct an empirical testing using policy implementation logs from 300 companies.

REFERENCE

Alberts, C. J., and Dorofee, A. 2002. *Managing information security risks: the OCTAVE approach*, (Addison-Wesley Longman Publishing Co., Inc.

Berger, U. 2011. "CSI/FBI Computer Crime and Security Survey. 2011-2012," *CSI Computer Security Institute*).

Chai, S., Kim, M., and Rao, H. R. 2011. "Firms' information security investment decisions: Stock market evidence of investors' behavior," *Decision Support Systems* (50:4), pp 651-661.

Code, U. "USC § 3542 (b)(1)."

De Bruijn, W., Spruit, M. R., and Van Den Heuvel, M. 2010. "Identifying the Cost of Security," *Journal of Information Assurance and Security* (5:1).

Engeström, Y. 2000. "Activity theory as a framework for analyzing and redesigning work," *Ergonomics* (43:7), pp 960-974.

Engeström, Y. 2001. "Expansive learning at work: Toward an activity theoretical reconceptualization," *Journal of education and work* (14:1), pp 133-156.

Engeström, Y. 2014. *Learning by expanding*, (Cambridge University Press.

Engeström, Y., Miettinen, R., and Punamäki, R.-L. 1999. *Perspectives on activity theory*, (Cambridge University Press.

Gordon, L. A., and Loeb, M. P. 2002. "The economics of information security investment," *ACM Transactions on Information and System Security (TISSEC)* (5:4), pp 438-457.

Hausken, K. 2006. "Returns to information security investment: The effect of alternative information security breach functions on optimal investment and sensitivity to vulnerability," *Information Systems Frontiers* (8:5), pp 338-349.

Hevner, A. R., March, S. T., Park, J., and Ram, S. 2004. "Design science in information systems research," *MISQ.* (28:1), pp 75-105.

Hovav, Anat, and John D'Arcy. 2003. "The Impact of Denial‐of‐Service Attack Announcements on the Market Value of Firms." *Risk Management and Insurance Review* (6:2), pp 97-121.

Hovav, A. 2014. "Using scenarios to understand the frontiers of IS: Fifteen years later (a postscript)," *Information Systems Frontiers* (16:3), pp 347-352.

Hovav, A., and Gray, P. 2014. "The ripple effect of an information security breach event: a stakeholder analysis," *Communications of the Association for Information Systems* (34:50), pp 893-912.

Jeon, S., and Hovav, A. Year. "Empowerment or control: Reconsidering employee security policy compliance in terms of authorization," System Sciences (HICSS), 2015 48th Hawaii International Conference on, IEEE2015, pp. 3473-3482.

Kaptelinin, V. 2005. "The object of activity: Making sense of the sense-maker," *Mind, culture, and activity* (12:1), pp 4-18.

Kaptelinin, V., Kuutti, K., and Bannon, L. 1995. "Activity theory: Basic concepts and applications," in *Human-computer interaction*, Springer, pp. 189-201.

MacLean, D., MacIntosh, R., and Grant, S. 2002. "Mode 2 management research," *British Journal of Management* (13:3), pp 189-207.

McCumber, J. 2004. *Assessing and managing security risk in IT systems: A structured methodology*, (CRC Press.

Morin, J.-H., and Hovav, A. 2012. "Strategic value and drivers behind organizational adoption of enterprise DRM: The korean case," *Journal of Service Science Research* (4:1), pp 143-168.

Otim, S., Dow, K. E., Grover, V., and Wong, J. A. 2012. "The impact of information technology investments on downside risk of the firm: alternative measurement of the business value of IT," *Journal of Management Information Systems* (29:1), pp 159-194.

Peffers, K., Tuunanen, T., Rothenberger, M. A., and Chatterjee, S. 2007. "A design science research methodology for information systems research," *Journal of management information systems* (24:3), pp 45-77.

Pressman, R. S. 2005. *Software engineering: a practitioner's approach*, (Palgrave Macmillan.

Purao, S., Baldwin, C. Y., Hevner, A., Storey, V. C., Pries-Heje, J., Smith, B., and Zhu, Y. 2008. "The sciences of design: observations on an emerging field," *Harvard Business School Finance Working Paper*:09-056).

Talbot, J., and Jakeman, M. 2011. *Security risk management body of knowledge*, (John Wiley & Sons.

Vaishnavi, V., and Kuechler, W. 2008. *Design science research methods and patterns : innovating information and communication technology / Vijay K. Vaishnavi, William Kuechler Jr*, (Boca Raton : Auerbach Publications , c2008.

Van Aken, J. E. 2005. "Management research as a design science: Articulating the research products of mode 2 knowledge production in management," *British journal of management* (16:1), pp 19-36.

Vygotsky, L. S. 1980. *Mind in society: The development of higher psychological processes*, (Harvard university press.

Whitman, M., and Mattord, H. 2013. *Management of information security*, (Cengage Learning.

Whitman, M. E. 2003. "Enemy at the gate: threats to information security," *Communications of the ACM* (46:8), pp 91-95.

Whitman, M. E. 2008. "Security Policy," *POLICY, PROCESSES, AND PRACTICES*), p 123.

Zowghi, D., and Coulin, C. 2005. "Requirements elicitation: A survey of techniques, approaches, and tools," in *Engineering and managing software requirements*, Springer, pp. 19-46.