Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2005 Proceedings

Americas Conference on Information Systems (AMCIS)

2005

Making Sense of Information Systems Security Standards

Gurvirender Tejay
Virginia Commonwealth University, tejaygp@vcu.edu

Making Sense of Information Systems Security Standards

Gurvirender Tejay
Virginia Commonwealth University
tejaygp@vcu.edu

ABSTRACT

In the realm of information systems (IS) security, a plethora of standards have come into existence. Too many IS security standards have been proposed, which an organization could adopt to secure its information systems. On what criteria then an organization shall base its decision as to what standards need to be implemented? We address this concern employing basic economic concepts. The core argument of research presented in this paper is that an organization should incorporate a minimum set of standards to cover maximum IS security needs of an organization. The position of adopting a different IS security standard for every process in an organization defies the concept of efficiency.

Keywords

Economics, efficiency, IS security, standards.

INTRODUCTION

In today's interconnected world organizations are increasingly becoming dependent on information systems (IS). The security risks to IS have also steadily increased. As Dhillon (1997) argues, IS security can be viewed in terms of minimizing risks arising because of inconsistent and incoherent behavior with respect to the information handling activities of organizations. The implementation of IS security standards becomes important as it would allow us to minimize security risks facing an organization. However, a number of different standards for IS security have come into existence in recent years. On what criteria then an organization should base its decision as to what standards need to be implemented?

IS security is only as strong as the weakest link in the system. This statement might be misinterpreted by overzealous security enthusiasts to imply that an organization needs to adopt a wide variety of standards such that no link is left exposed to any weaknesses. However, it is also neither prudent nor economical for an organization to adopt all the existing standards of the industry in entirety. The position of adopting a different standard for every process in an organization defies the concept of efficiency. It makes more sense for an organization to give up, if required, few degrees of security so as not to implement an exhaustive set of standards. The argument of research presented in this paper is that an organization should incorporate a minimum set of standards to cover maximum IS security needs of an organization. Also, the implemented standards must be aligned with the business objectives.

The paper is organized into six sections. Following a brief introduction, section two outlines key standards for IS security. Section three presents the efficiency model of IS security standards. Section four addresses the challenges of institutionalizing standards. Finally, section five presents the conclusions.

IS SECURITY STANDARDS

IS security follows the ensuing 'life cycle': security evaluation, security development, risk management, and security management. In this section, we have organized key IS security standards along the four categories of IS security life cycle. In our view, each of these categories addresses a different aspect of IS security crucial to an organization. The concept of 'life cycle' captures the cyclical on-going nature of IS security in an organization.

Security Evaluation

Security evaluation is the examination and testing of the security features of an IS. The aim of security evaluation is to ensure that the system does not exhibit vulnerabilities and perceived security threat. The recommended standard for security evaluation is ISO/IEC IS15408. The roots of IS15408 could be traced back to Trusted Computer System Evaluation Criteria (TCSEC). TCSEC mainly addressed US military security needs and its focus was confidentiality.

Information Technology Security Evaluation Criteria (ITSEC) identifies Target of Evaluation (TOE) as either a system or product. TOE is evaluated in the context of operational requirements and the threats it would encounter. As such, the evaluation factors are correctness and effectiveness.

Canadian Trusted Computer Evaluation Criteria (CTCPEC) classifies the functionality and assurance requirements separately. The functional criteria comprises of confidentiality, integrity, availability, and accountability, while the assurance criteria are applied across the entire system.

Federal Criteria (FC) was influenced by Minimum Security Functional Requirements (MSFR), CTCPEC and ITSEC. MSFR follows CTCPEC in separating the functionality and assurance criteria. In FC, Protection Profile was introduced as an implementation-independent set of functionality and assurance requirements for a category of products.

Common Criteria (CC) is a product of joint effort between the organizations of TCSEC, ITSEC, CTCPEC, and FC. It was adopted as IS15408. CC introduces the general model and concepts of IT security evaluation. It then addresses the functional requirements of security. Finally, it provides the catalog of standardized Security Assurance Requirements. Package, Protection Profile, and Security Target are the security requirement constructs defined in CC.

Evaluation Criteria for IT Security (ECITS) followed CTCPEC in separating the functionality and assurance criteria. It was later published as IS15408. ECITS identifies four functional privacy families: anonymity, pseudonymity, unlinkability, and unobservability.

Security Development

ISO/IEC DIS21827, System Security Engineering Capability Maturity Model (SSE-CMM), is the recommended standard for security development. It is a process reference model to improve and assess security-engineering capability. The scope of SSE-CMM encompasses the entire secure system, the whole organization, and concurrent interactions with other organizations.

SSE-CMM model addresses the continuity, repeatability, efficiency, and assurance qualities required in the production and operation of secure systems and products. It separates the characteristics of security engineering process from its management characteristics. The domain dimension consists of “base practices” that collectively define security engineering. On the other hand, the capability dimension consists of “generic practices” that indicate process management and institutionalization capability.

Risk management

Risk management is the process to ensure the identification, analysis, control, and communication of IS security risks to which an organization is exposed. There is no internationally accepted standard for risk management yet. However, ISO/IEC TR13335, Guidelines for the Management of IT Security (GMITS), deals partly with risk management. GMITS outlines the principles of risk assessment and provides guidance on the selection of safeguards for the management of risk. Also, there are other risk management standards: NIST SP800-30 (US), MG-2 (Canada), BSI PD3002 (UK), and SAA/SNZ HB231 (Australia, New Zealand).

Security management

Security management outlines the objectives necessary for managing IS security. ISO/IEC 17799, Code of Practice for Information Security Management, is the recommended security management standard. It is a set of controls that are important to achieve the security objectives of an organization. Security policy, organizational security, personnel security, business continuity management, and compliance are the guiding areas in ISO/IEC 17799 for effective security management practice.

GMITS contains guidance on the management of IT security. It addresses subjects and techniques essential for security. This standard also identifies and analyzes the communication factors that are critical in establishing network security requirements.

Organization for Economic Cooperation and Development (OECD) guidelines recognizes the commonality of security requirements across various organizations and has developed an integrated approach. This approach is outlined as principles that are essential to IS security.

Generally Accepted Information Security Principles (GAISP) documents security principles that have been proven in practice and accepted by practitioners. Pervasive Principles outline high-level recommendations on effective IS Security strategy. Broad Functional Principles provide guidance for operational accomplishment of the Pervasive Principles. Detailed Principles specify how to implement optimal IS security practices.

In this section, we have described international standards for IS security. The standards discussed under the four categories overlap each other in terms of functionalities. As such, it would not be pragmatic for an organization to adopt all the standards as outlined. This would entail redundancy and wastage of valuable resources.

EFFICIENCY MODEL OF IS SECURITY STANDARDS

A free and competitive economy maximizes net benefits. That is, by being efficient an economy gets the best value for the least cost. An economy is said to be allocatively efficient when no additional mutually beneficial trades can be made between any two persons or groups (Wessels, 2000:422-424). According to Wessels, this occurs when marginal benefit equals marginal cost. If a firm doesn't produce efficiently it endures losses and eventually goes out of business.

We can extend the above efficiency concept to understand the current trend in IS security standards. The x-axis represents the number of prevalent standards. And, the degree of security of IS (assuming we are able to measure it by some metric) is represented on the y-axis. The producers are the organizations or institutions that have the responsibility to enact standards. A consumer would be a firm that needs to implement the standard to achieve a certain degree of security. The benefit will be the degree of security and cost is the number of standards implemented. The resulting model of efficiency for IS security standards is represented in figure 1.

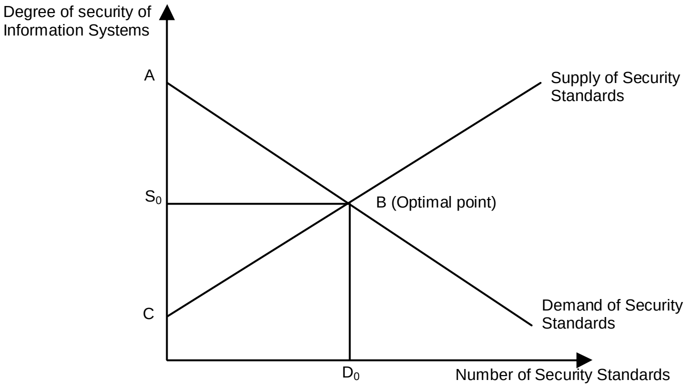

Figure 1 Efficiency Model of IS Security Standards

It can be seen that the laws of supply and demand hold for this representation. Interpreting the law of supply for security standards, the degree of security of IS increases when the number of standards implemented goes up and decreases when the number of standards goes down (figure 2). As the number of standards implemented increases, the process is carried out in a regulated manner to achieve optimal conditions of security. This leads to an increase in the overall degree of security. As per the law of demand, IS security standards would be in greater demand when the degree of security decreases (figure 3). The deterioration of security would impel the organizations to find appropriate solutions. This would lead to an increase in the demand for standards that would enable an organization to achieve the desired level of security.

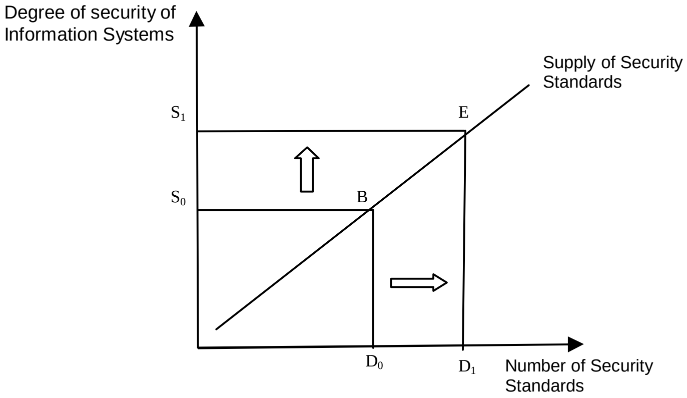

Figure 2 Supply Dynamics of IS Security Standards

The gain in net benefits can be measured by the total surplus, which is the area of the triangle ABC in figure 1. Total surplus comprises of consumer surplus (going to consumers) and producer surplus (going to producers). Here, the consumer surplus is the number of standards the firm might have had to implement in order to achieve a degree of security less the number of standards that it actually had to implement in the process to achieve the same degree of security. The producer surplus is the number of standards implemented less the marginal costs involved.

The model in figure 1 provides us with a point (B) at which an efficient number of standards can be implemented so as to achieve an efficient degree of security in an organization. Based on the efficiency model we can conclude that the desired degrees of security cannot be achieved by blindly implementing all the concerned existing standards of the industry. There is a certain trade off involved in terms of achieving certain degrees of security in lieu of number of standards to be implemented.

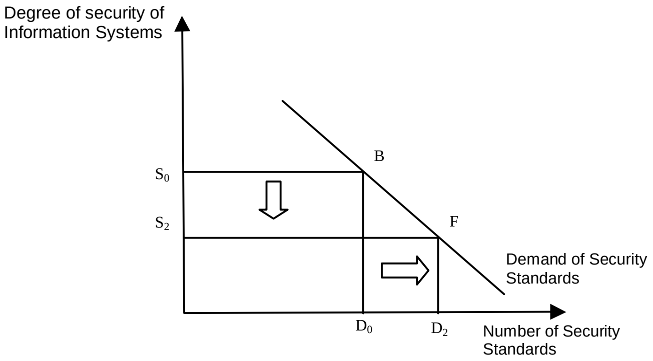

Figure 3 Demand Dynamics of IS Security Standards

CHALLENGES OF INSTITUTIONALIZING STANDARDS

Let us concentrate on the tradeoff involved in terms of degrees of security and number of standards to be implemented. According to the law of diminishing marginal utility, as people consume more units of a good in a given period (i) their total utility goes up, but (ii) each added unit of good adds less to their total utility, that is, the marginal utility of each added unit declines. The point to be careful about is that as more is consumed, total utility is going up but the addition of total utility is diminishing. The application of this principle to the problem at hand would imply that as degree of security increases the marginal utility of each added degree of security declines. That is, the total security is going up but each added degree of security after the point of efficiency adds less to the overall security.

As such, one has to give up certain degrees of security in order not to implement an exhaustive set of standards. This requires a careful analysis of risk that a firm might face and the level of security that might be needed to achieve the business goals.

At the other end, a careful selection of standards must be undertaken by a firm so as to attain the desired degree of security. In order to cover the maximum degree of security, a number of key standards can be integrated into a model.

The integrated model would be comprised of four categories, working coherently to cover maximum IS security needs of an organization. This model would strive to position itself at point B in figure 1. Such a model would be applicable to most organizations and in most environments. In this model, ISO/IEC IS15408, ISO/IEC DIS21827, ISO/IEC TR13335 and ISO/IEC 17799 should be adopted as the recommended standards. However, selecting standards based upon IS security risks should be the ultimate focus of an organization.

CONCLUSION

In a standardized world, it would seem that we should adopt and implement all the prevalent standards so as to perform organizational activities in an ideal fashion. However, it is neither prudent nor economical for an organization to adopt the existing standards of the industry in entirety. The position of adopting a different standard for every process in an organization defies the concept of efficiency. The aim of an organization is not to enhance standardization but to achieve its business objectives in an efficient manner. An organization should incorporate a set of IS security standards working coherently as an integrated model and aligned with its business objectives. Such a model would integrate a minimum set of standards to cover maximum IS security needs of an organization.

In this research, we have argued for a pragmatic approach towards IS security standards. We have extended the concept of efficiency and the law of diminishing marginal utility to standards. In terms of practical contribution, key IS security standards have been outlined that can be adopted by an organization as an integrated model.

REFERENCES

1. Common Criteria for IT Security Evaluation, Version2.1 (1999). National Institute of Standards and Technology & National Security Agency, USA.
2. Dhillon, G (1997). *Managing information system security*. London: Macmillan.
3. DOD5200.28-STD Trusted Computer System Evaluation Criteria. (1985). Department of Defense, USA.
4. Federal Criteria for Information Technology Security, Version1.0 (1992). National Institute of Standards and Technology & National Security Agency, USA.
5. Generally Accepted System Security Principles (GASSP), Version2.0 (1999). Information Systems Security Association.
6. ISO/IEC 17799 Information technology – Code of practice for information security management, First edition (2000). International Standards Organization (ISO).
7. ISO/IEC IS15408 Evaluation Criteria for IT Security (1999). International Standards Organization (ISO).
8. ISO/IEC TR13335 Guidelines for the Management of IT Security (GMITS), First edition (2000). International Standards Organization (ISO).
9. IT Security Evaluation Criteria, Version1.2 (1991). Office for Official Publications of the EC, European Commission.
10. MG-2 A Guide to Security Risk Management for IT Systems, Communications Security Establishment, Canada.
11. OECD Guidelines for the Security of Information Systems (1992). Organization for Economic Cooperation and Development.
12. PD3002 Guide to BS7799 Risk Assessment, British Standards Institution.
13. SAA/SNZ HB231 Information Security Risk Management Guidelines (2004). Standards New Zealand & Standards Australia.
14. SP800-30 Risk Management Guide for IT Systems (2002). National Institute of Standards and Technology, USA.
15. System Security Engineering Capability Maturity Model (2003). International Systems Security Engineering Association (ISSEA).
16. The Canadian Trusted Computer Product Evaluation Criteria (CTCPEC), Version3.0 (1993). Canadian System Security Centre.
17. Wessels, W.J. (2000). *Economics*. 3rd edition. New York: Barron's Educational Series.