Journal of Software Engineering and Applications, 2014, 7, 883-890
Published Online September 2014 in SciRes. http://www.scirp.org/journal/jsea
http://dx.doi.org/10.4236/jsea.2014.710079

The Challenge of Implementing Information Security Standards in Small and Medium e-Business Enterprises

Ja'far Alqatawna

King Abdulla II School of Information Technology, The University of Jordan, Amman, Jordan
Email: j.alqatawna@ju.edu.jo

Received 14 July 2014; revised 10 August 2014; accepted 5 September 2014

Abstract

The dynamic nature of online systems requires companies to be proactive with thwarting information security threats, and to follow a systematic way for managing and evaluating the security of their online services. The existence of security standards is an important factor that helps organisations to evaluate and manage security by providing guidelines and best practices that enable them to follow a standard and systematic way to protect their e-Business activities. However, the suitability of available information security standards for Small and Medium e-Business Enterprises (e-SME) is worth further investigation. In this paper three major security standards including Common Criteria, System Security Engineering-Capability and Maturity Model and ISO/IEC 27001 were analysed. Accordingly, several challenges associated with these standards that may render them difficult to be implemented in e-SME have been identified.

Keywords

Information Security Standards, e-Business, Small and Medium Enterprises

1. Introduction

Diffusion of Information and Communication Technology (ICT) has its impact on many of our daily activities. New channels for communication, selling, buying, and learning have been developed based on the new innovations of ICTs. A huge part of business activities has become dependent on ICTs. Businesses have become more electronic than any time before. New online business concepts, models and modes have been invented.

One aspect of this technological diffusion is the adoption of Electronic Business (e-Business). It refers to the use of information and communication technology for various business activities. e-Business is utilizing Web

How to cite this paper: Alqatawna, J. (2014) The Challenge of Implementing Information Security Standards in Small and Medium e-Business Enterprises. *Journal of Software Engineering and Applications*, **7**, 883-890.
http://dx.doi.org/10.4236/jsea.2014.710079

and communications technologies to enhance customer service, simplify business processes, increase revenue and reduce costs. The Internet and the Web technologies provide the building block of e-Business [1]. IBM defines e-Business as "*a business process transformed to leverage WWW* (*Internet*, *intranet*, *and extranet*) *technology for business benefit*. *It is about using the Internet infrastructure and related technologies to enable business anywhere and anytime*" [2].

Adoption of e-Business in the developing world that represents large part of the marketplace is insufficient. Many challenges and issues are facing the use and development of e-Businesses in this part of the world; these include poor or lack of infrastructure, social problems and the lack of an appropriate legal, political and economic framework [3] [4].

According to [5] Small and Medium Enterprises (SME) play an important role in the economics of the developing countries and they are in a better situation to get the benefits of e-Business because:

- SMEs count for 60% - 70% of all employment in developing countries.
- SMEs adapt to the new technology faster than larger companies (less bureaucracy and stricter staffing hierarchies).

The ability of SMEs to securely use and utilize ICT in their businesses is an important prerequisite for successful e-Business. However, many studies showed that security is a significant barrier for the adoption of e-Business [6]-[8]. For instance, Wymer *et al*. [8] conducted a study in which 26 factors were collected from the literature. Thirty different studies related to factors (either barriers or incentives) that influence e-Business adoption in SMEs were reviewed. Based on this review these factors were categorized in to four groups: *Environmental factors*, *Knowledge factors*, *Organisation factors and Technological factors*. Security was regarded as an important issue and included with the technological factors.

The dynamic nature of online information systems requires companies to be proactive with thwarting information security threats, and to follow a systematic way for managing and evaluating the security of their online services. The existence of security standards is an important factor that helps organisations to evaluate and manage security by providing guidelines and best practices that enable them to follow a standard and systematic way to secure their online business activities.

This paper aims to review the available security standard and evaluate their suitability for SMEs in developing countries. In Section 2, an overview of available security standards is provided. In Section 3, two technical security standards (Common Criteria and Systems Security Engineering-Capability Maturity Model) will be discussed. In Section 4, one security management standard (ISO 27001 standard for Information Security Management System) will be discussed. Finally a critical evaluation for the selected standards is presented in Section 5.

2. Overview of Security Evaluation Standards

Many national and international efforts have been devoted to develop frameworks for evaluation and managing the security of computerized systems. An early effort was in the 1970s when the US Department of Defense funded the Trusted Computer System Evaluation Criteria which is commonly known as the "Orange Book". After that, other countries such as Canada, Germany and UK presented similar evaluation criterion such as:

- ITSEC—Information Technology Security Evaluation Criteria developed by France, Germany, the Netherlands, and the UK in the early of 1990s.
- CTCPEC—Canadian Trusted Computer Product Evaluation Criteria in 1993.

Based on all these efforts the Common Criteria (CC) was developed as an international standard for security evaluation of IT products and systems [9].

The primary focus of many of these standards is on technical aspects such as information technologies and networks. For instance, the Common Criteria can be used by organisations to evaluate the security of their IT produces through a rigid technical evaluation process. This evaluation process is conducted by a team of security technical experts known as "testing laboratory" to ensure that particular software is satisfying the predefined security requirements [9]. Other security technical standards focus on issues such as cryptography techniques, digital signature and key management [10].

However, other aspects such as individual, organisational and managerial issues have become very significant for information security [11]. Some researchers argue that security has moved away from its technical perspective and has other factors which must be considered to build secure IT environments [12]. This new way of looking to the security problem is based on the idea that business information and communication systems have interconnecting and interacting components including people, software, hardware, procedures and data, and should be looked upon as information systems, including a technological infrastructure and organisational framework, rather than a pure technological infrastructure [13]. Consequently, several standards have been developed based on the fact that security should be enforced from the top level management in organisations. For instance, ISO/IEC 27001:2005 standard [14] was developed particularly for information security management.

A possible way for categorizing security standards, models and guidelines that help in evaluating and managing information security could be as follow [15]:

- **Technical Security Evaluation standards:** Focus on the technical requirements for designing and implanting secure systems and IT products.
- **Security Management approaches:** Focus on security activities within organisation as business process and emphasis management participation.

3. Technical Security Evaluation Standards

Organisations need to ensure information and communication systems security. One way for doing this, is by specifying security functional requirements and conditions that should be satisfied by Information Technology (IT) related products and systems used within organisations. Company may purchase products that meet its security requirements or develop its own systems following the specified security requirements. In both cases, the existence of a security standard to evaluate IT related products and systems, is very essential. These standards can be used for evaluating end product or the software development process and include:

- IT Products and Systems Security Evaluation Standards (e.g.: Common Criteria): specify security functional and assurance requirements for secure systems.
- Secure Software Engineering Standards (e.g.: SSE-CMM): specify the security engineering activities that need to be integrated with the IT systems lifecycle.

Well-known examples of this group are the Common Criteria (CC) and the System Security Engineering-Capability and Maturity Model (SSE-CMM). These are discussed in the following subsections.

3.1. Common Criteria

The Common Criteria (CC) is a security standard enables organisations to evaluate security of products and systems. It is a result of international efforts to create security evaluation criteria which increases the confidence in the IT products that widely used in the international community. The CC is based on the US's TCSEC (*The Orange book*), The Canadian's CTCPEC, and European ITSEC. Version 1.0 of the CC has been released in 1996, and then version 2.0 in 1998 which later has been adopted as ISO standard ISO/IEC 15408 [9] (**Figure 1**).

The CC provides Security Functional Requirements and Evaluation Assurance Levels as common framework that allows comparability between clients and vendors independent security evaluations. A client/user can define his security requirements using Protection Profile (PP) which is an implementation-independent set of security requirements for a category of products/systems that meet the client's needs. A vendor or developer can claim that his product meets the security requirements and he should provide Security Target (ST) document which support the evaluation or the product against the PP. The IT product/system which is subject to the evaluation is called Target of Evaluation (TOE).

The evaluation process does not say that the system is secure or not, however it provides assurance levels and gives the confidence that security specification, implementation and evaluation of the product have been done in a standard way [9].

Products under the CC can be certified at different Evaluation Assurance Levels (EAL):

- ➢ EAL1—functionally tested.
- ➢ EAL2—structurally tested.
- ➢ EAL3—methodically tested and checked.
- ➢ EAL4—methodically design, tested and reviewed.
- ➢ EAL5—semiformally design and tested.
- ➢ EAL6—semiformally verified design and tested.
- ➢ EAL7—formally verified design and tested.

EALs provide increasing scale which balance between the level of evolution, cost and feasibility. EAL1 is the

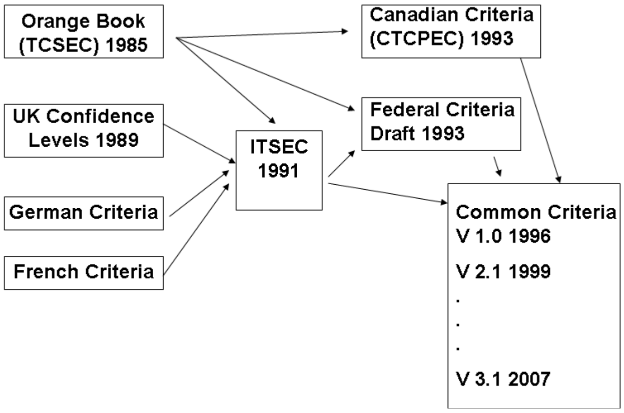


Figure 1. The development of common criteria.

lowest evaluation level and the less expensive. EAL7 is the highest and most complex and expensive level. Being certified at a higher level does not mean that a system is more secure, but it has been more rigorously evaluated [9].

3.2. Systems Security Engineering-Capability Maturity Model (SSE-CMM)

Systems Security Engineering-Capability Maturity Model (SSE-CMM) is an international standard (ISO/IEC 21827) which has been developed by the International Systems Security Engineering Association (ISSEA). According to SSE-CMM.org:

"*The SSE-CMM® is a process reference model. It is focussed upon the requirements for implementing security in a system or series of related systems that are the Information Technology Security* (*ITS*) *domain… Within the ITS domain the SSE-CMM® Model is focussed on the processes used to achieve ITS*, *most specifically on the maturity of those processes*" [16].

SSE-CMM addresses the security engineering activities that should exist in the IT system's lifecycle. It focuses on the security processes in the complete software development lifecycle which includes: concept definition, requirements analysis, design, development, integration, installation, operation and maintenance.

SSE-CMM is intended to be used by security developers, security integrators as well as organisations that provide security service. Furthermore, the framework has been developed to be applicable for all types and sizes of security engineering organisations; commercial, government as well as academic.

The standard uses the term "Security Engineering Organisation" which is applicable to different types of organisations. Such Security organisations may include: developers, product vendors, integrators, acquirers (acquisition organisation or end user), security evaluation organisations (system certifier, product evaluator, or operation accreditor), and trusted third parties (certification authority). The standard allows the security engineering organisation to measure its security process maturity based on the following capability maturity levels:

- ➢ Capability Level 1—Performed Informally.
- ➢ Capability Level 2—Planned and Tracked.
- ➢ Capability Level 3—Well Defined.
- ➢ Capability Level 4—Quantitatively Controlled.
- ➢ Capability Level 5—Continuously Improving.

The SSE-CMM's basic model has two dimensions:

1) The Domain dimension: includes all the security practices that define security engineering. These practices refer to as "Base Practices".

2) The Capability dimension: includes practices that are applied across wide range of domains. They are called "Generic Practices" and should be performed as a part of the base practices.

SSE-CMM can be used as a tool that allows the interested party to evaluate the maturity of their security engineering practices and improve them. The use of the standard provides the evaluators or the security certifiers with inputs that allow them establish confidence and assurance levels. Additionally, it provides customers with standard method for evaluating vendors' security engineering capability [16].

4. Security Management Approaches

The previous security standards focus on the technological aspects of information security. The primary players in the scope of these standards are security professional and experts. These standards do not incorporate other factors such as management, cultural and legal factors that affect organisation's information security.

Another approach for ensuring information security in organisations is the one which is based on applying management practices in order to achieve more comprehensive approach for information security. Common examples of this category are [17]:

- Security Managements Standards (e.g.: ISO/IEC 27001).
- Security Management Best Practices (e.g.: NIST security publications).
- Information Security Guidelines (e.g.: OECD Security Guidelines).

ISO/IEC 27001 Information Security Management System Standard is selected as an example on this approach as it is widely used by many organisations to manage security. The standard is discussed in the following section.

4.1. ISO/IEC 27001 Information Security Management System Standard

ISO/IEC 27001 is a well-known standard for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS). It has been developed by the joint technical committee of ISO (the International Organisation for Standardization) and IEC (the International Electrotechnical Commission) [14]. This standard is based on BS7799 standard which has been developed by the British Standards Institute (BSI).

ISO/IEC 27001 defines the requirements for successful ISMS. Compliance with the standard means, that organisation is following a standard approach for establishing, implementing and maintaining its ISMS. The standards does not provide specific process on how organisation can manage its ISMS, instead it is defines what are the requirements of ISMS. For this reason, the standards is provided with ISO/IEC 17799:2005 Code of practice for information security management as guideline that describes and clarifies how ISMS can be initiated, implemented, maintained, and improve based on ISO/IEC [14].

The standard adopts a process approach which includes essential processes for ISMS. These processes define the requirements for:

1) Establishing ISMS.
2) Implanting and operate the ISMS.
3) Monitor and review the ISMS.
4) Maintain and improve the ISMS.

The process approach can be simply defined as input-process-output model. However, it is more complicated in the case of the ISMS. Each ISMS process's output form input to another process. It allows organisation to gather information security requirements and expectations from different interested parties and manage the resources that are needed to process these requirements. The security requirements form input to the ISMS processes that create output which satisfies the expectations and fulfil the requirements.

The previous processes (1 - 4) are structured and integrated with each other based on the PLAN-DO-CHECK-ACT (PDCA) model (**Figure 2**).

The standard defines eleven security control areas and defines their objectives:

1) Information security policy.
2) Organisation of information security.
3) Asset management.
4) Human resource security.
5) Physical and environmental security.
6) Communications and operations management.
7) Access control.
8) Information systems acquisition, development and maintenance.
9) Information security incident management.
10) Business continuity.
11) Compliance.

It is very clear that the standard is covering wide range of areas that affect organisation security. The standard

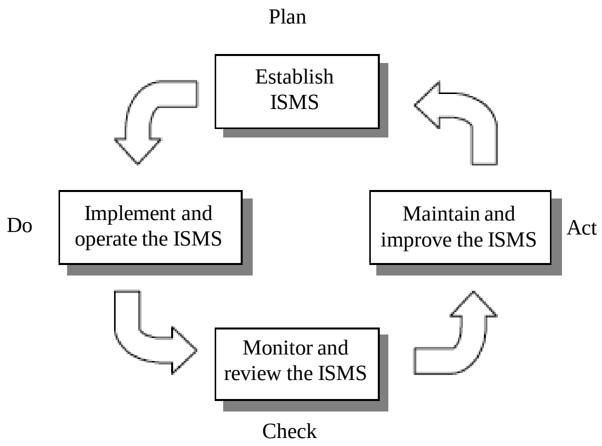

Plan
Establish ISMS
Do
Implement and operate the ISMS
Maintain and improve the ISMS
Act
Monitor and review the ISMS
Check

Figure 2. PDCA model of ISO/IEC 27001 standard [14].

is heavily based on risk assessment. Each of the previous control area contains a number of controls that are defined by the standards as "means of managing risk, including policies, procedures, guidelines, practices or organisational structures, which can be of administrative, technical, management or legal nature" [14]. An organisation is free to choose or discard any of these controls given that a sufficient justification for the choice is given.

5. Evaluation and Discussion

As discussed previously, security standards helporganisations to evaluate and manage security by providing guidelines and best practices that enable them to follow a standard and systematic way to secure their e-Business activities. However, there are several challenges associated with these standards that may render them difficult to be implemented in SME especially in developing countries. In this section the challenges associated with each one of the security standards presented above will be discussed.

5.1. The Challenges of Using Common Criteria

Unfortunately, The CC is the only available international standard for evaluating the security of IT products and systems, and there are many criticisms and objections against the standard. Some of the claimed objections against the CC are [18]:

- Evaluation IT products using CC is very costly: as the assurance level increases so the cost increases, however, this does not necessarily imply greater security.
- Burdensome: great effort is required to prepare the evolution evidences and related documents. This means time and resources consuming.
- Focuses more on documentation rather than on testing the product itself especially from EAL1-EAL4 where most products are evaluated.

The evaluation process of Common Criteria requires a long period of time. The dynamic nature of e-Business requires small and midsize businesses to be dynamic and to react very quickly to such environment. e-Business technologies are changing sometimes in less than six months leaving no time for companies to spend in preparing the CC's protection profile, waiting for vendors to prepare their target of evaluation and then asking a testing laboratory for accrediting the product in question. As a result, the overall process is time consuming.

Moreover, many SMEs, especially in the developing countries are suffering from the lack of budget and resources for implementing or acquiring IT solutions. Hence, CC is considered a very expensive standard for such organisations.

The lack of IT technical skills, particularly in the field of security, increases the burden of using the CC in SMEs. Even some security experts complain that CC is complex and cumbersome.

In additional to these obstacles that prevent SMEs from using the CC, CC only provides a framework for evaluating the security of IT products that the SMEs want to use, without providing comprehensive approach for deploying and managing IT products in a secure way.

5.2. The Challenges of Using Systems Security Engineering-Capability Maturity Model

It has been argued that the SSE-CMM is limited to security engineering and software design [19]. The main goal of the SSE-CMM is to measure the level of maturity of the Systems Security Engineering processes implemented by the organisation [20]. As discussed before, the primary stakeholder of the SSE-CMM is the Security Engineering Organisations that may include system security developers, security evaluators, security integrators or even customers who want to evaluate the maturity of security vendors and providers. The standard is not intended for e-Business as much as it is intended for security engineering organisation.

The primary objective of the standards is to define security engineering as a defined, mature and measurable discipline. Thus, it will allow the interested parties to have a method to evaluate and select security engineering provider based on capability-based assurance [16]. However, the standard defines fundamental security engineering activities and allow organisation to improve these process over time. Also it does not define specific processes, instead it gives guidelines that are applied regardless the processes that are performed. Thus, a modified version of the standard that integrates the e-Business processes with security engineering activities might be a possible way for evaluating the maturity of security practices in e-Business organisations.

5.3. The Challenge of Using ISO/IEC 27001

ISO/IEC 27001 gives organisations that are looking for securing their business a flexibility to develop their own information security management system (ISMS). This is because the standard does not specify any particular approach or method for developing ISMS. Instead, it defines requirements for ISMS. This gives organisations more freedom to choose their preferred risk management methodology for example. On the other side, this may create burden for some organisations that lack security knowledge and do not have competency for developing their ISMS.

Zuccato [17] claimed that security management approaches that depend only on risk analysis, such as ISO 27001, are not convenient for e-Business, since they only depend on the value of asset, threats, and the probability of exploiting vulnerabilities by the threats. However, this is not completely true. Risk analysis may consider other sources for eliciting security requirements and threats. For instance, company reputation can be considered as asset to be protected, involving customers in the risk analysis and considering market forces.

Furthermore, the standard is intended to all size of organisations [14]. From a practical rather than financial point of view, it might be more convenient and easy for SMEs to adopt this standard. In a small company, it is easier to manage ISMS, since you have a small number of assets to be considered. However, cost and lack of awareness of the standard contents act as a main barrier for adopting the standard [21].

6. Conclusions

This study has identified several challenges associated with several available information security standards including Common Criteria, System Security Engineering-Capability and Maturity Model and ISO/IEC 27001. The identified challenges represent barrier which may prevent e-SMEs from implementing a proper security approach to protecting their information and online services. While Common Criteria can be very helpful for evaluating the security of IT products, the author emphasised that the evaluation process of such method requires a long period of time. The dynamic nature of e-Business leaves no time for companies to spend in preparing the CC's protection profile, waiting for vendors to prepare their target of evaluation and then asking a testing laboratory for accrediting the product in question. Thus, the overall process of the CC is time consuming, costly and burdensome. With respect of SSE-CMM, the study found that it does not define specific processes, instead it gives guidelines that are applied regardless of the processes that are performed. Accordingly, it can be suggested that a modified version of the standard that integrates the e-Business processes with security engineering activities might be a possible way for evaluating the maturity of security practices in e-Business organizations. The last standard evaluated in this study was ISO/IEC 27001. This standard gives organisations freedom to develop their own information security management system (ISMS) as it does not specify any particular approach or method for developing ISMS. However, this may create burden for some organisations that lack security knowledge and do not have a competency for developing their ISMS.

It can be argued that security is a socio-technical problem and needs to be studied in relation to its environments considering all the factors that may affect security [22]. Security problem is a multi-disciplinary one and requires a holistic approach which covers managerial as well as technical aspects of the problem [23]-[25].

References

[1] Awad, E.M. (2004) Electronic Commerce: From Vision to Fulfilment. 2nd Edition, Prentice Hall, Upper Saddle River.

[2] Smith, B., Chatfield, V. and Uemura, O. (2001) IBM RedBooks, iSeries e-Business Handbook, A Technology and Product Reference.

[3] Bakari, J. (2007) A Holistic Approach for Managing ICT Security in Non-Commercial Organisations. A Case Study in a Developing Country. PhD Thesis, Department of Computer and Systems Sciences, SU/KTH Sweden.

[4] Jennex, M. and Amoroso, D. (2004) e-Business and Technology Issues for Developing Economies: A Ukraine Case Study. *The Electronic Journal on Information Systems in Developing Countries*.

[5] Payne, J. (2007) e-Commerce Readiness for SMEs in Developing Countries: A Guide for Development Professionals. Academy for Educational Development/LearnLink.

[6] Hartono, E., Holsapple, C., Kim, K., Na, K. and Simpson, J. (2014) Measuring Perceived Security in B2C Electronic Commerce Website Usage: A Respecification and Validation. *Decision Support Systems*, **62**, 11-21. http://dx.doi.org/10.1016/j.dss.2014.02.006

[7] Iglesias-Pradas, S., Pascual-Miguel, F., Hernández-García, A. and Chaparro-Peláez, G. (2013) Barriers and Drivers for Non-Shoppers in B2C e-Commerce: A Latent Class Exploratory Analysis. *Computers in Human Behavior*, **29**, 314-322.

[8] Wymer, S. and Regan, E., (2005), Factors Influencing e-Commerce Adoption and Use by Small and Medium Businesses. *Electronic Markets*, **15**, 438-453. http://dx.doi.org/10.1080/10196780500303151

[9] (2007) Common Criteria: An Introduction. http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R4.pdf

[10] ISO Security Standards. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=45306

[11] Kajava, J., Anttila, J., Varonen, R., Sovola, R. and Roning, J. (2006) Information Security Standards and Global Business. *IEEE International Conference on Industrial Technology*, Mumbai, 15-17 December 2006, 2091-2095.

[12] Solms, B. (2001) Information Security: A Multidimensional Discipline. *Computers & Security*, **20**, 504-508. http://dx.doi.org/10.1016/S0167-4048(01)00608-3

[13] Katsikas, S.K., Lopez, J. and Pernul, G. (2005) Trust, Privacy and Security in e-Business: Requirements and Solutions. *Proceedings of the* 10*th Panhellenic Conference on Informatics* (*PCI*'2005), Volos, 11-13 November 2005, 548-558.

[14] ISO/IEC 27001:2005 Information Technology, Security Techniques, Information Security Management Systems, Requirements. http://www.iso.org/iso/catalogue_detail?csnumber=42103

[15] Solms, R. (1996) Information Security Management: The Second Generation. *Computers & Security*, **15**, 281-288. http://dx.doi.org/10.1016/0167-4048(96)88939-5

[16] (2003) Systems Security Engineering Capability Maturity Model®, SSE-CMM®, Model Description Document, Version 3.0.

[17] Zuccato, A. (2006) Holistic Security Management Framework Applied in Electronic Commerce. *Computers & Security*, **26**, 256-265.

[18] Jackson, W. (2007) Under Attack: Common Criteria Has Loads of Critics, But Is It Getting a Bum Rap? Government Computing News.

[19] Davis, A. and Steven, A. (2005) How Security Can Be Measured, Copyright© 2005 Information Systems Audit and Control Association. http://www.isaca.org/

[20] Hopkinson, J. (1999) The Relationship between the SEE-CMM and IT Security Guidance Documentation. Copyright EWA-Canada Ltd., Ottawa. https://www.cccure.org/Documents/OCSIG/hopkinson1.doc

[21] DTI Information Security Breaches Survey (2006) Technical Report. UK Department of Trade and Industry.

[22] Alqatawna, J., Siddiqi, J., Akhgar, B. and Btoush, M.H. (2009) e-Business Security: Methodological Considerations. *International Journal of Business*, *Economics*, *Finance and Management Sciences*, **1**, 47-54.

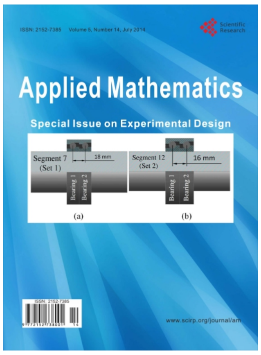
[23] Alqatawna, J., Siddiqi, J., Akhgar, B. and Btoush, M. (2008) Towards Holistic Approaches to Secure e-Business: A Critical Review. *Proceedings of EEE*'08, 14-17 July 2008, Las Vegas, 245-251.

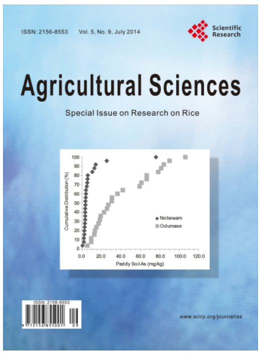
[24] Alqatawna, J., Siddiqi, J., Akhgar, B. and Btoush, M. (2008) A Holistic Framework for Secure e-Business. *Proceedings of EEE*'08, 14-17 July 2008, Las Vegas, 257-263.

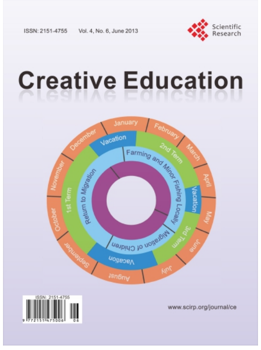
[25] Alqatawna, J. (2010) Multi-Stakeholder Enquiry for Securing e-Business Environments: A Socio-Technical Security Framework. Sheffield Hallam University, Sheffield.

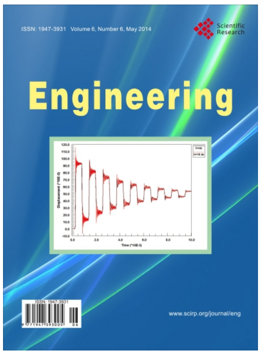
Scientific Research Publishing (SCIRP) is one of the largest Open Access journal publishers. It is currently publishing more than 200 open access, online, peer-reviewed journals covering a wide range of academic disciplines. SCIRP serves the worldwide academic communities and contributes to the progress and application of science with its publication.

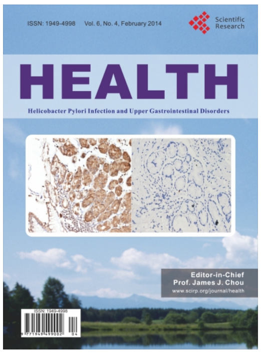
Other selected journals from SCIRP are listed as below. Submit your manuscript to us via either submit@scirp.org or Online Submission Portal.










HEALTH
Helicobacter Pylori Infection and Upper Gastrointestinal Disorders
Editor-in-Chief
Prof. James J. Chou

Journal of Cancer Therapy
Special Issue on Bone Tumor Research