Security Assurance Through Strategic Information Systems Planning

Abdisalam Issa-Salwe, Khurram Mustafa

Abstract*—. Strategic Information Systems Planning (SISP) and pertinent Information Security Policy (ISP) in organisations are largely inevitable in the contemporary business systems. Embedding information security policy within the organisation's strategic information system planning is essential for the effectiveness of using information systems in modern systems in a secure environment. A survey of relevant literature on SISP and ISP in organisations' processes reveals a close relationship between them and draws attention to how contradictions within this relationship may threaten as well. We explore the importance of embedding the ISP process within the SISP, and how these two issues are vital to organisations. It is further established the inevitable complementary role of these to ensure the effectiveness of contemporary information systems. The strategic planning information system makes certain that new systems are deployed in a way that maintains the strategic objectives of an organisation while the security policy provides a framework for verifying that systems are shaped and managed in a secure manner. Embedding ISP in SISP appears to increase progressively the security capability of an organisation, and hence, the deliverables from the SISP process may be more effective, efficient and hencefsystems came with huge complexities beneficial to the organisation. Although organisations may face security glitches throughout the application and operational phase, they must try hard such an inevitable embedding to avoid certain catastrophic risks, assure business continuity and enhance overall productivity. Finally, a cyber sensitive audit and control based ISP Components-based framework is proposed for embedding ISP into SISP, right from instantiation..

Index Terms*— Strategic Information Systems Strategy, Information Systems (IS), Information Technology (IT), Information Security Policy, Contemporary Business, Security Risk, Business Continuity Planning (BCP).

I. INTRODUCTION

Strategic information systems planning (SISP) and strategic information security are two of the most important characteristics in information systems world. A compressive Strategic Information Systems Planning (SISP) puts in place to assure that the information security is installed in a method that coincides with an organisation's strategic goals. Moreover, Information Security Policy (ISP) provides a structured control to guarantee that systems are developed, operated and maintained in an utmost secure manner. Despite the awareness and sensitivity, SISP is still a rare initiative in the majority of organisations and more so on ISP embedding. Undoubtedly, such an absence may jeopardise the organisational security, and may incur needless efforts costing highly at large.

Recently, there has been a growing awareness within organisations the importance of integrating information security with the organisation's SISP. However, some managers take these two operations separately, therefore jeopardising organisational security and incurring needless efforts at a later point [20]. One of the main goals of SISP is to establish the organisational IS and assure it in the most effective as well as efficient manner, leading overall value added of significance. An SISP makes it easier for organisations to identify their portfolio of computer-based applications, which in turn is used to line up business strategy and create competitive advantages. Therefore, SISP implementation has to be a continuous activity to allow organisations to get precedence for information systems development [8, 25] and assure the organisation's competitive position.

As system's planning is an effectual means to grow and maintain systems as a whole, this paper aims to establish and emphasise the contribution of SISP to information systems protection by embedding the same ISP within an organisational setting. It also explores the contribution of SISP to ISP within an organisational context, BCP and optimisation of overall productivity. The rest of the paper is organised as follows: Section 2 explores the perceptions on SISP; Section 3 describes the aspects of the ISP; Section 4 describes and establishes the requisite linkages between SISP and ISP for an organisation, with a case study; and Section 5 includes a contextual discussion and concludes with prospective findings..

II. STRATEGIC INFORMATION SYSTEMS PLANNING

The advances in IS/IT have had enormous effects on our day-to-day lives. As technology evolves immensely, the opportunities for organisations to attain competitive advantage changes as well. To do an IS/IT based systems, it is important to maintain an appropriate system that defines organisational systems and provides a means to handle them [2, 12]. SISP starts with the identification of the organisation's strategic information needs. King and Teo [14] view the strategic plan as capability architecture, i.e. a flexible and continuously improving the infrastructure of organisational capabilities. It also means to serve as the primary foundation for a company's sustainable competitive advantage [8, 14]. They emphasise the need for continuously updating and improving the strategic capability architecture. Although the main objective of SISP is generally interpreted in terms of the identification of new applications, Beynon-Davies [5] suggests that SISP can be used to arrive up

Revised Version Manuscript Received on May 18, 2016.

Dr Abdisalam Issa-Salwe, Department of Information Systems College of Computer Science and Engineering, Taibah University, Madinah, Saudi Arabia.

Prof Khurram Mustafa, Department of Information Systems, College of Computer Science and Engineering, Taibah University, Madinah, Saudi Arabia.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

to a wider scope of issues, thereby enabling the realisation of a portfolio of systems and related engineering science projects [8, 19], including the following:MATH

If you are using *Word,* use either the Microsoft Equation Editor or the *MathType* add-on (http://www.mathtype.com) for equations in your paper (Insert | Object | Create New | Microsoft Equation *or* MathType Equation). “Float over text” should *not* be selected.

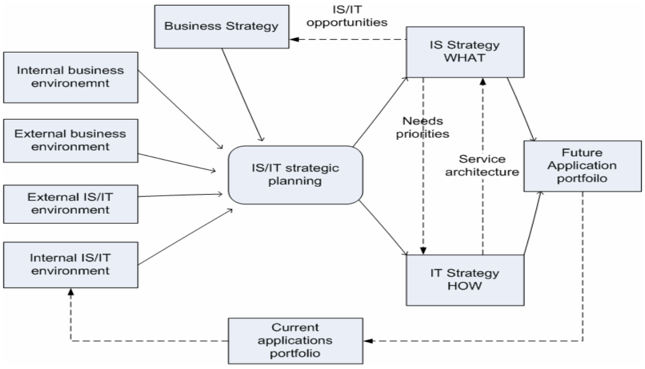
Business Strategy
IS/IT opportunities
IS Strategy WHAT
Internal business environemnt
External business environment
External IS/IT environment
Internal IS/IT environment
IS/IT strategic planning
Needs priorities
Service architecture
Future Application portfolio
IT Strategy HOW
Current applications portfolio

Figure 1: Inputs and Outputs of IS/IT strategy. Ankit Bhatnagar, 2006 [6]

- Corrections to existing information systems;
- Enhancements of existing information systems;
- New major information systems development projects; and/or
- New major infrastructure systems or technologies, for instance, those that seek to integrate systems across the organisation

Rogerson and Fidler [23] argue that SISP provides the information needed to support business functions as well as an outline to apply strategies to business operations. Information strategy planning also examines how systems relate to an organisation’s general business environment [8]. SISPis primarily the process of deciding the objectives for organisational. The contemporary organisation should implement for overall improvisation, optimisations, BCP or desirable value additions.

One of SISP focuses is the detection of appropriate IS for the organisation, investment appraisal and implementation planning with the overall well-aligned IS/IT and business strategies. Lederer and Sethi [16] interpret SISP as a formal, rational exercise in which a series of logical steps are undertaken, resulting in end products which define IS requirements and identify a long-term hybridised strategy. Figure 1 adapted from [5] shows a model of five key stages in developing an IS/IT strategy.

The form outlines the inputs and outputs of the Information Systems/ Information Technology strategy, which clearly shows that a continuous cycle, with planning needed to achieve the outputs [7, 20]. According to Bhatnagar [6, 21], the following is a typical framework for IS planning:

- Phase 1: The initial purpose, process and the scope of the IS strategy.
- Phase 2: In-depth analysis of essential information needs, business processes and business requirements.
- Phase 3: Envisage an IS plan that would be appropriate for the company, after careful investigation and without missing any of the elements of an effective IS strategy.
- Phase 4: Outline a well-documented IS strategic plan, which can be used to examine and explore the features most vital for the organisation, leading to an IS strategy.

In any strategy, there are at least three elements: inputs, processes and outputs. An outline of the planning process given in [8, 29] includes the input activities are as follows:

- Internal Business Environment, including the current corporate strategy, objectives, resources, processes and culture and values of the business.
- External Business Environment, including the economic climate, industry and competitive environment in which the system operates.
- External/IT Environment, including the current IS/IT perspective of the business, its due date, the reporting and the contribution of commercial enterprise, skills, imaginations and the technology infrastructure. It also allows the current portfolio of existing systems and application development.
- External/IT Environment, including the current trends in technology and the opportunities and use of IS/IT by outside bodies.
- Moreover, an IS strategy addresses future business needs for in ways that align closely with the business strategy [12]. It should also describe the task needed to successfully utilise the portfolio. Figure 2 adapted from [6] outlines the generic but diverse steps in developing an IS plan by beginning with the definition of the project range that entails the description of the business needs. Then step is accompanied by the examination of the business environment and applications. Then this will follow the detection or selection of new options.

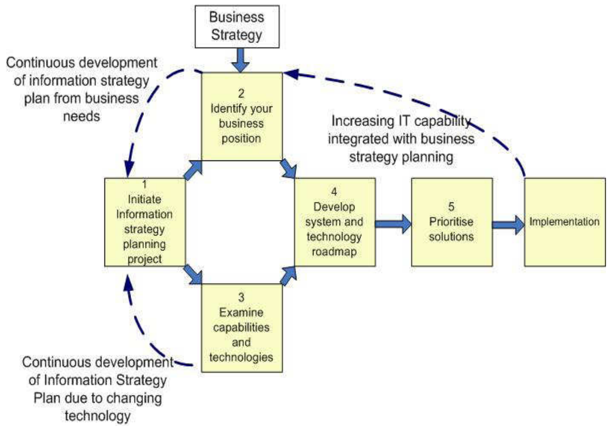
Business Strategy
Continuous development of information strategy plan from business needs
2 Identify your business position
Increasing IT capability integrated with business strategy planning
1 Initiate Information strategy planning project
4 Develop system and technology roadmap
5 Prioritise solutions
Implementation
3 Examine capabilities and technologies
Continuous development of Information Strategy Plan due to changing technology

Figure 2: IS Development Plan. Ankit Bhatnagar, 2006

The developments in the field of IT appear to characterise for distinguishable developments. For instance [28], the 1960s was reckoned to the beginning of real business data processing with standalone computers. The decades of the 1970s and 80s are characterised by MISs with distributed processing, interconnection, user-friendly interfaces, etc. The decades 1980s, 1990s and beyond may be reckoned to Strategic IS, enterprise IS etc. There has been growing recognition of the need for information systems, and developments were witnessed to cater to fast-growing requirements. However, as nothing comes free of cost, these systems came with huge complexities and size, making the strategic importance of managing as essentially inevitable.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

Lederer and Sethi [16] define SISP as a procedure of identifying the high-level IS requirements of an administration by identifying "a portfolio of information processing system-based applications that will serve an organisation in making its business plans and realising its business goals." In summation, they denote to the research by Sabherwal (et al) to propose formal or sensible procedures that can be suitably modified depending on the surroundings. [10, 20, 24]. King and Teo [14] forward that SISP is complete when organisations can effectively apply its IS applications revise business procedure and gain from competitive advantage [14]. Rogerson and Fidler [23] also argue that SISP provides a reason of the information required to realise business objectives and implement the necessary arrangements.

In order to deal with complexity and size of the contemporary systems, a serious framework is immensely needed. Before deriving an information systems framework, IT/IS professionals should set an IS planning framework that includes all of the essential elements needed to derive an IS strategy that reaches out to a consistent corporate strategy [6]. As in the initial stage in the setting of an IS strategy, a detailed plan must be set [8].

III. INFORMATION SECURITY POLICY WITHIN THE ORGANISATION

Information security primarily means protecting information from unauthorised access, use, disclosure, disruption, modification, scrutiny, inspection, recording or destruction [27]. Despite some subtle differences between information security and computer security, these themes are interrelated and often partake in the common goals of protecting the confidentiality, integrity and accessibility of data. Their differences lie primarily in the approach to the Information Security Policy, the methodologies employed, and the areas of concentration. Defending and protecting information confidentiality is a business requirement, and in many cases, it is also an ethical and legal requirement.

According to Gaston [8] ISP, however, "focuses on the broad guiding statements of goals to be achieved" with regards to the security of corporate information resources. This description is in universal agreement with the International Standard on Information Security Management (ISO 17799), which urges that an information security policy must provide the management with direction and reinforcement for information protection. ISP characteristically comprises of general statements regarding organisational goals and objectives [8, 13, and 20]. One way to devise a successful information security management is to utilise a top-down approach by leading away with the organisation's goals. According to Doherty and Fulford, it is desirable to identify "some information security goals that are not derived directly from the organisation's strategic plan, but the information security goals should never be in dispute with the organisation's goals" [8].

A security policy sets in place a scheme to provide security controls. It also offers a comprehensive description of the information system, as it references key documents that support the organisation's information security programme. [8] Primarily, ISPs to mitigate the risk associated three elements as goals known and depicted in Figure 3, as CIA Tried reprinted from [31], as follows:

- Confidentiality: The prevention of unauthorised use or disclosure of information. Privacy is a closely related topic that has lately been enjoying more and more visibility.
- Integrity: Ensuring that information is accurate and complete, and that it has not been modified by unauthorised users or processes.
- Availability: Ensuring that users have timely and reliable access to their information assets

These three elements are the basis around which all security programmes are developed. They are linked together through the idea of information protection. [31] The main idea is to show that information is an asset that requires protection. Kajava et al [13] argue that senior managers often have a poor understanding of information security. They also observe that only 20% of managers understood that information security was of strategic value to their organisations. [13]. They found that "enhancing information security awareness among all employees was necessary, but that the key to success was to raise the awareness level of senior management – who have often shied away from any training with regards to these matters" [20].

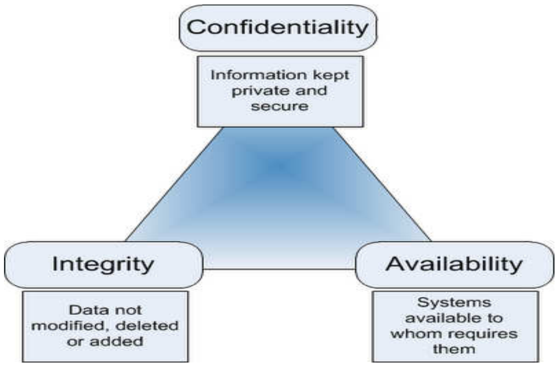
Confidentiality
Information kept private and secure
Integrity
Data not modified, deleted or added
Availability
Systems available to whom requires them

Figure 3: CIA Triad

These three elements are the basis around which all security programmes are developed. They are linked together through the idea of information protection. [31] The main idea is to show that information is an asset that requires protection. Kajava et al [13] argue that senior managers often have a poor understanding of information security. They also observe that only 20% of managers understood that information security was of strategic value to their organisations. [13]. They found that "enhancing information security awareness among all employees was necessary, but that the key to success was to raise the awareness level of senior management – who have often shied away from any training with regards to these matters" [20].

IV. RELATIONSHIP BETWEEN ISP AND SISP

Information systems are the lifeline of major as well as minor establishments now-a-days. Doherty [8] suggests that information is imperative to the triumph of the occupation and will be responsible for the business's various signs of success. SISP plays a critical part in helping to avoid "lost opportunities, duplicated effort, incompatible systems, and

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

wasted resources. Moreover, the process of developing an information systems plan helps to focus explicitly the planners' attention on “major opportunities for exploiting information” [8, 26, and 48].

In the last decade, researchers and practitioners are being aware the importance of relating information security policy with the organisational objectives [8].

According to Doherty and Fulford, Information security policy is the start of security management [8]. He observes it as “the caveat that the strategic information systems plan is a critical prerequisite for policy formulation, as it defines the business context in which information security will be managed, and therefore, priorities for security management”. [8] As Lederer and Sethi [16] note, strategic SISP plays a vital role in helping to avoid “lost opportunities, duplicated effort, incompatible systems, and wasted resources”. Ward and Peppard [28] also observe that the factual challenge is to certify that the uppermost value achievable, particularly regarding “timeliness, accuracy, completeness, and confidence in the source, reliability and appropriateness”.

Despite that that there is a shift in the importance of security management, in its report Information Security Breaches Survey 2008, the UK Department of Business, Enterprise and Regulatory Reform (BERR) shows that many companies are not practising enough to protect their data and client data [4, 22]. Practically, these companies fall short in providing adequate security information resources for their businesses. Many businesses reported a security breach in 2015, as compared with 81% in 2014. There has been an increase in the number of both large and small organisations experiencing breaches [30] as 90% of large organisations reported that they experienced a security breach, up from 81% in 2014. Small organisations recorded similar breaches, with “nearly three-quarters reporting a security breach; this is an increase on the 2014 and 2013 figures” [30]. Likewise, Austin and Darby [3] report that in the United States “security breaches affect 90% of all commercial enterprises in every year, and cost around $17 billion.” They likewise indicate that protective measures can be expensive; “the ordinary company can easily spend 5%–10% of its IT budget on security” [10, 22]. One significant method to “strive to detect, prevent and react to security breaches is through the concept and application of an information security policy” [8]. To protect corporate businesses in this changing world, BERR report recommends the following five guidelines [quoted in 4]:

- Understand the security threats faced by the organisation.
- Use risk assessments to target your security
- Invest in the most beneficial areas.
- Integrate security into normal business behaviour through clear policy and staff education.
- Deploy integrated technical controls and keep them up to date.
- Respond quickly and effectively to breaches, e.g., by planning ahead for contingencies.

Beyond these aforementioned studies, it also established that security cannot be taken as an afterthought, delayed measures account highly regarding cost and risk, and must be build-in right through the initial stages to be conducive. That is, the ISP must be embedded in SISP. To implement the major security recommendations and protect contemporary information systems, the formulation and application of state-of-the-art ISP are inevitable within SISP.

V. SECURITY-EMBEDDED SISP FRAMEWORK

The importance of security lies in heavy reliance placed on IT, the pressure to deliver services, increasing the range of threats and ever-increasing security risks. General perceptions about productivity include the relative cost of requisite procurements, training, operations and maintenance; the return on investment such as insurance; inefficiencies; and negative images that may bring restrictions and devaluations. Most general typical security problems have been witnessed in the form of natural disaster, industrial inaction, system breakdown, system failures, sabotage, theft, malware attacks, error, negligence, etc. And the most generous as well as primary goals of IS/IT security are confidentiality, integrity, availability and non-repudiation. Undoubtedly, any ISP must be security products, i.e. comprehensive and robust while being cost-effective, cost-efficient, simplest possible, economically operable, highly protective, acceptable, and unobtrusive. In order of security assurance several IT Security Standards and Frameworks, such as ISO/ IEC 17799, CoBIT, NIST and Trusted Computer Systems, came gradually into existence. ISO 17799 (based on BS 7799) originally released in 2000; subsequently improved ISO 17799: 2005 was released in June 2005.

A retrospective ISP assessment must measure the organisation’s information security setting which includes exposure assessments, predictive threat models, monitoring, detection and response [32]. In order the security controls based on ISO/ IEC 17799 2005 among other things included security policy, the organisation of Information security. However, the fraternity of technocrats, planners and business developers is witnessing real (and growing) need for IT security with generally poor perceptions. The achievement of security goals with real value for typical investments within the context of security embedded SISP is highly inevitable.

Secondly, today’s systems need to necessarily expand their focus of their security activities to cope with the changing cyber-sensitive environment. The uncertainty about cyber threats will continue to hamper good decision-making around security; and, pragmatic approaches are needed to cope with this. It is estimated that up to 80% of security breaches could be prevented by implementing basic good practices [33]. Therefore, there appears an inevitability about cyber sensitivity with regard to much needed comprehensive (inclusively sufficient) ISP based SISP.

Development of such an ISP embedded with SISP appears need of the hour and has huge potential for the sustenance of the IT enabled systems. Hence, twelve security components are hereby identified to be placed in a comprehensive ISP, and details of those needs to be developed and taken care of during any SISP, strictly under the ambit of Threat and Vulnerabilities Audit on one dimension and their controls on the other – having requisite sensitivity to cyber context. Such a framework is hereby proposed as follows in Figure 4 that is a guiding force for developing an ISP embedded SISP with regard to comprehensive security aspects with regard to audit as well as controls, under context now led/sensitised by cyber environment and context.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

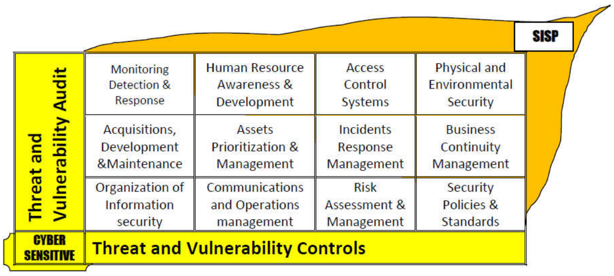
SISP
Threat and Vulnerability Audit
Monitoring Detection & Response
Human Resource Awareness & Development
Access Control Systems
Physical and Environmental Security
Acquisitions, Development &Maintenance
Assets Prioritization & Management
Incidents Response Management
Business Continuity Management
Organization of Information security
Communications and Operations management
Risk Assessment & Management
Security Policies & Standards
CYBER SENSITIVE
Threat and Vulnerability Controls

Figure 4: Cyber Sensitive ISP Embedding Framework

The details of the different components of the framework need not be included as they can be easily drawn from the standard definitions. However, the usability of the framework will largely depend on the component-wise developments, precise specifications and embedding adequately in the SISP.

VI. CONCLUSION

In the contemporary world, security has emerged as one of the basic needs and can no more be considered a non-functional requirement but an integral factor of quality of ISs. The exercise of SISP focuses on the identification of suitable IS for the organisation, investment appraisal and the implementation plan; with the overall aim of aligning IS strategy with business strategy. Information security plans can neither exist alone not as an afterthought. Instead, an organisation's information security has to be characteristically part of overall organisational objectives by choice or compulsion. An ISP should be in alignment with broader organisational goals. To carry out SISP, an organisation carries out an intensive study. The majority of firms pursue some predefined and documented methodologies, whereas others set their plans. During a multi-step study, a portfolio of applications is defined with appropriate priorities.

Embedding ISP in SISP should increase the security capability of an organisation. Moreover, the deliverable from the SISP process will be more beneficial to the organisation, especially in terms integrity. Although organisations can add value to the security components rather than restart the security planning from the start. All the same, such benefits will not be realised from the utilisation of data if the associated information systems and engineering sciences are used in an unfocused or piecemeal fashion. Such embedded SISP may play a critical part in helping to avoid security failures and lost opportunities and in producing a compatible system. As foretold, the security of information technology is a challenging issue facing managers. The unambiguous integration of IS into the SISP process can provide managers with a powerful and effective new approach to amending the protection of their organisations. In doing so, this should ensure that IS should not be spoken in isolation from other business operations

REFERENCES

1. Issa-Salwe, M. Ahmed, K Aloufi and M. Kabir, "Strategic Information Systems Alignment: Alignment of IS/IT with Business Strategy", Journal of Information Processing Systems, Vol.6, No.1, pp….March 2010.
2. Altameem , A. I. Aldrees and N. A. Alsaeed. 2014, "Strategic Information Systems Planning (SISP)", Proceedings of the World Congress on Engineering and Computer Science, San Francisco, USA, 22-24 October, 2014,
3. R.D. Austin and C.A. Darby, ". The Myth of Secure Computing", Harvard Business Review, Vol.…121–126, June 2003
4. BERR (Enterprise and Regulatory Reform). 2008. Security Breaches Survey 2008, UK Department of Business.
5. Beynon-Davies P. Business Information Systems. 2013. Palgrave/Macmillan, Houndmills, Basingstoke. 2nd edition.
6. Bhatnagar, A. (2006). Strategic Information Systems Planning: Alignment of 'IS/IT' Planning and Business Planning. Unpublished thesis submitted in partial fulfillment of the degree of Master of Computing, Unitec Institute of Technology, New Zealand.
7. Brian Fergerson. 2012. Key Stages of Strategic Information System Planning (SISP) Methods and Alignment to Strategic Management Planning Concepts, ERP and Virtualization Services Columbia Forest Products, Applied Information Management Program, University of Oregon.
8. Neil F. Doherty and Heather Fulford (November 2005): Aligning the information security policy with the strategic information systems plan. Computers & Security, Vol 25, Issue 1, 55–63. February 2006.
9. Garg A., J. Curtis and H. Halper. 2003. Quantifying the Financial Impact of Information Security Breaches, Information Management and Computer Security 11 (2), 74–83.
10. Höne Karin and J. H. P. Eloff. 2002. Information Security Policy — What Do International Information Security Standards Say? Computers & Security, Volume 21, Issue 5, 1, 402-409.
11. ISO/IEC 17799. 2005. ISO. Information technology -- Security techniques -- Code of practice for information security management. International Standards Organisation.
12. John Lindström and Ann Hägerfors. 2009. A Model For Explaining Strategic IT and Information Security To Senior Management, International Journal of Public Information Systems. Vol 5:1. 17-29.
13. Kajava J., Varonen R., Anttila J., Savola R., and Röning J. Senior Executives Commitment to Information Security – from Motivation to Responsibility, Proceedings of the International Conference on Computational Intelligence and Security, IEEE. 2006.
14. King, W. and Teo, T. S. H. (1997) Integration between business planning and information systems planning: Validating a stage hypothesis. Decision Sciences, 28:2, pp. 279-308.
15. Kolkowska E. Value Sensitive Approach to IS security – a socio-organisational perspective, Proceedings of the Eleventh Americas Conference on Information Systems. 2005.
16. Lederer, A. L., & Sethi, V. Key prescriptions for strategic information systems planning. Management Information Systems, 35-60. 1996.
17. Lindström John and Ann Hägerfors. A Model For Explaining Strategic IT and Information Security to Senior Management, Luleå University of Technology, Sweden, International Journal of Public Information Systems, Vol 1.2009.
18. Luftman, J. N. Competing in the information Age Align in the Sand (2nd ed.). New York: Oxford University Press. 2003.
19. Md Hafiz Selamat, Adam Suhaimi, Husnayati Hussin. January 2006. "Integrating Strategic Information Security with Strategic Information Systems Planning". National ICT Conference 2006 (UiTM), Kangar.
20. Newkirk, H., and Lederer, A. The Effectiveness of Strategic Information Systems Planning for Technical Resources, Personnel Resources, and Data Security in Environments of Heterogeneity and Hostility. The Journal of Computer Information Systems, 47 (3), 34-44. 2007.
21. Jens Bartenschlager. 2011. Implementing IT Strategy: Laying a Foundation. Informatik. Management Research Centre Frankfurt School of Finance & Management.
22. PWC, 2013 Information Security Breaches Survey: Technical Report. Department for Business, Innovation & Skills (BIS).
23. Rogerson, S. & Fidler, C. 1994. Strategic Information Systems Planning: Its Adoption and Use, Information Management and Computer Security, (2),1-7.
24. Sabherwal, R., & Chan, Y. E. (2001). Alignment between business and IS strategies: A study of prospectors, analysers, and defenders. Information Systems Research, 12(1), 11-33.
25. Siponen, Mikko, Designing Secure Information Systems and Software: Critical Evaluation of the Existing Approaches and a New Paradigm. Academic Dissertation. University of Oulu. 2002
26. Vincent LeVeque. 2006. Information Security – A Strategic Approach, John Wiley & Sons, pp. 3-20, 149-152.
27. Ward, J. & Griffith, P. Strategic Planning For Information Systems (2nd Edition). John Wiley & Son, London. 2000.
28. Ward J. and J. Peppard, Strategic Planning for Information Systems, John Wiley & Sons, Chichester. 2002.
29. Wylder J. 2004. Strategic Information Security, Auerbach/CRC Press LLC, pp1-16, 139-153.

30. PWC, 2015 Information Security Breaches Survey: Technical Report, HM Government, UK.
31. Geraint Williams (2015): CIA Triad. .Information SecurityProfessional Blog. {WWW document} http://geraintw.blogspot.com/2012_09_01_archive.html . Visited 01 January 2016
32. Ten key IT considerations for internal audit - Effective IT risk assessment and audit planning: http://www.ey.com/Publication/vwLUAssets/Ten_key_IT_considerations_for_internal_audit/$FILE/Ten_key_IT_considerations_for_internal_audit.pdf
33. Ten Steps to Cyber Security: https://www.cyberessentials.org/system/.../10-steps-to-cyber-security.pdf

Dr Abdisalam Issa-Salwe is currently an Associate Professor at Faculty of Computer Science and Engineering, Taibah University, Kingdom of Saudi Arabia. Between 2003 to end of 2008, he was lecturer in Information Systems at Thames Valley University in the United Kingdom. Between 1992 to end of 2003 he worked as Information Technology tutor at the Training & Employment Section of the British Refugee Council. Issa-Salwe's research interest includes Information Systems Management, strategic Information Systems, and Information Security. He earned his PhD in Information Management at Thames Valley University, UK. Issa-Salwe is also a writes matters pertaining to the Horn of Africa and has published several works dealing with the region in general, some of these are: (1) The Collapse of the Somali State: The Impact of the Colonial Legacy, Haan Associates Publishers, 1996; and (2) Cold War Fallout: Boundary Politics and Conflict in the Horn of Africa, Haan Associates Publishers, 2000. In 2010, he published his dissertation as two books: (1) Electronic Communication and an Oral Culture: The Dynamics of Social Web Environment Case Study; and (2) Oral Culture and Computer Mediated Communication, LAP LAMBERT Academic Publishing.

Prof. Khurram Mustafa is currently on a visiting assignment in the Department of Information Systems, CCSE, Taibah University, Saudi Arabia being on EOL from Jamia Millia Islamia, New Delhi, India. He graduated first with MSc (Mathematics with Computer Science) from JMI-Delhi, followed by MTech (Computer Applications) & PhD (Computer Assisted Instruction) from IIT-Delhi, India. He has been working at university level in regular capacity since 1997, as a Professor since 2008; and he served as founder Head, Department of Computer Science during 2000-01 & subsequently headed it during 2007-13. He also served as Associate Professor for an academic session each during 2004-07 in AHU-Jordan, AU-Yemen and KFU-Saudi Arab. Though, he did his PhD on an interdisciplinary topic related to eLearning, he continues to supervise, write and lecture on diverse topics pertaining to eLearning, information security and 'Research Methods in Computer Science'. He has already supervised ten PhD students to completion, co-authored 2 *books (published by Narosa, India and the international edition by Alpha Science, UK)*, out of those one has been translated to *Chinese language*. Apart from these he has also authored/co-author several book chapters and more than 90 research papers (published in journals/conference proceedings), led a 3-years government funded project as PI - in the field of Software Security and delivered more than 30 invited-talks/keynote-addresses. Besides regularly being a member several statuary committees, review boards, UGC/MHRD expert committees, academic bodies of several universities; he has been a member of several professional scientific societies including ACM-CSTA, ISTE, ICST, EAI, eLearning Guild & InfoPier..