# The Impact of Business-IT Alignment on Information Security Process

Mohamed El Mekawy, Bilal AlSabbagh, and Stewart Kowalski

Department of Computer and Systems Science (DSV), Stockholm University, Sweden
{moel,bilal}@dsv.su.se, stewart@fc.dsv.su.se

**Abstract.** Business-IT Alignment (BITA) has the potential to link with organizational issues that deal with business-IT relationships at strategic, tactical and operational levels. In such context, information security process (ISP) is one of the issues that can be influenced by BITA. However, the impact has yet not been researched. This paper investigates the BITA impact on ISP. For this investigation, the relationships of elements of the Strategic Alignment Model and the components of Security Values Chain Model are considered. The research process is an in-depth literature survey followed by case study in two organizations located in United States and the Middle East. The results show clear impact of BITA on how organizations would distribute allocated security budget and resources based on the needs and risk exposure. The results should support both practitioners and researchers to gain improved insights of the relationships between BITA and IT security components.

**Keywords:** Business-IT alignment, BITA, Information Security Process, Security Value Chain, Security Culture.

## 1 Introduction

The importance of IT as an enabler of business has spawned research on effective and efficient deployment of IT to gain strategic advantage (Sim and Koh, 2001). However, many companies still fail to gain values and advantages from huge IT investments. This failure is partially attributable to a lack of Business-IT alignment (BITA) (Leonard & Seddon, 2012). Strategic alignment refers to applying IT in a way that is timely and appropriate and in line with business needs, goals and strategies (Luftman, 2004). Therefore, in an increasingly competitive, IT-driven and vibrant global business environment, companies can only gain strategic advantages and derive values from IT investments when efforts are made by management to ensure that business objectives are shaped and supported by IT in a continuous fashion (Kearns & Lederer, 2000).

The achievement of such objectives requires strong relationships between business and IT domain not only at strategic level, but at also tactical and operational levels (Tarafdar and Qrunfleh, 2009). This highlights the importance of ensuring internal coherence between organizational requirements and delivery's capability of IT domain. It also highlights the importance of Information Security Process (ISP) as integrated part of IT strategy tactics and operations (Avison et al., 2004). In particular,

F.F.-H. Nah (Ed.): HCIB/HCII 2014, LNCS 8527, pp. 25–36, 2014.

BITA at operational level requires social perspective and aspects like interaction, shared understanding/knowledge across teams and personnel. Even thought BITA is shown to have potential impact on ISP at different organizational levels, little research has been done is this area (Saleh, 2011). Given the fact that the ISP focuses on relationships between business and IT for supporting BITA, the complexity of its nature is increased when considering different views on IT in organizations and how to utilize it in regard of business objectives.

This paper investigates the impact of BITA on ISP. For this investigation, the relationships of elements of the Strategic Alignment maturity Model (SAM) developed by Luftman (2000) and the components of the Security Values Chain Model (SVCM) developed by Kowalski & Boden (2002) are considered. The remainder of the paper is structured as follows: the research approach is discussed in section 2. The implications of BITA and ISP are presented in section 3 and 4 respectively. Potential relationships between BITA components and SVCM are presented in section 5. Results and analyses are presented in section 6 followed by conclusions in section 7.

## 2 Research Approach

The followed research method and process are namely an in-depth literature survey followed by case study research. The literature survey aimed to study theories behind BITA and ISP and hypothesize the impact of BITA criteria on SVCM's components. Following that, qualitative data was collected from two organizations through semi-structured interviews with four respondents in each organization i.e. selected to represent strategic and senior management at both business and IT in both organizations. The results where codified and compared to the proposed hypotheses.

The first organization (Referred as Company-A) is a midsize insurance company in the Midwest of the United Stated. The second organization (Referred as Company-B) is a governmental entity located in the Middle East and acts as national regulator for communication and technology business.

## 3 Implications of Business-IT Alignment

In literature, BITA is related to different scopes, and it is therefore defined differently. While some definitions focus more on the outcomes from IT for producing business value, others focus on harmonizing business and IT domains with their objectives, strategies and processes. These two views have affected the way in which BITA is expressed in publications. Publications which studied benefits of IT for business look at leveraging/linking (Henderson and Venkatraman, 1993), enabling (Chan et al., 1997), transforming (Luftman et al., 2000) and optimizing (Sabherwal et al., 2001) business processes. Other studies which focus on relationship between business and IT refer to BITA as fitting (Benbya & McKelvey, 2006), integrating (Lacity et al., 1995), linking (Reich & Benbasat, 2000), matching (Chan et al., 1997), bridging (Van Der Zee and De Jong, 1999), fusion (Smaczny, 2001) and harmonizing (Chan, 2002).

Results from BITA research show that organizations that successfully align their business and IT strategy can increase their business performance (Kearns & Lederer, 2003). BITA can also support analysis of potential role of IT in an organization when it supports to identify emergent IT solutions in the marketplace that can be opportunities for changing business strategy and infrastructure (Henderson & Venkatraman. 1993). Not only researchers, but business and IT practitioners have also emphasized the importance of BITA. In the annual survey of the Society for Information Management, BITA was first on the top management concern from 2003-2009 with the exception of 2007 and 2009 in which it was second (Luftman & Ben-Zvi, 2010). Therefore, practitioners should place special attention on BITA and particularly on how it is achieved, assessed and maintained in organizations.

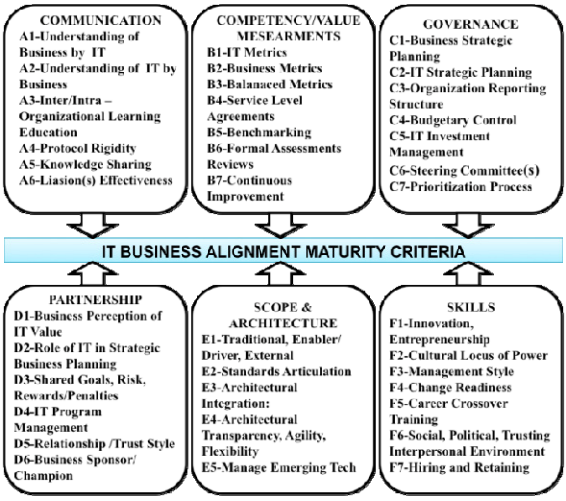


**Fig. 1.** Luftman's Strategic Alignment Maturity (SAM) (adapted from Luftman. 2000)

Different efforts have been oriented towards assessing BITA by proposing theoretical models that can be applied as supportive tools for addressing different BITA components. An extensive study by El-Mekawy et al. (2013) collected those models with their components in a comparative framework. Although Henderson and Venkatraman are seen as the founding fathers of BITA modeling (Avison et al., 2004), Luftman's model (SAM) has gained more popularity in practice (Chan & Reich, 2007). This gain is due to the following motivation: a) It follows a bottom-up approach by setting goals, understanding linkage between Business and IT, analyzing and prioritizing gaps, evaluating success criteria, and consequently sustaining alignment, b) It presents strategic alignment as a complete holistic process which encompasses not only establishing alignment but also its maturity by maximizing alignment enablers and minimizing inhibitors (Avison et al., 2004), c) SAM focuses on different BITA areas by modularity in six criteria, and d) Since its inception, SAM has been used by several researchers and in number of industries for assessing BITA and its components. Therefore, SAM is selected to be used in this study for assessing BITA

and analyzing the proposed impact on ISP. SAM classifies BITA in six criteria (Table 1) consisting of 38 attributes (Figure 1) in five maturity levels: Ad Hoc, Committed, Established Focused, Managed, and Optimized Process. This classification gives clear view of alignment and helps to spot particular areas of where an organization needs to improve for maximizing values of IT investments.

**Table 1.** Criteria of SAM

| BITA Criterion | Definition and Questions Attached |
|---|---|
| **Communications** | Refers to clear understanding between business and IT communities with an effective exchange and sharing of each ideas, processes and needs. |
| **Competency/ Value Measurements** | Concerns about demonstrating IT values in compatible figures with the business community understanding. Therefore, both business and IT have usually different metrics of values they add. |
| **Governance** | Ensures that business and IT communities formally and periodically discuss and review their plans. Priorities are important for allocating the needed IT resources. |
| **Partnership** | Refers to the relationship between business and IT in having shared vision of organisation's processes IT as an enabler/driver for business transformation. |
| **Scope and Architecture** | Illustrates IT involvement in organisational processes, and in supporting flexible and transparent infrastructure. This, however, facilitates applying technologies effectively and providing customised solutions responding to customer needs. |
| **Skills** | Refers to human resource aspects that influence/(are influenced) by changes and cultural/social environment as components of organizational effectiveness. |

## 4 Information Security Process (ISP)

Information systems (IS) in organizations are implemented to support their business processes that enable to achieve business objectives. With such systems, one should consider information security as a process of answering questions of '*what is needed to protect organization resources*', '*why do resources need to be protected? from whom and how*' (Schwaninger, 2007). In such context, information security, given its socio-technical nature, requires both social and technical activities. Globalization of Internet has created situations in which security problems are not limited within groups, organizations, or nations. With current trends in IS outsourcing and movement towards open distributed systems, people from different organizational culture are charged to administer security processes that need to meet security requirements and expectations of data owners. International security standards have been made available to address part of the issue by providing standard measures. However, standards are by design attempt to be contextual neutral i.e. do not consider organizational cultures, governance or alignment between business and IT domains.

ISP traditionally has been linked to three main objectives; confidentiality, integrity, and availability. However, achieving information security is unlimited to only achieving these objectives. It is attached to sustaining IS for achieving organizational objectives against security attacks and accidents (Saleh, 2011). One of the main problems

in organizations' security is that it is often viewed as an isolated island without established bridges between security requirements and business goals. The rationale for this problem is mainly referred to financial aspects and controls in organizations. This often results in lack of security and financial investments in the organizational core IS. It is therefore important that security to be built as a process with both planning and designing phases of IS. This includes adaptability of security architecture for ensuring that regular and security related tasks are deployed correctly (Amer & Hamilton, 2008). It has been emphasized that security requirements should be linked to business goals and IS through a process-oriented approach (Schwaninger, 2007). This clearly supports for building-up information security as a process dealing with organization's governance, organizational culture, IT architecture and service management (Whitman & Mattord, 2003). In addition to that, best practices in implementing security in organizations is indicated by factors such as complying regulatory equirements and fiduciary responsibility, measuring information security practices and improving efficiency/effectiveness (Saleh, 2011).

Unlimited to researchers, business and IT practitioners also have emphasized the ISP importance. In the annual survey of the Society for Information Management, ISP was among the top 10 management concerns from 2003-2009 and is the only technical issue in 2009 (Luftman & Ben-Zvi, 2010). Therefore, practitioners should place special attention on how information security should be practiced as a process joined with organizational planning, design and performing tasks.

Research in modelling ISP has been going since the introduction of computer systems to business. An early attempt to holistic models in this area is the Security by Consensus (SBC) framework developed by Kowalski (1991) for comparing different national approaches to security. Following that, socio-technical frameworks were developed (e.g. Lee et al., 2005; Al-Hamdani, 2009) for understanding security management as a social process. Other frameworks were developed emphasizing mental models of security (e.g. Adams, 1995; Oltedal et al., 2004; Kowalski & Edwards, 2004; Barabanov & Kowalski, 2010) for linking information security as a cultural process to business objectives. In this study, the Security Value Chain (SVC), developed by Kowalski & Edwards (2004), (Figure 2) is selected to analyze BITA impact on ISP. This is motivated by arguing on its establishment in analyzing different steps of business development process which is clearly influenced by aligning business and IT views. In addition to that, it represents patterns of mental security spending on its steps for visualizing how business and IT inputs intervene.

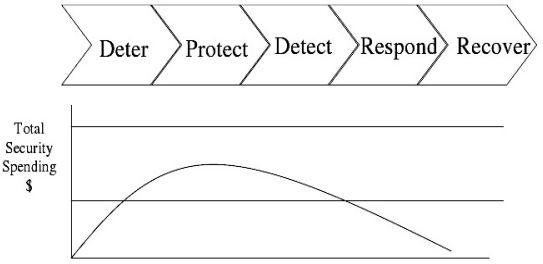


**Fig. 2.** Security Value Chain

The chain consists of five security access controls: deterrent, protective (preventive), detective, responsive (corrective) and recovery. These controls represent input points to IS (Table 2) in which an action may take place to stop undesired actions on the system. AlSabbagh & Kowalski (2012) operationalized the security value chain as a social metric for modeling the security culture of IT workers individuals at two organizations. Their research showed how IT workers' and individuals' security culture diverse given security problem at personal, at enterprise and national level. The research also studied the influence of available fund on security culture.

**Table 2.** Definitions of Security Value Chain Control Measures

| Control | Definition |
|---|---|
| **Deter** | for reducing chances of exploiting existing vulnurability without actually reducing the exposure. E.g. consequences of violating a company security policy. |
| **Protect** | for preventing occuring of security incident (e.g. access control implementations). |
| **Detect** | for identifying and characterize a security incident (e.g. monitoring system alarm). |
| **Respond** | for remediating the damage caused by a security incient (e.g. incidet response plan). |
| **Recover** | for compensating for the losses incurred due to a security incident (e.g. security incident insurance). |

## 5 BITA Impact on Information Security Process

Over years, different studies have shown clear impact of business objectives and performance on ISP (e.g. Huang et al., 2005; Johnson & Goetz, 2007). Other studies focused on the impact of IT strategies and how IT is perceived on ISP (e.g. von Solms and von Solms, 2004; Doherty & Fulford, 2005). As the relationship between business and IT is represented by BITA, the impact of BITA on ISP is apparent. However, it is neither analyzed in studies of BITA nor in studies of ISP (Saleh, 2011). In this section, indications of BITA impact on ISP are presented. Each criterion of SAM is described by which it influences the access controls of the security value chain. Hypothetically, we expect to find at least one existing reflection of each SAM criterion on an access control. With the help of SAM's attributes in each criterion, more various interesting relations may be addressed.

- **Communications.** Based on the findings of Herath & Herath (2007), it is indicated that matured channels and metrics for communications between business and IT have a strong impact on how ISP is perceived in an organization. This also influences the way the organization reacts and responses to the security attacks. However, as found by Huang et al. (2006), it can be concluded that achieving complete information security is virtually impossible. This is due to the need for matured communications in an organization to be further extended to include suppliers, partners and customers which potentially increases the risks to attacks. Therefore, matured communications in BITA is found to have less expenditure in *detecting*, *responding* and *recovering* but no clear indications for *deterring* and *protecting*.

- **Competency/ Value Measurements.** Kumar et al. (2007)'s findings indicated the importance of developing IT and business metrics to the expenditure on ISP. They are not only indicating risks through process, but also in incorporating changes in organizational aspects compared to previous results. In addition to that, the findings of Gordon et al. (2005) show that attacks on IS come not only from outside the organization. The loss from 'theft of proprietary information' was, for example, shown to be three times than from virus in 2005 according to the CSI/FBI survey. This indicates that developing matured business and IT metrics will reduce investments in *Detecting* and *Responding* of ISP but increasing expenditure in *Deterring* and *Protecting*. However, there is no clear indication on *Recovering*.
- **Governance.** According to the results of Johnson & Goetz (2007), effective distribution of investment on ISP is influenced by fitting IT security into business goals and processes through its governance structure. In addition to that, Beautement et al. (2008) argue that the misalignment in governance would lead to friction between ISP and business processes into the organizational system. It is then indicated that matured governance can result in reducing the expenditure on *detecting* and *responding*, but increasing the expenditure on *protecting* and *recovering*. No indications can be highlighted for the deterring.
- **Partnership.** According to the findings of Ogut et al. (2005), organizations with high partnership have interconnection between business and technology which supports the organization in better planning and decision making for security. According to Yee (2005), this partnership makes clear goals and trust all over the organization and supports for faster matured ISP. Therefore, it can be indicated that matured partnership would be attached to less expenditure in *detecting*, *responding* and *recovering* but no clear indications for *deterring* and *protecting*.
- **Scope and Architecture.** As found by Huang et al. (2006), complete information security is impossibly achieved. Gordon and Loeb (2002) found that optimal investment in information security is not necessarily increased with vulnerability. Organizations should prioritize to protect the most significant IS. Johnson & Goetz (2007), additionally, found that advancing IT architecture with rigid structure would influence expenditure on ISP. It is then concluded that matured IT architecture would increase its complexity level, and consequently indicates slower *detection* and *responding* to attacks with increasing their expenditure. However, rigid and strong architecture will reduce the cost of *deterring*, *protecting* and *recovering*.
- **Skills.** Huang et al. (2005) found that skills and experiences of decision makers are important players in information security investments. Although, there are strong arguments from different researchers (e.g. Beautement et al., 2008) on reasoning for cost and benefit of ISP to include the impact of individual employees, but it is mainly related to complying security policies. It is then influenced by individual's goals, perceptions and attitudes. However, they influence the development level of systems, platforms and protecting important applications as well. Therefore the impact of matured skills can be indicated on reducing expenditure on *protecting*, *detecting*, *responding* and *recovering*.

# 6 Results and Analyses

In this section, results and analyses of BITA assessment are presented in subsection 6.1 followed by the analyses of BITA and ISP in subsection 6.2.

## 6.1 BITA in the Organizations

- **Communications.** In Company-A, the understanding of business by IT is characterized to be higher than understanding of IT by business. Understanding of business by IT is seen focused and established process, but it should be more tied to performance appraisals throughout IT functions. However, the business senior and mid-level managers have limited understanding of IT which results in less Committed process. In overall, communications is assessed at level 2. In Company-B, understanding of business by IT is also more matured than understanding of IT by business. As an IT-related organization, senior and mid-level IT managers have good understanding of business in order to achieve the targeted objects. Knowledge sharing is limited to the strategic level. Such conditions were indicated at matured level 3.
- **Competency/ Value Measurements.** IT metrics and processes in Company-A are perceived primarily technical (e.g. system availability, response time). They do not relate to business goals or functions. However, business metrics are seen far matured than IT metrics and extended as value-based on contributions of customers. The organization has formal feedback processes in place to review and take actions based on results of measures and to assess contributions across organisational functions. In overall, the maturity level is assessed at level 3. In Company-B, IT metrics are more matured. They are extended to formally assess technical, cost efficiency, and cost effectiveness measures (e.g., ROI, ABC). They are also followed by formal feedback processes in place to review and take actions based on results of measures. The business metrics are also matured and customer-based representing an enterprise scope. The overall maturity level is highlighted 2.
- **Governance.** It is indicated in Company-A that both business and IT strategic planning are characterized by formal planning at functional levels. However, it is extended at the business domain. In the IT domain, it is more occasional responsive according to projects or involvement scale in business. The overall maturity level is 2. The governance in Company-B is characterized by strategic business planning at functional units and across the enterprise with IT participation. It is further extended to business partners/alliances. However, the strategic IT planning is less matured without an extended enterprise view to customers/alliances. The federated reporting system further supports for an overall maturity level as 4.
- **Partnership.** Although there is good insights for matured alignment in Company-A, but IT is perceived as a cost to the organization for doing business rather a strategic partner. IT is involved in strategic business planning in limited scope. IT co-adapts with business to enable/drive for some projects and strategic objectives. In overall all, the maturity level is highlighted as 3. In Company-B, IT is perceived having a better role, however, it is still seen as enabler to future business activities.

It is also seen to bring values to the organization and co-adapt with business to enable/drive strategic objectives. These conditions indicate a level of maturity 4.

- **Scope and Architecture.** In both Company-A and Company-B, IT is considered as a catalyst for changes in the business strategy with a matured IT architecture. In addition to that, IT standards are defined and enforced at the functional unit level with emerging coordination across functional units. Although they are integrated across the organisation, but they are not extended to include customer and supplier perspectives which make a matured level of 3.
- **Skills.** In Company-A, the environment is characterized as innovative and encouraging especially at functional units. However, it has initial, technical training and little rewards. The career crossover is limited to only strategic levels, and the environment is dominated by top business managers who have more locus of power than IT managers. The overall matured level is then assessed as 1. In Company-B, innovation is strongly motivated especially at functional units with cross training and limited change readiness. The top business management has domination and locus of power for IT management. Career crossover is extended but to the senior management and functional units. The overall maturity is indicated at level 3.

### 6.2 BITA Impact on ISP

- **Company-A.** The interviews show potential impact of BITA maturity on ISP. For instance, while business perceives IT as a cost for business, senior and mid-level business managers have limited understanding of IT. Business seems not to care about security spending. The budget is allocated with no questions or awareness on how effectively used. This is also reflected in the fact that IT metrics are primarily technical. BITA maturity level seems to be focused and managed process. There is a formal feedback process for reviewing and improving measurement results. Both business and IT conduct formal strategic planning across the organisation but not extended to partners/alliances. What has also been understood during the interviews is that there is no awareness regarding the need for having the five types of security access controls. One of the interviewees was even supported to get figures providing spending distribution according to the five controls.

**Table 3.** Ideal and Expected Security Value Chain in Company-A based on Collected Data

| Security Access Control | Deter | Protect | Detect | Correct | Recover |
|---|---|---|---|---|---|
| Ideal Budget Dsribution (%) | 5 | 40 | 35 | 15 | 5 |
| Expected Current (%) | 10 | 30 | 25 | 20 | 15 |

- **Company-B.** The interviews revealed potential impact of BITA maturity on ISP. The current SVC distribution almost matches what would be seen ideal. The reason behind this is the optimized levels of BITA *Value Measurements* and *Governance*. The limited business understanding for the importance of implementing deterring controls are apparent. However, there is a potential support and motivation for developing security policies that would state the consequences of misconduct and

accountability when security is violated. More than 10% of security budget is allocated to such deterring controls. The same problem is observed regarding recovery controls implementations. As business does not understand why IT needs to have active support licenses for its applications, the business decided not to renew any license. It is known in IT that having such support available is vital for providing means of recovery for potential issues. The business has considered having active support licenses as an extra cost which is not used most of the time. The limited maturity in *Communications* and *Skills* has also resulted in more severe issues related to human resourcing. Business is not allocating enough funds for hiring senior security consultants who can improve the organization's security position. Business perceives IT as an enabler to business objectives and changes, however, with insufficient turnovers. This perception has resulted in having budget constraints for IT and difficulties in approving it.

**Table 4.** Ideal and Current Security Value Chain in Company-B based on Collected Data

| Security Access Control | Deter | Protect | Detect | Correct | Recover |
|---|---|---|---|---|---|
| Ideal Budget Dsribution (%) | 12 | 23 | 23 | 20 | 22 |
| Expected Current (%) | 10 | 25 | 25 | 18 | 22 |

## 7 Conclusions and Future Work

In this paper, the potential impact of BITA maturity on ISP was explored in two organisations based on SAM and SVCM respectively. The study revealed correlations between BITA maturity level and existing security process. For instance, the lack of *Communications* maturity between business and IT had significant impact on security culture. When business management had limited understanding of IT, it was correlated to difficulties in approving IT security budgets including required human resourcing for hiring security consultants. This lack of communications had also negative impact on implementing *Deterrent* controls desired by IT department. It was also observed that limited business participation in IT strategic planning (i.e. *Governance*) was correlated to limited business understanding while *Recovery* security controls are needed. In turns this had a negative impact on implementing *Recovery* controls.

Immature alignment in *Value Measurement* and *Partnership* was found leading to immature security culture. For instance, when IT uses only technical metrics with no business considerations, it is perceived as a cost for business. This leads to lack of security awareness where business neither has interest to know nor it is aware of security spending or its performance. Optimized levels of BITA *Value Measurement* and *Governance* were correlated with increasing security awareness and its importance in business side and thus have raised interest in requirements related to IT security. This resulted in immediate approval of IT security budgets. Such situation has enabled IT managers to implement the SVC they believe to be ideal.

Suggested future work for this paper would be to conduct more case organisations to confirm whether the findings will lead to the same results we have in this paper.

## References


1. Adams, J.: Risk. Taylor & Francis, London (1995)
2. Al-Hamdani, W.A.: Non risk assessment information security assurance model. In: Proceedings of the Information Security Curriculum Development Conference, pp. 84–90. ACM, Kennesaw (2009)
3. AlSabbagh, B., Kowalski, S.: Developing Social Metrics for Security – Modeling the Security Culture of IT Workers Individuals (Case Study). In: Proceedings of the 5th International Conference on Communications, Computers and Applications (2012)
4. Amer, S.H., Hamilton, J.A.: Understanding security architecture. In: Proceedings of the Spring Simulation Multi-conference, Society for Computer Simulation, Canada (2008)
5. Avison, D., Jones, J., Powell, P., Wilson, D.: Using and Validating the Strategic Alignment Model. Journal of Strategic Information Systems 13, 223–246 (2004)
6. Barabanov, R., Kowalski, S.: Group Dynamics in a Security Risk Management Team Context: A Teaching Case Study. In: Rannenberg, K., Varadharajan, V., Weber, C. (eds.) SEC 2010. IFIP AICT, vol. 330, pp. 31–42. Springer, Heidelberg (2010)
7. Beautement, A., Sasse, M.A., Wonham, M.: The compliance budget: managing security behaviour in organisations. In: NSPW 2008, pp. 47–58 (2008)
8. Benbya, H., McKelvey, B.: Using Coevolutionary and Complexity Theories to Improve IS Alignment: A multi-level approach. Journal of Information Tech. 21(4), 284–298 (2006)
9. Chan, Y.E., Huff, S.L., Barclay, D.W., Copeland, D.G.: Business Strategic Orientation, IS Strategic Orientation, and Strategic Alignment. ISR 8(2), 125–150 (1997)
10. Chan, Y.E.: Why haven't we mastered alignment? The Importance of the informal organization structure. MIS Quarterly 1, 97–112 (2002)
11. Chan, Y.E., Reich, B.H.: IT alignment: what have we learned? Journal of Information Technology 22(4), 297–315 (2007b) (advance online publication)
12. Doherty, N.F., Fulford, H.: Do information security policies reduce the incidence of security breaches: an exploratory analysis. IRM Journal 18(4), 21–38 (2005)
13. El-Mekawy, M., Perjons, E., Rusu, L.: A Framework to Support Practitioners in Evaluating Business-IT Alignment Models. AIS Electronic Library (2013)
14. Gordon, L.A., Loeb, M.P.: The Economics of Information Security Investment. ACM Transactions on Information and Systems Security 5(4), 438–457 (2002)
15. Gordon, L.A., Loeb, M.P., Lucyshyn, W., Richardson, R.: CSI/FBI Computer Crime and Security Survey. Computer Security Institute (2005)
16. Henderson, J., Venkatraman, N.: Strategic alignment: leveraging information technology for transforming organizations. IBM Systems Journal 32(1), 472–484 (1993)
17. Herath, H.S.B., Herath, T.C.: Cyber-Insurance: Copula Pricing Framework and Implications for Risk Management. In: Proceedings of the Sixth Workshop on the Economics of Information Security, Carnegie Mellon University, June 7-8 (2007)
18. Huang, C.D., Hu, Q., Behara, R.S.: Investment in information security by a risk-averse firm. In: Proceedings of the 2005 Softwars Conference, Las Vegas, Nevada (2005)
19. Huang, C.D., Hu, Q., Behara, R.S.: Economics of Information Security Investment in the Case of Simultaneous Attacks. In: Proceedings of the Fifth Workshop on the Economics of Information Security, Cambridge University, pp. 26–28 (2006)
20. Johnson, M.E., Goetz, E.: Embedding Information Security into the Organisation. IEEE Security & Privacy 16 – 24 (2007)
21. Kearns, G.S., Lederer, A.L.: The Effect of Strategic Alignment on the use of IS-Based Resources for Competitive Advantage. Journal of Strategic IS 9(4), 265–293 (2000)

22. Kowalski, S.: The SBC Model: Modeling the System for Consensus. In: Proceedings of the 7th IFIP TC11 Conference on Information Security, Brighton, UK (1991)
23. Kowalski, S., Boden, M.: Value Based Risk Analysis: The Key to Successful Commercial Security Target for the Telecom Industry. In: 2nd Annual International Common Criteria CC Conference, Ottawa (2002)
24. Kowalski, S., Edwards, N.: A security and trust framework for a Wireless World: A Cross Issue Approach, Wireless World Research Forum no. 12, Toronto, Canada (2004)
25. Kumar, V., Telang, R., Mukhopahhyay, T.: Optimally securing interconnected information systems and assets. In: 6th Workshop on the Economics of IS, CM University (2007)
26. Lacity, M.C., Willcocks, L., Feeny, D.: IT outsourcing: maximise flexibility and control. Harvard Business (1995)
27. Lee, S.W., Gandhi, R.A., Ahn, G.J.: Establishing trustworthiness in services of the critical infrastructure through certification and accreditation. SIGSOFT Softw. Eng. Notes 30(4), 1–7 (2005)
28. Leonard, J., Seddon, P.: A Meta-model of Alignment. Communications of the Association for Information Systems 31(11), 230–259 (2012)
29. Luftman, J.: Assessing Business-IT Alignment Maturity. Communications of the Association for Information Systems 4, Article 14 (2000)
30. Luftman, J.N.: Managing IT Resources. Prentice Hall, Upper Saddle (2004)
31. Luftman, J., Ben-Zvi, T.: Key Issues for IT Executives: Difficult Economy's Impact on IT. MIS Quarterly Executive 9(1), 49–59 (2010)
32. Oltedal, S., Moen, B., Klempe, H., Rundmo, T.: Explaining Risk Perception. An evaluation of cultural theory. Norwegian University of Science and Technology (2004)
33. Ogut, H., Menon, N., Raghunathan, S.: Cyber Insurance and IT security investment: Impact of interdependent risk. In: Workshop on the Economics of Information Security, WEIS 2005, Kennedy School of Government, Harvard University, Cambridge, Mass. (2005)
34. Reich, B.H., Benbasat, I.: Factors That Influence The Social Dimension of Alignment Between Business And IT Objectives. MIS Quarterly 24(1), 81–113 (2000)
35. Sabherwal, R., Chan, Y.E.: Alignment Between Business and IS Strategies: A Study of Prospectors, Analyzers, and Defenders. IS Research 12(1), 11–33 (2001)
36. Saleh, M.: Information Security Maturity Model. Journal of IJCSS 5(3) (2011)
37. Schwaninger, M.: From dualism to complementarity: a systemic concept for the research process. International Journal of Applied Systemic Studies 1(1), 3–14 (2007)
38. Smaczny, T.: Is an alignment between business and information technology the appropriate paradigm to manage IT in today's organisations? Management Decision 39(10), 797–802 (2001)
39. Tarafdar, M., Qrunfleh, S.: IT-Business Alignment: A Two-Level Analysis. Information Systems Management 26(4), 338–349 (2009)
40. Whitman, M.E., Mattord, H.J.: Principles of Information Security. Thomson Course Tech. (2003)
41. Van Der Zee, J.T.M., De Jong, B.: Alignment is Not Enough: Integrating business and information technology management with the balanced business scoreboard. Journal of Management Information Systems 16(2), 137–156 (1999)
42. von Solms, B., von Solms, R.: The ten deadly sins of information security management. Computers & Security 23(5), 371–376 (2004)
43. Yee, K.P.: User Interaction Design for Secure Systems. In: Faith Cranor, L., Garfinkel, S. (eds.) Security and Usability: Designing Secure Systems that People Can Use, pp. 13–30. O'Reilly Books (2005)