Proceedings of the Tenth International Symposium on
Human Aspects of Information Security & Assurance (HAISA 2016)

Agile Changes of Security Landscape: A Human Factors and Security Investment View

R. Alavi and S. Islam
School of Architecture, Engineering and Computing, University of East London,
e-mail: {reza, shareeful}@uel.ac.uk

Abstract

The information security experts are finding it challenging to timely response the emerging threats. The rapid changing of security landscape and dependency on the agile software and system development projects make it challenging to address these threats in a real time. This could create potential risks to the overall business continuity. Furthermore, critical human factors, cost and investment in the information security field will add more anxiety in dealing with risks in an agile environment. There is a need for a unified approach to address the principles of information security, human factors and security investment in an agile environment. This paper provides a solution for constructing an effective information security system by taking into consideration an adequate risk assessment and controls, considering critical human factors and security investment within agile changes of security landscape. A list of concepts is considered for the purpose of an effective information security system. The paper also includes a short review of existing knowledge on the topics of agile development and information security.

Keywords

Agile Development, Information Security Systems (ISS), Human Factors, Security Investment (SI), Return on Information Security Investment (ROISI), Feature Driven Development (FDD), Secure Feature Driven Development (SFDD).

1. Introduction

Adequate and effective balance between organizational objectives and information security goals has always been a divisive issue in the field of information security and the gap between these two supported by many professionals (Sennewald and Baillie 2015). In many instances, particularly in financial institutions, information security professionals disagree with the rest of the organization on number of issues related to security, including critical human factors and security investment (Alavi et al. 2015). Such disagreement at organizational level comes at the time that business environment has more agility. This discrepancy creates impacts on information security system to achieve its objectives (McHugh et al. 2012). The concept of agile security straight advanced from agile software development applications. The agile projects have been replacing people with the process and scrapping plans for the purpose of just a response to changes (Hecker and Kolb 2015). This enables organizations to save in expenditures, including information security development process. Therefore, people and cost factors adversely impacted information security objectives. Whilst traditional approach uses resources such as time, budget and

people to enhance quality and fulfil goals, agile approach sacrifices quality with less use of the resources to achieve the goals (Baskerville 2004).

This paper contributes on analyzing the impact of the main human factors, security cost and investment on information security in an agile environment. These factors have been identified in previous studies (Alavi et al. 2013) (Alavi et al. 2014) (Alavi et al. 2015). In particular, the paper proposes a language using a set of concepts to analyze the impact caused on the effectiveness of information security in an agile environment. This paper has adopted the Secure-Tropos methodology to identify and analyze agile information security concepts and extend it with the critical human factors and Security Investment (SI) so that appropriate justification can be taken into consideration in assuring reliability and effectiveness of Information Security Systems (ISS) in an agile environment (Mouratidis and Giorgini 2009).

2. Related Works

There have been a number of works that focus on analyzing agile methods and approaches in information security. This section includes the works that are relevant to the study's approach.

2.1. Agile Development Background

Agile approach is a substitute to customary project management and characteristically used in software design development. It assists organizations for responding to unpredictability through additional and constant work intonations, where requirements and resolutions develop through collaboration between self-organizing and cross-functional panels (Dybå et al. 2014). However, in case of running both traditional and agile projects at the same time, it is appropriate to having a balance in them (Serrador and Pinto 2015). Whilst factors such as project size and requirements are important in upfront planning in traditional methods, the importance of critical human factors and investment must be considered in agile projects as a security point of view. But lack of balance between two main methods can end up in waste of resources (Boehm 1996). The waste of resources put a limitation on organizations to address risks resulted from emerging threats. Some authors considered main discussed human factors in agile projects. Chagas, et al, used a systematic literature review in studies that carried out on human factors in agile projects (Chagas et al. 2015). They concluded that Communication, Collaboration and Trust are the most important in the literatures, as they are significant to the core of Agile projects (Chagas et al. 2015). In this paper we would argue that the critical human factors which we have concluded previously; communication, awareness and the support of management are as important as trust and collaborations in regards to the security in agile projects. We also argue that the role of security investment is as crucial as other factors in the agile process.

2.2. Characteristics of Agile Projects

As agile projects are kicked off, responding to new security threats enter to a new environment where traditional planning and security approaches do not seem capable to deal with new requirements (Dove 2011). However, whilst agile projects bring some benefits to organizations, such as more frequent and dynamic product features, but there are some downsides, such as impact on security (Dove 2011). To understand the impacts on security in agile projects, the characteristics of such projects and impacts are reviewed. The main features of agile projects and security impacts are:

- Proactive and innovative team members
- Adapting and evolving through constant and dynamic changes
- Responding to changes in a situation-driven not planning approach
- Accelerated process using alternative direction
- Very little but ongoing planning
- Inconsistent and contradictory stakeholder goals
- Financial uncertainty in regards to ROISI and cost-benefit analysis

Furthermore, the security impacts of agile features can be summarized based on some of the main information security concepts. They are:

Vulnerabilities: The weakness in the design, implementation, operation or internal controls in an agile process that could be exploited to violate security of the system which require to be identified and analyzed, using vulnerability assessment.
Threats: The possible hazard to exploit the vulnerability which result to risk. Agile projects are potential threats to organizations which require an adequate risk analysis to be identify them and related vulnerabilities. Threat profiling is one of the essential steps to define them.
Risk: The combination of the probability of an event and its consequence.
Investment: Used by ROISI to established the monetary value of the losses.
Goal: Both organizational and security goals must be considered to evaluate how investment helped to achieve goals.

3. Main Factors in Agile Security Context

3.1. Role of Human Factors in Agile Projects

Dynamic software projects created new security requirements and whilst a big part of an agile software project includes the team-work between developers and people in an organization, critical human factors left untreated (Lin 2015). Whilst people do not have any specific motivation for agile development but they will support such method for making their job simpler. Three critical human factors in information security noted as: communication, security awareness and management support [1]. Other authors concluded quite similar factors as knowledge and leadership (Chagas et al. 2015). The nature and principle of agile projects create an urgency of consideration of human factors and socio-technical forces in which the technical matters become less important. This can be explained with ad-hoc and lack of

planned approach to such projects where non-technical forces become more powerful than traditional and planned software projects. Therefore, traditional and formal modelling requirements for software projects cannot be sought. Such outcome will have consequences on security matters. The problem, therefore, would be constant changes to meet agile requirements which have impacts on security system and policy. This creates challenges for the key elements of information security risk management where risk assessments, implementation of controls and security management metrics collide with changes in organizational agile requirements. Such challenges are met with critical human factors which are extremely difficult to be quantified and therefore, create a high security risk for organizations if they are left untreated. The difference between traditional software development projects and agile projects are mainly focused in planning where in the traditional plan-based methodologies human factors are not key consideration. However, in agile methodologies human factors are introduced in to the software development process in which the communication, awareness and senior management support and involvement are highlighted (Lin 2015). The absence of effective quantitative methods for analyzing the importance and impact of critical human factors left organization to rely extensively on project managers and project teams (Lin 2015). Such absence and challenges create an inadequate risk and vulnerability analysis which build information security ineffectiveness. In this paper we intend to highlight such critical factors and present a solution for greater consideration of critical factors and security investment.

3.2. Cost and Investment in Agile Projects

It is already well known that an investment and return on investment are important matters for enterprises. Software development and information security projects are both influenced greatly with economic factors where the cost benefit analysis plays an important role in it. Application software development and enterprise analysis use the advantage of agile methods to advance process quality and rise the opportunities to deliver a project in time, within budget, whilst they produce a high quality product **(**Dove 2011). The success in achievement of project objectives within a specified budget is considered to be an important principle. Budgets, investment and associated costs are therefore crucial factors. Such variables are easy to quantify and can be simply assumed by senior management team as they can be presented in numbers with a monetary value. Therefore, a quantification of return on security investment assists in the process of cost benefit analysis in agile process where there is no formal and advance planning in place. The use of Risk-Driven Security Investment Model (RIDIM) enables organizations to quantify the return on the security investment in regards to security incidents (Alavi et al. 2015). This model will help the organizations to achieve a quantifiable measurement for security incidents that help them to consider it when they run their agile software projects. The main factors which influence the cost and investment in agile projects can be summarized in a number of issues (Wu and Bailey 2007). Firstly, agile lifecycle projects unlike traditional development process, facilitates the investment to be used resourcefully throughout the lifecycle of the process. The agility process is to able to adjust the use of investment in order to maximize the return on the investment.

Secondly, agile development process enables organizations with significantly less time and transaction cost. This is in contrast with traditional techniques in which process requires a long time and costly exercise. The third factor is concerning the risk control and mitigation. Agile process carries more risks than traditional methods because constant repetitions and hasty process contains more risk which ironically benefited organization more. This is because organizations will be able to mitigate those risks that are based on the early completion and therefore, controls are more justified.

3.3. Threats in Agile Projects

Threat is described as an event with an unwanted effect on a security system where threats are the root causes of impacts and risk are the effects (Baskerville 2004) (Brotby 2009). Potential threats in agile projects can contribute to the integrity, availability and confidentiality of data system by exploiting vulnerabilities in an established IT infrastructure. Threats are potentially hampering the goals and creating risks and restraining investment as return on the security investment point of view. Threats in traditional projects can be defined and understood differently from agile projects for the differences which we described for both approaches. Whilst agile methods providing a platform for responding quickly to emerging threats, they can create new types of threats too. It is therefore important the identification of threats and opportunities within an agile project in order to balance the desire for reward against the risk incurred in its pursuit as the security point of view. This requires thorough understanding of risk appetite and tolerance within an agile project.

4. Framing Concepts

The process of securing information assets in agile environment has developed greatly during the last decade. Sometimes information security is seen as it is in odds with agility. It is vital for organizations to find a balance between security and agility. This includes the change of risk evaluation and prioritization, return on security investment as well as change of trend of human factors that should be in line with organizational objectives. It is also important to define clearly and separately the risk concept and security threats with an understanding of the threats concept from a risk perspective.

4.1. Concepts

In order to understand risk-investment dependencies in the agile security environment, it is necessary to understand the relationships among the relevant concepts such as actors, goal, risk, security investment, threats and security agile in the organizational environment. Specifically, an understanding of the impacts and dependencies between the actors and security agile characteristics are required to address information security requirements and objectives. To achieve this, the paper used some features from Secure Tropos-modelling language, based on risk analysis, actor, goals, security investment and agile security. The Meta-model characterizes

the primary conceptual components and consistent relationships amongst the attributes related to information security agile changes. Therefore, the Meta-model forms an abstraction view of the features. Figure 1 illustrates the Meta-model of the proposed risk-investment approach incorporating actor, goal, security investment, risk, controls and agile security.

Actor: is an active concept that purposefully performs crucial activities to achieve critical goals. It characterizes an entity that has intentional objectives within a system and organizational context for achieving goals whilst set of requirements to be satisfied, such as completing tasks, within dependencies between actors. Stakeholders (customers and employees), project team, information security system and management are the actors. Management team initiated the agile software development project. The project's documentation, elicitation, analysis and verification will be done by the project team which will be using by the stakeholders after management team in the organization approve it. Whilst, organization and management team have concerns over business-management practices and cost, the security is the concern of the information security system. Therefore, each actor follows their own strategic goals. This creates a quite difficult environment where the relationship between actors are constrained and hard to manage. At initial stage the identification of all actors are important as the agile development concerns all, which includes security too. It is also the impact on the actors which effects the agile project itself. For example, modifications in security requirements will have impacts on other actors in the organizational context. Therefore, time should be given for actors to receive adequate training and awareness education. It is also important for senior management team to promote the culture of security awareness and trust in their teams. Actors require to stay focus and team to reflect on their method of functioning and constantly improve themselves. This helps when security is breached, then actors can instantly and adequately take action to address the issue and avert additional damage to assets. People from different disciplines should act collectively to form a shared understanding and come up with methods to address the issue, solve it, and help the security team to put the updated control into process. Actors require to be involved fully to be able to act quickly and effectively.

Goal: is the actors' desire for the development of a project and its environment which provides an understanding of the needs and support the clients in an agile project. Identifying goals would help to know what to form before the project development begins so as to avert expensive and costly amendment. However, the process of goal fulfilment must be attained with an agreement of all actors. This also applies in agile projects in which all actors should have an agreement of shared planned. However, the important issue in agile projects in regards to goal is that such projects focus on characters and functionality requested by the stakeholders and actors over information system and organizational context. In case of any changes in the organizational context the agile security goals stay same. Goal concept has two categories, the security goal and organizational goal. These goals should be set up in the early phase of agile projects to ensure security is considered fully. The clarity in setting goals enables organizations to prevent future complexity in an agile environment.

Risk: In the context of this paper, risk is a likely harm to information assets in an organization, as consequence of an uncertainty of security arrangements in an agile project. Risk to information assets ought to be defined and managed, considering risk is an event that can be determined (Sillaber and Breu 2015). In a traditional approach defining and quantifying its impact is somewhat straightforward which is a function of threats as they try to exploit vulnerabilities, and in light of the controls, information assets can be protected. There are various ways to measure this such as:

$$\text{Risk} = \left(\frac{\text{Threats} \times \text{Vulnerabilities}}{\text{Controls}} \right) \times (\text{Asset Value})$$

As it is clearly shows in this formula the clarification of tangible values used for somewhat intangible assets. One the main concern for a better risk management should be a consideration of the likelihood of an identified risk and the impact of the risk. Considering definition of risk in relation to threats which exploit vulnerabilities and the value of the information assets, the exposure section must be clearly defined in information security policy. This also concerns investment and the return of it. Such factors are pressing and challenging issues in agile security. Since agile development promises the flexibility and speed in a dynamic environment, creates some uncertainties in maintain adequate and effective security strategy. The most uncertainties come from human factors and training people in regards to deal with ad-hoc security matters when they arise. Investment also an important matter which may create uncertainties as agile project are developed in a very short of time in which they financial impact assessment may have not been considered in details and correctly. However, organizations can provide a better security resilience with the consideration of return on security investment, security in each alteration, proactive maintenance of security, team-working and adequate response to security incidents. One of the mechanism to reduce risks and minimize their impacts is automation. The use of automation and business applications assists some of the time-consuming, tedious and error-prone activities to be carried out more effectively. Use of automating can considerably improve accuracy, reduce risk whilst at the same time to help for minimizing the time, quite significantly, for processing the changes. It is important to mention that agile is not a single entity in organizations but includes multiple areas of organizational activities. Therefore, there are various dimension are involved as information security point of view in which risk is one of the core aspects of such considerations. Identification and prioritization of risks therefore are important to deliver security as it required.

Vulnerabilities: are any types of weakness in an organization's information system, including software, hardware and internal controls, which leave information security expose to threats. Information security systems can use a risk-based approach to address and manage the vulnerabilities, considering they know where they are. Whilst vulnerabilities are located then they can be expressed in detailed and quantifiable rapports. There are certain elements in a vulnerability assessment that should be considered, such as resource identification and importance, as well as threat and control measure clarifications. Having a less well-defined threat analysis

which some organizations consider brings little attention than a vulnerability assessment that attempt an itemized list of weaknesses to address. It requires a combination of a threat source with a vulnerability to score in an asset exploit. Therefore, an arrangement of both sets of information must be contemplated. The vulnerability assessments are the combination of a performed, technical, administrative, physical processes and controls. However, it is more preferable that such assessments are being evaluated in the context of the threat assessments. A coherent, definitive and corrective action of prioritization and proper scheduling can be assumed if the vulnerabilities and threats to be considered jointly.

Investment: In the context of this paper, investment is the budget that is being allocated for security controls for supporting organizational and security goals and better deployment, integration, and customization of various security controls. Such controls assist organization to mitigate information security risks. Whilst security investment is seen essential for risk mitigation, the approach, strategy and levels of investment are disputed (Pandey and Snekkenes 2013). Despite the various approaches and analysis, organizations require to link the security investment requirements to the main organizational objectives. On-off investment in information security would not be able to deal with agile requirements as they happen to have fast and dynamic natures. Therefore, security investment should be considered fragmentally and on ad-hoc and situation-driven basis.

Controls: are protecting organizations' information assets by the means of prevention and/or detection. Well-executed information security controls provide a prime opportunity for organizations in regards to their conformity and performance. This can be used as a competitive advantage in the market for such organization. Strong approach by organizations to information security controls can leverage their competitive differentiators to boost market share, reputation, and profitability. In an agile environment the way controls are set up is important. Dynamic agile requirements, demands a dynamic security controls. In agile project a constant and situation-driven controls are required in order for security matter arisen on different and ever-changing environment.

Return on Information Security Investment (ROISI): Information security systems and security strategies are essential to day-to-day operation in organizations. However, they ought to be cost effective. But information security professionals struggle to demonstrate the cost effectiveness and ROISI in a language that senior executives to understand. Each asset in an information system has a value and its own monetary value in organizations. Therefore, each threat and vulnerability associated with one or more than one asset has financial impacts on organizations. One of the purpose of pursuing agile project is to minimize cost (Serrador and Pinto 2015). Despite this goal agile security hamper both organizational and security goals and put a lot of stress on the security investment.

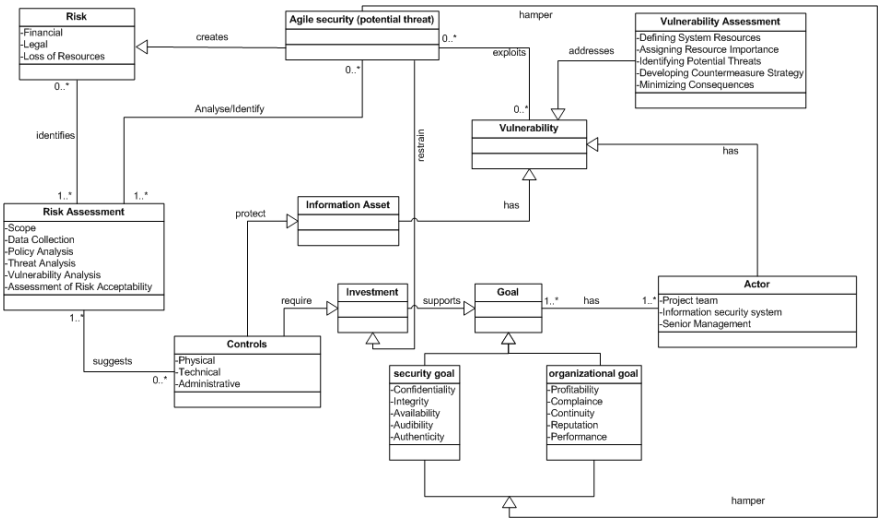

Figure 1: Meta-Model: Risk-Investment Agile Security

Figure 1 presents the Meta-Model, which is the combination of the above concepts, linked with some of the Secure Tropos security concepts to show risk-investment concepts in agile security projects. An actor has goals within an organization context which is also involving within the change of business context and these goals influenced the investment and controls. Therefore, both investment and controls need to align with the change of agile security landscape as the substance and value of information assets can be varies as the project requirements change. Risk assessment is also influenced by the agile context, for instance the value of perceive and residual security risks can change any time based on the severity of potential threats. In addition, the scope and threat profiling and vulnerability assessments within the risk assessment process will be influenced by agile context. This stimulates the visibility of risk, ensuring collective possession and accountability in relation to risk, and supporting well-informed decision making in an organizational context in respect to both organizational and security goals.

4.2. Process

Organizations and firms demand that information systems and consequently information security systems to adjust themselves to the ever changing and dynamic business environment. Thus agile projects introduce to respond to such demands. Despite surge of agile projects, there are many critical arguments that oppose them. Table 1 shows characteristic differences between traditional and agile approaches.

Traditional Approach	Agile Approach
technological-centric	human-centric
process-centric	collaborative decision-making
continual control and refining the process	iterative development cycles
Fully documentation of process	minimal documentation

Table 1: Characterization of Traditional and Agile Approach

There are several agile development methods. However, the most relevant to this paper and information security field is, the Feature Driven Development (FDD) development technique. FDD is a client, people and architecture-centric software method which delivers a robust modelling techniques (Box 2008). It emphases on the lifecycle phases of design and features are the main aspect of it. FDD used by many security and information assurance solutions. It contains some main activities that includes, developing high-level object model, building a feature list, grouping features into related subject areas, to plan by feature and identification of class owners and feature set owners. FDD has a number of security limitations and issues such as privileges and associated risks and security investment (Firdaus et al. 2014). For such limitations and problems some authors introduced the Secure Feature Driven Development (SFDD) (Firdaus et al. 2014). The concepts which this paper provided with the consideration of critical human factors and security investment on the basis of a risk-based solution can be fitted into SFDD methodology. SFDD introduced two additional phases known as Build Security and Test Security by features (Firdaus et al. 2014). The risk-based approach by this paper can be fitted to these new phases in the SFDD model at both stages.

5. Discussion

This paper offers a risks-investment based language considering human factors and security investment in agile security. It forms from some concepts such as goal, actor, investment, vulnerability, risk, and control that allow the analysis of agile security and recommendations for adequate control to ensure security is served in an agile environment. The control phase which includes attributes such as physical, technical and administrative, must be based on three pillars, transparency, inspection and adaptation that noted by Scrum technique (Fitzer 2015). These three pillars are important as security and its adequate architecture in an agile project always discussed up at top layers of organizations. The high-level solutions to security in agile environment remain relatively constant, even when there are local disparities in how the solutions are achieved. Flexibility and creativity guarantee security objectives are met in the appearance of change. This is particularly correct in an agile environment where critical human factors, risk and security investment play an intertwined role. The key to successful implementation of new controls is with ongoing involvement and profound engagement by people whilst human factors are considered and risks are defined adequately. Right allocation of investment for new

control and help stakeholders and actors to understand the reasoning behind security requirements assists security to achieve its objectives in an agile environment. One of important part of the discussion about security in agile environments, would be enterprise risk management which directly affect security arrangements, requirements and architecture. Enterprise risk management (ERM) consider risk from both internal and external perspectives and sources. These risks, mainly accompanying with swift and unanticipated changes which can be handled in a better manner when organizations are able to address human factors and security investment adequately.

6. Conclusion

In this paper we discussed a novel approach to deal with security in an agile environment. There is a constant claim that security makes it harder for organizations to be agile and more responsive. This is referred and related to the security standards, process, governance and more importantly security architect and controls. With the proposed language in this paper, organizations can be agile and at the same time to have their own security controls and policies. Having a solid security foundation which enforced by adequate investment and consideration of critical human factors, effective vulnerability assessment and adequate risk identification process, organizations can form a well-built security architecture. This process should be continually reviewed and revised. The security matters should be discussed holistically at board level with consistent risk identification, considering human factors which allows right investment to be made available for security controls.

7. Limitations and Future Studies

This paper has its own limitations. Firstly, we have not used any case study to acquire language applicability. The future study should consider a case study to find out whether the approach can be applied to real scenario. This is quite important matter, as security related subjects always behave with discrepancies when they used in real world case studies. The concepts used in this language requires more clarity in regards to detailed reactions of each concept when they put in an agile environment framework. This would be another limitation which future study should consider to ensure the maturity of the approach. The solution this paper provides can be considered for future studies considering SFDD model

8. References

Alavi, R., Islam, S. and Mouratidis, H., (2015), “Human Factors of Social Engineering Attacks (SEAs) in Hybrid Cloud Environment: Threats and Risks”, In Global Security, Safety and Sustainability: Tomorrow's Challenges of Cyber Security (pp. 50-56). Springer International Publishing.

Baskerville, R., (2004), "Agile security for information warfare: A call for research", ECIS 2004 Proceedings, p.13.

Brotby, K., (2009), "Information security governance: a practical development and implementation approach", (Vol. 53). John Wiley & Sons.

Alavi, R., Islam, S., Jahankhani, H. & Al-Nemrat, A. (2013), "Analyzing Human Factors for an Effective Information Security Management System", International Journal Of Secure Software Engineering (IJSSE) 4, 50-75.

Alavi, R., Islam, S. and Mouratidis, H., (2014), June. "A Conceptual Framework to Analyze Human Factors of Information Security Management System (ISMS) in Organizations", In HCI (24) (pp. 297-305).

Mouratidis, H. and Giorgini, P., (2009), "Enhancing secure tropos to effectively deal with security requirements in the development of multiagent systems". In Safety and Security in Multiagent Systems (pp. 8-26). Springer Berlin Heidelberg.

Dybå, T., Dingsøyr, T. and Moe, N.B., (2014), "Agile Project Management. In Software Project Management in a Changing World" (pp. 277-300). Springer Berlin Heidelberg.

Serrador, P. and Pinto, J.K., (2015), "Does Agile work? A quantitative analysis of agile project success", International Journal of Project Management, 33(5), pp.1040-1051.

Boehm, B., (1996), "Anchoring the software process", Software, IEEE, 13(4), pp.73-82.

Chagas, A., Santos, M., Santana, C. and Vasconcelos, A., (2015), "August. The impact of human factors on agile projects", In Agile Conference (AGILE), 2015 (pp. 87-91). IEEE.

Dove, R., (2011), "Patterns of self-organizing agile security for resilient network situational awareness and sensemaking", In Information Technology: New Generations (ITNG), 2011. Eighth International Conference. (pp. 902-908). IEEE.

Sillaber, C. and Breu, R., (2015), "Using Stakeholder Knowledge for Data Quality Assessment in IS Security Risk Management Processes", In Proceedings of the 2015. ACM SIGMIS Conference on Computers and People Research (pp. 153-159). ACM.

Pandey, P. and Snekkenes, E.A., (2013), "A framework for comparison and analysis of information security investment models", In 6th Norsk Informasjons Sikker-hets Konferanse (NISK).

Box, D., (2008), "Business Process Security Maturity-A Paradigm Convergence", (Doctoral dissertation, Nelson Mandela Metropolitan University).

Firdaus, A., Ghani, I. and Jeong, S.R., (2014), "Secure Feature Driven Development (SFDD) Model for Secure Software Development", Procedia-Social and Behavioral Sciences, 129, pp.546-553.

Fitzer, J.R., (2015), "Agile Information Security Using Scrum".

Sennewald, C.A. and Baillie, C., (2015), "Effective security management", Butterworth-Heinemann.

McHugh, O., Conboy, K. and Lang, M., (2012), "Agile practices: The impact on trust in software project teams", Software, IEEE, 29(3), pp.71-76.

Hecker, P. and Kolb, A., (2015), "Agile Engineering Introduction of a new Management Concept", Journal of Applied Leadership and Management, 1(1).

Lin, J., (2015), "Human Factors in Agile Software Development", arXiv preprint arXiv:1502.04170.

Wu, J. and Bailey, D., (2007), "Return on Agility: Financial Perspectives on Agile Development", Cutter IT Journal, 20(10), p.24.