INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN PROGRESSIVE EDUCATION & DEVELOPMENT

OPEN ACCESS JOURNAL

Vol 7, Issue 3, (2018) E-ISSN: 2226-6348

Theoretical Modeling of Information Security – Organizational Agility Model based on Integrated System Theory and Resource Based View

Muhamad Khairulnizam Zaini, Mohamad Noorman Masrek , Mad Khir Johari Abdullah Sani, and Norizan Anwar

Faculty of Information Management, Universiti Teknologi MARA (UiTM) UiTM Selangor, Selangor, 40150 Shah Alam, Malaysia

To Link this Article: http://dx.doi.org/10.6007/IJARPED/v7-i3/4379 DOI:10.6007/IJARPED/v7-i3/4379

Published Online: 26 July 2018

Abstract

This study believes that information security is vital in protecting information resources (information systems as a whole) and use it as strategic resources for competitive advantages as part of organizational objectives. Having a secured strategic information resources allows organizations to be dynamics in the unpredictable business environment. This paper discusses the integration both concepts of information security and organizational agility to become a solid concept, in the effort of constructing a theoretical model for further study. There are several theories in relation to information security practices and organizational agility such as Socio-technical System Theory; Social Cognitive Theory; Integrated System Theory; Resource Based View and Dynamic Capabilities are adapted and served as underpinning theories in providing insights and guidance for the development of theoretical model for this study.

Keywords: Information Security Practices, Organizational Agility, Integrated System Theory, Resource Based View, Theoretical Modeling, Information Management

Introduction

From an information systems viewpoint, information security is concerned with protecting information (Siponen & Oinas-kukkonen, 2007). Information security is a continuous socio-technical process that needs to be managed, which combines human actors and their interactions with technical assets. In this context, information security belongs to information systems domain as it is matches the socio-technical systems approach that pinned information security as the act of protecting information that resides on computers. As most business organizations are focus on the continual creations of sustainably-viable resources that stems from information for their goals, it is very crucial that these organizations apply suitable controls of protecting their business information from threats (Horne, Ahmad, & Maynard, 2016). In this setting, information security plays a vital role as it focusses on what protection is suitable for the information resources that belong to an organization. Mining the literatures has found that there are several theories in relative to information security practices and organizational agility such as Socio-technical System theory (Bostrom & Heinen, 1977); Social Cognitive Theory (Bandura, 1986); Integrated System Theory (Hong, Chi, Chao, & Tang, 2003) and Resource Based View (Wernerfelt, 1984), (Rumelt, 1984).

Application of Theories in Information Security Research

Application of these theories in information security research has a various effect in each setting. *Socio-technical System* (STS) for example study the interaction of the human element (organizations) with the technologies surrounding them, seeking to understand how people search, obtain, evaluate, share, classify and make use of the information provided by the information technology (Bostrom & Heinen, 1977). As the technology progressively advancing every day, the concern about risks surrounding them have also increased (Westerman & Hunter, 2007). Risks such as information security for example requires serious attention from the management. Within this context, those risks related to information security is part of sociotechnical systems in which human and technological factors were part of it. In relation, when particularly a security risk affects a technical system, it will affect the social and environmental systems as the whole. For example, a security leak in a single component may threaten the whole system, and security violations might have severe consequences to the organization. Therefore, in this STS point of view, verifying and maintaining the satisfaction of social and organizational information security requirements through the procedural design of secure STS is vital. Specifically, ensuring that all elements in STS (structure, people and technology) working well to safeguard vital information resources could contributes to improved efficiency and better performance. It is evident that technological, individual and organizational attributes and the interactions between these elements contributed to the act of preserving and securing information in an organization (Albrechtsen, 2007). Therefore, this study regards security controls as vital parts in *Socio-Technical Systems.* Controls help organization to create robust systems, as it allows some changes in responding to threats. Within information security point of views, controls are the safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical property, information assets, computer systems, or other assets. Other than that, this study also stressed that the *Social Cognitive Theory* (SCT) as relevant to the subject of this research. (Bandura, 1986) developed a Social Cognitive Theory or SCT which posits human behavior as a trade and reciprocal interaction of personal factors, behavior, and the environment and maintains that when people perceive they have the capabilities to perform an act that benefits them, they will expend substantial effort to accomplish that act. This is known as self-efficacy. Self-efficacy in information security therefore can be defined as a belief in one's capability to protect information and information systems from unauthorized disclosure, modification, loss, destruction, and lack of availability for the benefits of the businesses (Rhee, Kim, & Ryu, 2009). In the context of this research, we believe that self-efficacy in securing IT systems are essentials for agility.

This study is also congruent with *Integrated System Theory (IST).* This Integrated Systems Theory (Hong et al., 2003) is based on Contingency Management which suggests that there is no best way to organize a corporation, to lead a company, or to make decisions. Instead, the optimal course of action is contingent (dependent) upon the internal and external situation and depends on the nature of the environment to which the organization must relate and shall be organized based on the environment and nature of the organization. In IST, contingency management is subsequently to any of the security management activities (Ismail, Sitnikova, & Slay, 2014). This model consists of five components; security policy, risk management, internal control, information auditing and contingency management. These components are inter-related and can be combined to achieve organizational objectives.

Apart from that, this study also adapts the *Resource Based View* (Rumelt, 1984; Wernerfelt, 1984) which suggested that a basis for the competitive advantage of a firm lies primarily in the application of a bundle of valuable tangible or intangible resources at the firm's disposal to portray agility traits of an organization. In relations to information security, it is believed that organization can prolong their competitive advantage by rendering the information resource private and immobile through practices that enhance secrecy and security (Nelson & Romer, 1996). RBV denotes that a firm’s resources could include all assets, capabilities, organizational processes, firm attributes, information, knowledge, etc. which controlled by a firm and enable the firm to conceive of and implement strategies that improve its efficiency and effectiveness (Barney, 1991). In this context, this study believes that information security is vital in protecting information resources (information systems) and use it as strategic resources for competitive advantages. Other than that, this study also adapts *Dynamic capabilities (DC)* as theoretical foundation for this study as extension to RBV as suggested by (D. J. Teece, 2007). As the RBV emphasizes more on sustainable competitive advantage; the DC view on the other hand, focuses more on the issue of competitive survival in response to rapidly changing contemporary business conditions. Ability to use sufficient information helps organizations to integrate, build, and reconfigure internal and external competencies to address rapidly-changing environments, thus allowing organizations to become more nimbleness and flexible in that manners.

Reviews of Related Research Models

This study aims are to integrates both concepts of information security and organizational agility to become a solid concept, then several models will be referred in the construction of the theoretical framework for the study. Specifically, for this study two models are referred; Integrated Systems Theory (Hong et al., 2003); and Resource Based View (Barney, 1991; Rumelt, 1984; Wernerfelt, 1984). There are no theories however where the locus of knowledge is in information security alone (Horne et al., 2016). This gap however is not because information security is uninteresting but rather information security research is getting less attention for almost two decades. Lack of literatures in and empirical studies means that currently there are lack of information security management theory has been developed. Several tremendous efforts have been made in the development of more solid framework ok information security management theories for the past two decades such as the development of Integrated Systems Theory (Hong et al., 2003) to be adapted for the current state of information security research. In the same time, the development of agility as dynamic capabilities in achieving competitive advantage is well discussed in literatures, there are however lack of theory that integrates information security approach as predictors for agility. Although there are well discussions presence in the literatures that signify agility as part of dynamic, there are however insufficient to build solid body of knowledge on this matter. As for that, the section below will discuss both theories in thorough and finally attempt to conceptualized both concepts as a research framework for this study. The **Table 2** below summarizes all theories found to be related to this study.

Table 2
Summary of theories related to the study

Theories	*Description*	*Application in Information Security Management Research*
Socio-technical Systems (Bostrom & Heinen, 1977)	*Socio-technical system as an organizational system that is comprised of interacting social and technical systems. The components of this system affect one another if any of them are changed.*	*Security is quite a relevant aspect in the design of socio-technical systems. A security leak in a single component may threaten the whole system, and security violations might have severe consequences. Verifying and maintaining the satisfaction of social and organizational security requirements through the procedural design of secure socio-technical systems is vital.* *References:* (Salnitri, Paja, & Giorgini, 2014)
Social Cognitive Theory (Bandura, 1986)	*Human behavior as a trade and reciprocal interaction of personal factors, behavior, and the environment.* *Social cognitive theory maintains that when people perceive they have the capabilities to perform an act that benefits them, they will expend substantial effort to accomplish that act (Bandura, 1977).*	*For people to take IS security precautions they must positively assess their ability to cope with the perceived threat. There are relationships between people's perceptions of their behaviors and their actual behaviors in a couple of respects; first, coping depends on whether people feel that their ability to take security actions have been reasonable (self-efficacy), providing that they perceived that the threat is preventable in the first place (locus of control).* *References:* (Workman, Bommer, & Straub, 2008)
Integrated Systems Theory (Hong et al., 2003)	*This theory is based on Contingency Management which points out that all components of managerial activities should be emphasized especially in a fast-changing environment. In this model contingency management is subsequent to any of the security management activities.*	*Integrated System Theory was implemented to evaluate the important factors in the system that influences security awareness and implementation, by looking at: measuring the security policies, risk management, internal control and contingency management factors. The integration of all components shows an undeniable influence to the level of organizational information security goals.* References:(Ismail et al., 2014)
Resource Based View (Barney, 1991; Rumelt, 1984; Wernerfelt, 1984)	*a firm's resources include "all assets, capabilities, organizational processes, firm attributes, information, knowledge, etc. controlled by a firm that enable the firm to conceive of and implement strategies that improve its efficiency and effectiveness (Barney, 1991).*	*The RBV of the firms suggests that combining resources, including cargo, facilities, information, and humans can generate unique and hard-to-imitate capabilities that contribute to supply chain security performance. The firms that can manage their resources and capabilities in a supply chain more efficiently are likely to gain competitive performance* *References:* (Dangayach & Deshmukh, 2001)
Dynamic Capabilities (D. J.	*the ability to react adequately and timely to external changes*	*Security analytics and ISRM capabilities indirectly influence competitive advantage in ISRM, an impact that is mediated by two types of capabilities (ISRM*

Teece, Pisano, & Shuen, 1997)	*requires a combination of multiple capabilities.* *Dynamic capabilities theory concerns the development of strategies to adapt to radical discontinuous change, while maintaining minimum capability standards to ensure competitive survival.*	*dynamic capabilities and analytics-enabled ISRM capabilities)* *References:* (Naseer, Maynard, & Ahmad, 2016)

Integrated Systems Theory (IST)

In theoretical point of view, this study adapts **Integrated System Theory** (Hong et al., 2003) in which the integrated components of information security management and its outcome on organizational objective as suggested in the IST model met the main idea of this study. In specific, IST proposed that application of this theory can help organization to predict organizational attitudes and behaviors against information security management which is important in explaining organizational behaviors in regard to information security practices based on a particular circumstance (Hong et al., 2003). The IST is based on contingency management and integrates information security policy, risk management, internal control and information auditing theories to form an Information Security Architecture that is consistent with organizational objectives (Hong et al., 2003). Congruently, the excellence business organizations will always look for necessary resources, and build them to create successful, responsive, and competitive especially in a complex business environment. The contingency management emerged from such environment. The above-mentioned environment absolutely requires contingency management. And as this study stand on the premise that information resources as crucial elements in foreseeing and anticipating the future to be flexible and nimbleness, then applying information security management activities as contingency approach is unquestionably a beneficial for organization.

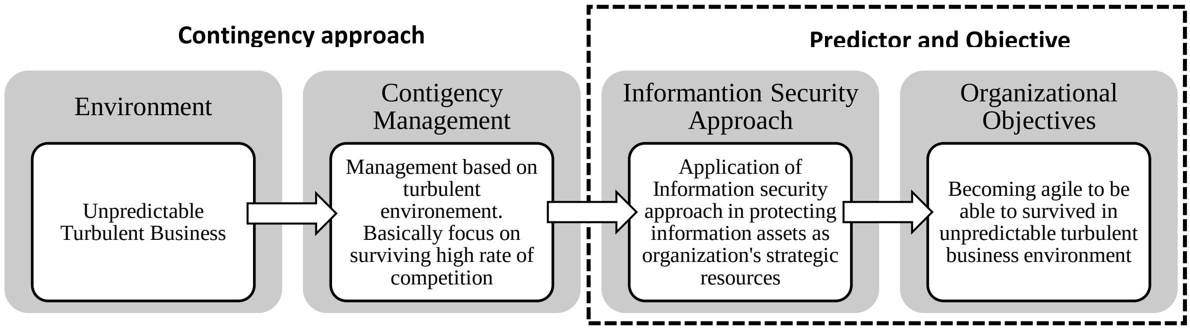
Contingency approach
Predictor and Objective
Environment
Unpredictable Turbulent Business
Contigency Management
Management based on turbulent environement. Basically focus on surviving high rate of competition
Informantion Security Approach
Application of Information security approach in protecting information assets as organization's strategic resources
Organizational Objectives
Becoming agile to be able to survived in unpredictable turbulent business environment

Figure 1: Congruency between the study and IST (Adapted from (Hong et al., 2003))

This study emphasized that Information security approach is a predictor to organizational objectives (as in this context becoming organizational agile) in the turbulent business environment as what globally has facing today. Overall this idea is totally in accordance with IST as depicted in **Figure 1** above. IST denotes information security as integrated approach consists of information security policy, risk management, internal control, information auditing and the contingency management itself. In addition to this, it also found that Internal control received special attention in IST, as it is an important measure to significantly attain information security objectives. Internal control in IST is associated elements such as personal security control, physical security control, systems and network security control, access control, systems development and maintenance control, business continuity and several others. In more detail, Information security approach/strategies in this context refers to the application of Information security in protecting and safeguarding information assets as organization's strategic resources.

Resource Based View (RBV)

On the other side, this study also adapted the **Resource Based View** (Barney, 1991), (Grant, 1991), (Wernerfelt, 1984), (Rumelt, 1984) suggested that a basis for the competitive advantage of a firm lies primarily in the application of a bundle of valuable tangible or intangible resources at the firm's disposal. In relations to information security, this study stands on the notions that an organization can prolong their competitive advantage by rendering the information resources privately and immobile through certain practices that enhance its secrecy and security (Nelson & Romer, 1996). In RBV view, if a firm has resources that is rare among its competitors, then it has the potential of producing comparative advantage in the market positions. Generally, there are three major constructs in the RBV model; resources that include all the asset, capability, organization process, enterprise character, information and knowledge, etc. that an enterprise be able to control, give the ruling, allocate the efficiency improving or achieve efficiency strategy; capabilities that could be in the form of internal and external capabilities; and components are the organization competitive performance (Barney, 1991). The Figure 3.2 below illustrate the core elements of RBV.

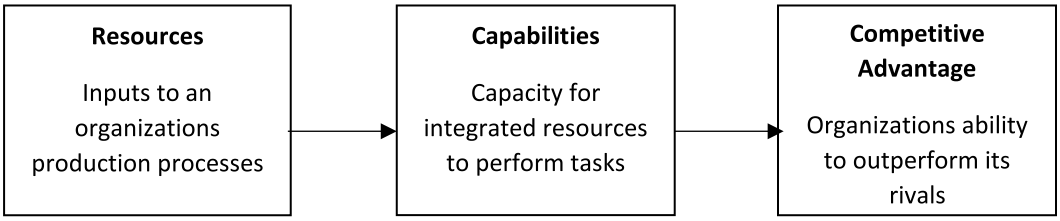
Resources
Inputs to an organizations production processes
Capabilities
Capacity for integrated resources to perform tasks
Competitive Advantage
Organizations ability to outperform its rivals

Figure 2: Resource Based View (RBV) core elements (Adapted from (Barney, 1991), (Grant, 1991))

Resources are inputs into the production process. RBV denotes that an organization's resources could include all assets, capabilities, organizational processes, firm attributes, information, knowledge, etc. which controlled by a firm and enable the firm to conceive of and implement strategies that improve its efficiency and effectiveness (Barney, 1991). Capabilities as the second component in RBV are also vital aspect. Capabilities "refer to a firm's capacity to deploy resource, usually in combination, using organizational processes, to effect a desired end (Barreto, 2010). They constitute the main source of competitive advantage in where it emphasizes the ability in appropriately adapting, integrating, and reconfiguring internal and external organizational skills, resources, and functional competences to match the requirements of a changing environment (D. J. Teece et al., 1997). In RBV, capabilities are processes or routines that arises from valuable, rare, inimitable and non-substitutable resources. However, non-substitutable resources could be copy or destroy by the competitors if left unprotected, thus eliminating the competitive advantage. Unless these superior resources are protected by some form of isolating mechanism preventing their diffusion throughout the firm's industry competitors, then the case is totally being different. According to (Barney, 1991), dynamic capabilities follow the theory of RBV of the firm. Dynamic capabilities are "the firm ability to integrate, build, and reconfigure internal and external competences to address rapidly changing environments" (Ambrosini & Bowman, 2009). Often, competitive advantage increasingly rests upon a dynamic capability to compete successfully in an environment of frequent, challenging and, often, unpredictable change (Meredith & Francis, 2000). In this context, organizations that has capabilities in foreseeing and predicting the future, will have the advantage to seizes opportunities and dodging threats, reacting and responding to internal and external changes in better ways. In this scope, some researches have also associated dynamic capabilities as equal to agility (D. Teece & Leih, 2016). This is aligned and correspond with the stands of this study that designate agility as capabilities organizational should possess in surviving competition.

The Information Security – Organizational Agility Model

In IST, the information security policy serves as a critical basis in the protection of organization's information. The security policy will act as guideline of information security in any organization. A well written security policy often comprises adequate guidelines on what must be done to protect information and people in the organization. In general, the information security policy is implemented and covers the elements of people, processes and technology controls. In this view, a well implemented security policy can guarantee that vital information assets are safeguarded. Risk management is the process of identifying, assessing and controlling threats to an organization's assets. Having well managed risk is considered imperatives in this context.

Other than that, the Internal Security controls are also acknowledged as important elements in this theory. Internal security controls are forms of safeguards or counter measures applied to avoid, counteract or minimize loss or unavailability due to threats. Applying internal controls can significantly improve the overall information systems security and it may help to minimize security risks that exist within organization's information systems. Administrative controls (policies, procedures, and processes to define and guide user actions and restrictions in dealing with sensitive information), technical controls (technology-based measures to control logical access to sensitive information) and physical controls (security measures, devices, and means to control physical access to a defined structure) are three broad categories define the main objectives of effective security implementation. Besides that, an information security audit is also essentials as it provides understanding on level of information security in an organization. It is a systematic, measurable technical assessment of how the organization's security policy is employed. Information security audit is part of the on-going process of defining and maintaining effective security policies. Drawing from IST, the information security management which comprises of security policy, risks management, internal controls and information auditing were considered as important measures for information security practices for this study.

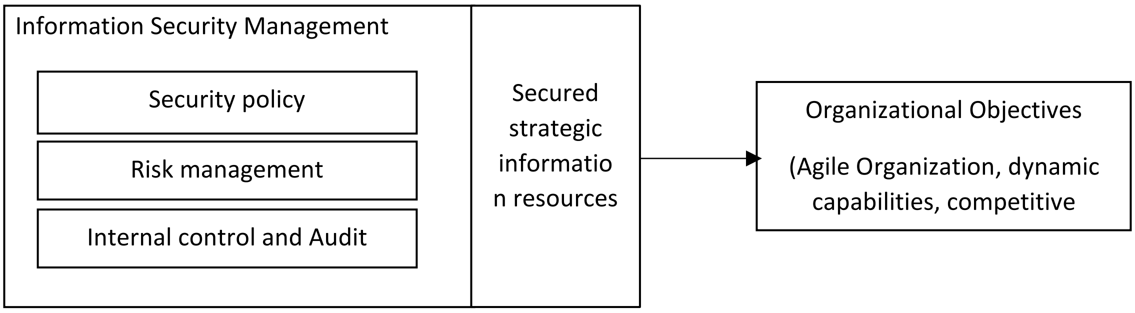
Information Security Management
Security policy
Risk management
Internal control and Audit
Secured strategic informatio n resources
Organizational Objectives
(Agile Organization, dynamic capabilities, competitive

Figure 2: Elements of theoretical model based on IST and RBV (adapted from Hong et al., 2003)

Information resources are strategic resources that can help organizations to achieve competitive advantage. Information assets can become superior resources for organization and for that reason these resources must be protected by some form of isolating mechanism preventing their diffusion throughout the firm's industry competitors. (Gunasekaran, 1999) highlighted in his literature that in the efforts of incorporating virtual elements within organizations, security issue is imperative in which sensitive business information and business processes must be protected. In this case, information systems with suitable protection may help to safeguard sensitive information. With this background, this study believes that information security is vital in protecting information resources (information systems as a whole) and use it as strategic resources for competitive advantages as part of organizational objectives. The **Figure 2** above depicts the integration of IST and RBV in modeling a theoretical foundation for this study.

Conclusions

While the development of agility as dynamic capabilities in achieving competitive advantage is well discussed in literatures, there are however lack of theory that integrates information security approach as predictors for agility thus insufficient to build solid body of knowledge on this area. This paper discusses both theories in thorough and finally attempt to conceptualized both concepts as a theoretical foundation for this study. It is allegedly believed that information security has a substantial effect on generating accurate, effective and efficient business decisions that leads to competitive advantages of an organization. Therefore, Information security programme is reckoned as essential reacting to above scenario. As information in an organization is considered as valuable assets, it is then requiring set of regular protection from security risks, threats and attacks. In this case, the integrations and adaptations of relevant theories on both concepts for this study is considered valid and served as important guides for the future works.

Acknowledgments

The authors would like to acknowledge the Research Management Centre (RMC) UiTM, Shah Alam and Ministry of Higher Education Malaysia (MOHE) for the financial support of this research. This research is supported by MOHE under the Fundamental Research Grant Scheme (FRGS) with project code: FRGS/1/2015/SS03/UITM/03/8.

References

Albrechtsen, E. (2007). A qualitative study of users' view on information security. Computers and Security, 26(4), 276–289.

Ambrosini, V., & Bowman, C. (2009). What are dynamic capabilities and are they a useful construct in strategic management? International Journal of Management Reviews, 11(1), 29–49.

Bandura, A. (1986). Social foundations of thought and action: a social cognitive theory / Albert Bandura. Englewood Cliffs, N.J: Prentice-Hall, 1986. xiii, 617 pp.

Barney, J. (1991). Barney 1991.pdf. Journal of Management.

Barreto, I. (2010). Dynamic Capabilities: A review of past research and an agenda for the future. Journal of Management, 36(1), 256–280.

Bostrom, R. P., & Heinen, J. S. (1977). MIS Problems and Failures: A Socio-Technical Perspective, Part II: The Application of Socio-Technical Theory. MIS Quarterly, 1(4), 11.

Dangayach, G. S., & Deshmukh, S. G. (2001). Manufacturing strategy: Literature review and some issues. International Journal of Operations & Production Management, 21(7), 884–932.

Grant, R. M. (1991). The Resource Based View of competitive advantage. California Management Review, Spring, 114–135.

Gunasekaran, A. (1999). Agile manufacturing: a framework for research and development. International Journal of Production Economics, 62, 87–105.

Hong, K., Chi, Y., Chao, L. R., & Tang, J. (2003). An integrated system theory of information security management. Information Management & Computer Security, 11(5), 243–248.

Horne, C. A., Ahmad, A., & Maynard, S. B. (2016). A Theory on Information Security. Australasian Conference on Information Systems, 1–12.

Ismail, S., Sitnikova, E., & Slay, J. (2014). Using Integrated System Theory Approach to Assess Security for SCADA Systems Cyber Security for Critical Infrastructures: A Pilot Study. 11th International Conference on Fuzzy Systems and Knowledge Discovery, 1000–1006.

Meredith, S., & Francis, D. (2000). Journey towards agility: the agile wheel explored. The TQM Magazine, 12(2), 137–143.

Naseer, H., Maynard, S., & Ahmad, A. (2016). Business analytics in information security risk management: The contingent effect on security performance. 24th European Conference on Information Systems, ECIS 2016.

Nelson, R. and Romer, P. (1996). Science, Economic Growth, and Public Policy. Challenge, vol. 39, no. 1, pp. 9–21.

Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. Computers and Security, 28(8), 816–826.

Rumelt, R. P. (1984). Towards a Strategic Theory of the Firm. Alternative theories of the firm. Competitive Strategic Management, 556–570.

Siponen, M. T., & Oinas-kukkonen, H. (2007). A Review of Information Security Issues and Respective Contributions. The Data Base for Advances in Information Systems, 38(1), 60–80.

Teece, D. J. (2007). Explicating dynamic capabilities: The nature and micro foundations of (sustainable) enterprise performance. Strategic Management Journal, 28, 1319–1350

Teece, D. J., Pisano, G., & Shuen, A. M. Y. (1997). Dynamic Capabilities and Strategic Management. Strategic Management Journal, 18(7), 509–533.

Teece, D., & Leih, S. (2016). Uncertainty, Innovation, and Dynamic Capabilities: An Introduction. California Management Review, 58(4), 5–12.

Wernerfelt, B. (1984). The Resource-Based View of the Firm. Strategic Management Journal, 3(June 1982), 171–180.

Westerman, G., & Hunter, R. (2007). IT Risk: Turning Business Threats into Competitive Advantage. Harvard Business School Press Books, (June), 1

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. Computers in Human Behavior, 24(6), 2799–2816.