Does the Development of Information Systems Resources Lead to the Development of Information Security Resources? An Empirical Investigation

Full Paper

Vasiliki Diamantopoulou
University of Brighton
v.diamantopoulou@brighton.ac.uk

Aggeliki Tsohou
Ionian University
atsohou@ionio.gr

Euripidis Loukis
University of the Aegean
eloukis@aegean.gr

Stefanos Gritzalis
University of the Aegean
sgritz@aegean.gr

Abstract

Information Systems (IS) are nowadays considered the most important leverage for organizations to operate and gain a competitive advantage. Investments in IS technology, in the recruitment of high qualified IT personnel and the establishment of internal and external robust IT related partnerships are considered determinant factors for business success and continuity. As organizations increasingly rely on IS resources, they face more advanced IS security challenges. This paper explores the relationship between the development of IS resources and security resources; are organizations willing to invest more in IS security resources as they invest more on IS resources? The authors conduct an empirical investigation in organizations located in five Mediterranean countries. The sample includes responses from 61 CEOs, information security managers and IS managers. The results reveal that IS resources positively affect the IS security resources. The human capital plays the most important role for the adoption of IS security.

Keywords

Information Systems Resources, Information Systems Security Resources, Resource-based view theory.

Introduction

There are numerous studies investigating the potential of Information Systems (IS) for organizations and their capacity to provide competitive advantage to them. IS have the capacity to enable new business models and innovative services, to optimize decision-making, to transform the organization to a pioneer in the provision of existing services, to improve relationships with customers and suppliers, or to achieve strategic advantage over competitors (Laudon and Laudon, 2016; Nevo and Wade, 2010). In order to take upon these capacities, the organizations are required to make significant investments in IS resources that include, amongst others, information technology (e.g., telecommunications, servers, equipment, software, and so on), business and system analysis services (e.g., change management, business processes redesign), and development of human capabilities (e.g., training). The use of IS in an organization relates to the support of core competencies (e.g., production, financial, sales, procurement), but also with the development of strategic processes (e.g., customer management, business intelligence). Most modern services offered by organizations today are increasingly reliant on IS, making the information technology (IT) behind a service to be inseparate from the service delivery itself (Sun et al., 2012). Because of this crucial role of IS for organizations, the IS resources represent their most important assets.

Although IS bear the capacity to enable significant improvements in organizations, they also involve significant challenges that imply indirect investments for organizations. Information security and the protection of users' privacy became crucial for organizations in order to maintain a high standard of services and retain competitive advantage (PWC Survey, 2017). Surveys report that among the most frequent attacks that organizations experience are malware, hacking, phishing, social engineering and the loss of mobile devices (ISACA, 2014). Technological advancements, including big data, cloud computing and Internet of Things, rapidly swift the requirements of information security, requesting organizations to make again significant investment on the protection information assets. Investments in information security may include the appointment of information security officers, threat assessment and threat intelligence, active monitoring, outsourced security and privacy services, authentication, data loss prevention, training (PWC, 2016; PWC, 2017). Although surveys reveal that security officers felt in the past that information security investments were insufficient (E&Y, 2012; 2014; CSI, 2008; 2009), there is a recent change; 'organizations no longer consider information security and privacy barriers to change or as an IT cost' but they see security as facilitators of business growth, market advantages and building brand trust (PWC, 2017) and organizations appear more willing to invest on information security and cybersecurity solutions (PWC, 2016).

The research objective of this paper is to explain the development of information security resources from the perspective of other IS resources. One would expect that there would be a balance between the IS resources that an organization holds and the information security resources developed to protect those IS resources. That is, as the organization builds more IS resources, it is expected that it also develops IS security resources for protecting them. Therefore, in this paper the authors examine if the development of IS resources indeed leads to the development of information security resources. As a first step towards this research objective, the authors seek for a classification scheme of IS resources that will allow them to capture the IS resources held by an organization. After reviewing the relevant literature (see following section), they selected for this purpose the IS resources classification by Ravichandran and Lertwongsatien (2005), which has also been used with some adaptations in the study of Gu and Jung (2013). Second, the authors have analyzed existing literature on information security, which lacks a similar classification scheme for information security resources. Combining the above classification with literature on information security countermeasures, they develop a measurement instrument for information security resources that will allow them to capture these resources held by an organization (see following section). Using this classification scheme, they conduct an empirical investigation exploring the IS resources and information security resources organizations, and the relationship among them. The paper concludes that IS resources positively affect the IS security resources. The significance of the IT human capital for the development of information security in an organization is highlighted. IS relationships also contribute, but to a smaller degree, to the development of IS security in an organization.

The paper is structured in six sections. The following Section II includes the necessary background concerning the IS resources and the IS security resources. Section III presents the hypotheses formulation while Section IV describes the method that has been followed for the empirical investigation of the relationships between these two entities. The results are presented and discussed in Section V, and finally, Section VI summarizes the conclusions and raises issues for further research.

Literature review

Information Systems (IS) Resources

The first component of this study is the IS resources within an organization. Their determination has been the topic of interest to practitioners and academics, since they are the main elements that affect both the core business operations (i.e. financial, sales, procurement, production) and also more specialized business operations (i.e. marketing, communication). The resources have been identified by Amit and Schoemaker (1993) as the appropriate stocks of available factors of production owned or controlled by an organization. IS resources have been identified by numerous studies as the main drivers of firm performance (Dierickx and Cool, 1989; Grant, 1991; Barney, 2001; Wade and Hulland, 2004; Melville et al., 2004; Nevo and Wade, 2010) which are necessary to conceive, choose and implement strategies. Researchers in the IS field have identified several IS resources as potential drivers of competitive advantage and performance within an organization. Apart from mere IS infrastructure, Mata et al. (1995),

investigating firms sustained competitive advantage, identified four attributes as resources; access to capital, technology that can be kept proprietary, technical IT skills and managerial IT skills. In the same direction, Ross et al. (1996) indicate the dimensions of skilled human resources, reusable technology base and relationships between the IS department and user departments as key IS resources within an organization. They emphasize that these assets, while quite distinct, are interdependent and mutually reinforcing. In order to examine the association among IT capability and business performance, Bharadwaj (2000) based on the resource-based view, classified IT resources as IT infrastructure, human resources and IT-enabled intangibles. Ravichandran and Lertwongsatien (2005) examine the way that IS resources and capabilities affect firm performance. In their study, they use IS resources in order to interrelate them with the IS capabilities and IT support for core competencies and firm performance. Likewise, they identify three IS resources, the human capital (separating it into technical and business skills and firm-specific knowledge), the infrastructure sophistication and the partnership. Gu and Jung (2013) also use the resource-based view theory in order to assess the IS contribution on firm performance, defining IS resources as a multidimensional construct that includes business expertise, internal and external relationships between the IS unit and the business units/IS providers, technical skills of the IS function staff and IS infrastructure.

The above studies reveal the potential of the resource-based view theory as the basis for the realization of the value that the IS resources add to an organization. The main argument of the resource-based view theory is that the performance of an organisation is determined by the resources it owns (Liang et al., 2010). This view is adopted in this paper and the authors draw from the resource-based theory in order to identify the IS resources of an organization, in order to make the IS resources comparable with any other resource that can affect the processes and the overall performance of an organization. In particular, this paper uses the IS resources classification developed by Ravichandran and Lertwongsatien (2005), which has also been used with some adaptations in the study of Gu and Jung (2013), which distinguishes between three categories of IS resources associated with IT related technology, human resources and partnership relationships. To this point, the category of *technology* identifies the physical IT assets which form the core IT infrastructure and the procedures that these assets support. The category of *IS human resources* identifies the technical skills (ability to adopt new technology, develop and operate IS), the experience, and the training of both the IT specialists and the general personnel. Finally, the *partnerships – relationships* examine the IS relationship quality of an organization, both internally, among the IT department and the various business units, and externally, with IT vendors and service providers.

Information Systems Security Resources

Following the resource-based view, the authors consider that the effectiveness of IS security resources depends on the efficient exploitation of their capabilities by the organizations. Our search in the literature for IS security resource schemes did not yield results and for this reason we developed a conceptualization of IS security resources combining the above IS resource frameworks and information security literature. Our purpose is to develop a framework that will allow us to capture the overall information security management resources in an organization. More specifically, we explored articles studying 'information security capital', studies reflecting 'information security measurement' and 'information security metrics'.

Brecht and Nowey (2013) create a classification scheme with categories of information security costs. They argue that classifying information security costs is a challenging task and they examine five perspectives for categorizing information security costs. According to the balance sheet approach, information security costs are divided into personnel, hardware, software, and managed security services. According to the life-cycle approach, this paper regards information security costs based on the countermeasure life-cycle; purchase, setup, operation and change. The ISO 27001 approach regards the fourteen security controls' categories as defined by the standard. Finally, another categorization regards security controls based on the level of management: operational, architectural, people, processes, management. Sans Institute (2010) separates security controls' costs into three categories: controls that are technological, controls that relate to people, and process controls. Torres et al. (2006) classify information security controls into three categories: the technical controls, which include hardware and software tools for protecting IS (e.g., antivirus, firewalls), the formal controls, which refer to the security policies and rules (e.g., strategies, risk assessment, compliance), and the informal controls which include any intervention for steering employees' security behavior (e.g., awareness, management commitment). NIST (2008) distinguishes the following categories of information security controls: vulnerability

management; access control; awareness and training controls; audit and accountability; identification and authentication; certification, accreditation and assessment; configuration management; contingency planning; incident response; maintenance; media protection; physical and environmental security; personnel; system and services acquisition, and others. ISO 27001 (2013) also offers a classification scheme for defining categories of IS security resources, and specifically 14 control categories including information security policies; cryptography; access control; asset management; organization of information security; physical and environmental security, etc. Following the analysis of the literature, the paper concludes that although there is no single information security classification scheme, there exist several approaches for capturing the IS security resources in an organization. Following a hybrid approach that integrates the classification of Ravichandran and Lertwongsatien (2005) and Gu and Jung (2013) for IS resources (i.e. technology, human resources, partnership-relationships) with the results from our literature analysis. More specifically, the authors adopted the following IS security resources classification in Table 1.

Category	**Description of IS Security Resources**
Technology	Asset inventory, identification and authentication system, access control, cryptographic key management, software protecting against malware, event logging
Security Policy and Processes	Information security policy, information security training, security by design in software engineering, definition of penalties for security policy violations, information security strategy
Human Resources	Security related knowledge and training of IT personnel, as well as of IT users, distinct roles for information security, special division/units for information security
Partnership relationships	Collaboration between IT personnel and business units personnel for information security, collaboration between IT suppliers and the organization

Table 1. IS Security Resources Classification

Hypotheses formulation

The research hypotheses of this paper, as depicted in Figure 1, concern the effect of IS resources on IS Security resources, namely the respective technology resources, human capital and partnerships – relationships, as they have been identified in the previews Section. Information security researchers have studied the factors driving information security investment decision, which mainly include risk and vulnerability related factors (Wang et al., 2006; Longstaff et al., 2000; Gordon and Loeb, 2002; Johnson, 2014). Other studies and surveys also highlight the determinant role of regulatory requirements for the development of information security (Johnson, 2014). This paper argues that, besides the above factors driving organizational decisions to invest in security resources, there are also other factors to be considered. Our argument is that the IS context itself also determines the development of information security. The authors see the IS resources as determinant to the development of IS security, and as complementary to the other factors (i.e. risk, compliance) identified by scholars. Moreover, they further proceed with investigating the effect of the different IS resources on the different IS security resources, in order to examine which particular elements of the IS context are determinant for the development of security resources. To the best of the authors' knowledge, similar study hasn't been conducted before.

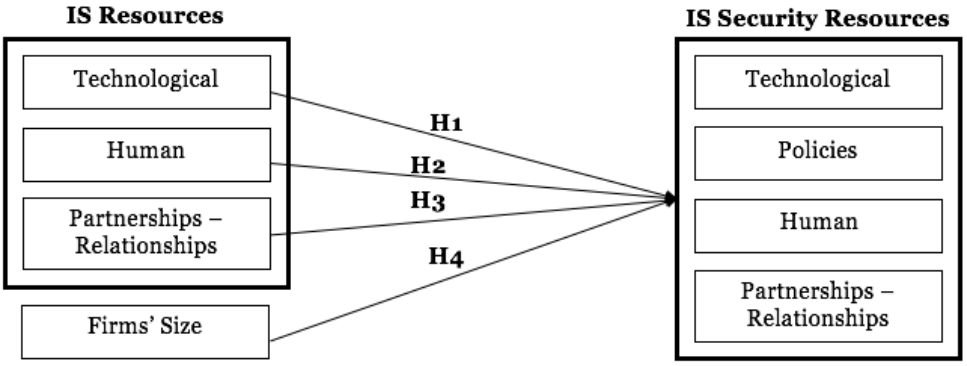

Figure 1. Research model of IS Resources and IS Security Resources

It is widely accepted that the investment on IS technological resources (e.g., telecommunications, servers, equipment, software, and so on) is essential to a firm's competitive survival and thus increases its business value (Gu and Jung, 2013; Laudon and Laudon, 2016). IS technological resources today are of outmost value to organizations for their survival, business function and maintenance of competitive advantage (Laudon and Laudon, 2016). On the other hand, information is considered as an asset which has a value requiring appropriate protection (ISO 27000, 2016). Protecting information assets through defining, achieving, maintaining, and improving information security effectively is essential to enable an organization to achieve its business objectives. Therefore, the authors expect that as IS technological resources increase in an organization, their value for the organization will also increase and thus IS security resources will also increase.

Hypothesis 1: IS technological resources have a positive impact on IS security resources

A valuable human capital can contribute to the positive performance of an organization (Skaggs and Youndt, 2004). This holds especially for the IS personnel, who are responsible for the monitoring and management of firm's IS, and also supporting and training their user; this allows the IS personnel to diagnose IS security related problems, propose solutions (both the use of security technologies, and the establishment of securities), provide training on them to the IT users, and in general collaborate with them on IS security issues. Thus, sufficient IS personnel is a prerequisite for effective security management processes. However, as cyber security attacks become more sophisticated, it becomes evident that the various information security controls within an information security management system require more specialized personnel. For example, a survey reports that health organizations have on average between 10-15 IT specialists working only on information security duties (AHIA, 2015). Similar are the results of a SANS Institute survey, which found that almost half of organizations spend 24.6% of IT budget on security staff (SANS, 2015). Organizations point out the necessity for dedicated personnel for disaster recovery personnel, IT audit and compliance, personal data protection, threats' detection and response, forensics, and others (AHIA, 2015; PWC, 2017). Therefore, the authors expect that as IS human resources grow the IS security resources increase, including security technology, human resources and partnerships. Our hypothesis is line with the results of Huang et al. (2006) who state that organizations should place equal attention to the tangible IT infrastructure and intangible human capital in order to form a successful base for information security.

Hypothesis 2: IS human resources have a positive impact on IS security resources

It has been argued that IS department and IS users should mutually appreciate and understand each other's environment, allowing IS to deliver value to the firm (Ravichandran and Rai, 2000). This IS specialized personnel – users partnership quality can affect the internal smooth flow, interaction and collaboration among them, which allows a better and more efficient realization of security related problems and needs, and implementing information safeguards that fit the business mission. As a representative example, organizations state that the most common problem for business continuity management is the lack of alignment and collaboration between business units and IT disaster recovery planning (E&Y, 2014). As far as the external IS partnership relationships is concerned, they facilitate the exchange of information about security problems and needs, as well as solutions for them, so it leads to

the development of IS security resources; it is expected that smooth collaboration especially with external IT vendors and service providers is crucial for information security development.

Hypothesis 3: IS Partnerships – Relationships have a positive impact on IS Security resources

In general, larger firms have more resources and capabilities in order to invest on the security of their IS, the security related training of their employees, and even on the recruitment of specialized security personnel and the establishment of units for IS Security. Interestingly, although security challenges are not differentiated by industry, they differ significantly by the organization's size (PWC, 2016). Therefore, the authors expect that as the size of an organization increases, the IS security resources will increase as well, first because they would have more security budget available, but also because they need to prepare for more sophisticated cyber-attacks. Thus, the final hypothesis is:

Hypothesis 4: Size has a positive impact on IS Security resources

Data and Method

For this study, the authors have used data they collected through a survey among firms with distinct sectors, in five Mediterranean countries, i.e. Greece, Cyprus, Italy, Spain, and Portugal. This paper focuses on the Southern European countries because they face similar financial and industrial problems, such as weaknesses concerning the size and structure of manufacturing, deficits in the public sector and business activity. Aiginger (2013) argues that despite the convergence that the European North and South have tried to achieve, the economic crisis has negatively influenced any attempt, widening this divergence. The financial crisis that the Southern European countries face, in comparison to the countries of the North, has constituted them weak, concerning the exploitation of economy globalization (Landesmann, 2015). The Southern European countries also have a larger share of low skill industries and a smaller share of higher skill ones; the technology driven industries are much smaller in comparison with the Northern European countries, and also declining.

The authors developed a questionnaire (available online at http://bit.ly/2fEJK5l) for the purposes of our study, based on the literature review analyzed in Section II, with questions concerning the IS resources (regarding technology, human resources and partnerships-relationships) and the IS Security resources (again regarding security technology, policy, human resources and partnerships-relationships). The survey was conducted in the period November 2016 to February 2017. The questionnaire has been sent to the CEOs, information security managers and IS managers of each organization, since they were the most informed about the IS resources and the IS security resources of their organization. The sample includes small, medium and large organizations that returned properly filled questionnaires.

The hypotheses were tested through the following four steps:

i. Calculation of the three composite IS technology, human resources and partnerships-relationships variables (ISTE, ISHR, ISRE), as averages of the corresponding individual variables.
ii. Calculation of the four composite IS security technology, policy, human resources and partnerships-relationships variables (ISSETE, ISSEPO, ISSEHR, ISSERE)
iii. Calculation of the correlations of the IS security resources variables (ISSETE, ISSEPO, ISSEHR, ISSERE) with each of the IS resources variables (ISTE, ISHR, ISRE) and the size (measured by the number of firm's employees); we also calculated the same partial correlations controlling for firm size
iv. Estimation of the following four regression models:

$$ISSETE = b10 + b11* SIZE + b12*ISTE + b13*ISHR + b14*ISRE$$

$$ISSEPO = b20 + b21* SIZE + b22*ISTE + b23*ISHR + b24*ISRE$$

$$ISSEHR = b30 + b31* SIZE + b32*ISTE + b33*ISHR + b34*ISRE$$

$$ISSERE = b40 + b41* SIZE + b42*ISTE + b43*ISHR + b44*ISRE$$

Also, before proceeding to steps iii and iv (calculation of correlations and estimation of regression models) for each of the above three composite IS resources variables (ISTE, ISHR, ISRE) and four composite IS security resources variables (ISSETE, ISSEPO, ISSEHR, ISSERE) we examined its uni-dimensionality through factor (principal components) analysis, and also its reliability by calculating its Cronbach's Alpha

value, based on its corresponding individual variables. For all seven composite variables, principal component analysis gave one component (based on the eigenvalues exceeding 1 criterion), on which individual variables had loadings exceeding 0.5; this indicates the uni-dimensionality of all the above composite variables. Also, the Cronbach's Alpha values of all seven composite variables exceeded 0.7, indicating acceptable reliability of them.

Results

In Table 2 we can see the correlations of the four IS security resources variables with the three IS resources variables and the size (** and * denote statistical significance at the 1% and 5% level respectively) in the first line of each cell; and, also, the same partial correlations controlling for firm size in the second line of each cell. All IS resources variables have strong medium to strong statistically significant positive correlations (simple and partial ones) with the IS security resources variables, with the IS human resources variable having in general the strongest ones, followed by the IS relationships variable. The size has statistically significant positive correlations with all IS security resources variables.

	ISTE	ISHR	ISRE	SIZE
ISSETE	0.281** 0.254**	0.448** 0.468**	0.362** 0.359**	0.205*
ISSEPO	0.382** 0.353**	0.445** 0.484**	0.398** 0.0.399**	0.257*
ISSEHR	0.445** 0.431**	0.648** 0.662**	0.535** 0.533**	0.140*
ISSERE	0.502** 0.484**	0.551** 0.606**	0.585** 0.551**	0.190*

Table 2. Correlations of IS security resources with IS resources and size

In Table 3 we can see (vertically) the four estimated models of the above step 4, having the four IS security resources variables as dependent variables, and the size and the IS resources variables as independent variables (the standardized regression coefficients are shown, with ** and * denoting statistical significance at the 1% and 5% level respectively). We can see that in all four models the coefficients of the IS human resources as well the size are statistically significant and positive (with the coefficients of the former being much larger than the ones of the latter); the coefficients of the IS relations are statistically significant and positive only in the IS security human resources and relations models. The coefficients of the IS technology are statistically non-significant in all four models. The examination of the correlations between the independent variables revealed the existence of high correlations between them, resulting in 'multi-collinearity problems' in these regression models, which are probably the reason for the above statistically non-significant. According to the econometric literature (e.g., Greene, 2011; Gujarati, 2008) if there are high levels of correlation between the independent variables of a regression, then the regression coefficients are not reliable estimates of the effects of the independent variables on the dependent variable. By estimating, again, the above four models, using one of the IS resources and the size as independent variable each time, the coefficients of all of them were positive and statistically significant, in agreement with the correlations of Table 2.

	ISSETE	ISSEPO	ISSEHR	ISSERE
SIZE	0.268*	0.281*	0.197*	0.201*
ISTE	-0.270	-0.075	-0.226	-0.035
ISHR	0.535**	0.412*	0.652**	0.440**
ISRE	0.196	0.180	0.271*	0.293*

Table 3. Regression models of IS security resource variables

The above results provide support of all our research hypotheses H1 – H4. They indicate that all three examined IS resources have positive impact on the development of IS security resources, with the IS human resources having the strongest effects, followed by the IS relationships, and then the IS technology. These indicate the importance of the 'soft ICT capital' (Arvanitis et al., 2013), consisting of

firm's IS personnel, and its relationships with firm's IT users, as well as external IT vendors and service providers, for the development of IS security technical, human and relational resources. Also, our results indicate that firm's size impacts positively the development of IS security resources.

Conclusions

The extensive investments made for the development of various IS within an organization, necessitate the balanced development of the information security safeguards for their protection. Practitioners have been arguing that information security investments are insufficient (E&Y, 2012; 2014). Researchers examined the factors influencing information security investments and they focused mainly on risk prevention factors and the potential impact of incidents, as the driving forces behind security investments (Longstaff et al., 2000). Regulatory compliance is also found to be determinant (Johnson, 2014). In this paper, the authors are interested to explore if other factors also contribute to the development of security resources; particularly factors deriving from the IS context of the organization. In order to achieve this aim an existing classification for IS resources from Ravichandran and Lertwongsatien (2005) has been used, as adapted by of Gu and Jung (2013). The authors then adapt the same classification for the information security resources, because literature lacks a framework for categorizing information security resources. Then, an empirical study for the relationship of the IS resources with the IS security resources is presented, in order to fill the research gap that the authors have identified regarding their relationship.

The results of this paper provide new contributions for researchers and practitioners as follows. First, our findings indicate the significant role of the IT staff for the development of information security in an organization. In order to handle IS in a secure way, IT human capital is the catalyst and the most important asset within an organisation. As it has also been argued by Huang and Kao (2006), the continuous training and the lifelong education are crucial for updating the necessary knowledge so as employees can follow and effectively encounter any violation. As human resources the authors also considered the role of employee's skills and abilities to learn new technologies, the existence of separate IT division, and their specialized knowledge. Human resources were found to positively influence all information security resources. Second, this research found that the IS security technology is not affected by investments in IS technology, as it would be expected, but instead it is mainly affected by the IS human capital. Thus, we realize that for the development of IS security, organizations do not invest more in the acquisition of technological solutions but the development of IT personnel leads to increased security resources. Third, the development of IS security policies was also affected by the IS human capital. We would expect that technical controls would be chosen by the organizations in order to enforce security policies, but instead we found that the IT personnel has a key role in the effective enforcement of security policies and strategies. Fourth, the internal and external partnership with regards to information security are also positively affected by the IS human resources and the IS partnership. This reveals the value of the IS human capital for the development of IS that not only functions according to the business mission, but also operates with information security considerations. Moreover, size constitutes an important determinant of information security adoption in an organization. Large firms have more resources and also the possibility to exploit economies of scale and scope, allowing them to invest on the security mechanisms, to support their employees on the continuous training, to recruit their units with specialized security personnel, capable to monitor both the internal and external relationships and sufficiently intervene; when necessary, to establish special security units, to name a few. Finally, this work offers a new classification for the information security resources, which is missing from the IS literature and thus it is expected that the information security researchers can benefit from.

Our study includes limitations mainly deriving from the source of empirical studies from Southern European countries. Southern European countries have similarities that led us to the justified decision to investigate our study in this region. On the other hand, our sample might limit the application of our results to other countries which may be significantly different, such as Northern Europe or North America. Future research may include further investigation in other countries and regions. Future work may also include the extension of our research model to other important IS aspects, such as privacy resources, that will further assist in a holistic view for the reasons driving top management to invest in protective resources for IS.

REFERENCES

AHIA, 2015. "IT Audit & Information Security Survey, Whitepaper Guidance for Healthcare Internal Auditors and Information Security Professionals", Available online at:
https://www.ahia.org/assets/Uploads/pdfUpload/WhitePapers/AHIAITAuditAndInformationSecuritySurvey.pdf.

Aiginger, K. (2013). "A new strategy for the European periphery" (No. 443). WIFO Working Papers.

Amit, R. and Schoemaker, P.J., 1993. "Strategic assets and organizational rent". *Strategic Management Journal*, 14(1), pp.33-46.

Arvanitis, S., Loukis, E. and Diamantopoulou, V., 2013. "The effect of soft ICT capital on innovation performance of Greek firms", *Journal of Enterprise Information Management* (26:6), pp. 679-701.

Barney, J.B., 2001. "Resource-based theories of competitive advantage: A ten-year retrospective on the resource-based view". *Journal of Management*, 27(6), pp.643-650.

Bharadwaj, A.S., 2000. "A resource-based perspective on information technology capability and firm performance: an empirical investigation". *MIS Quarterly*, pp.169-196.

Brecht, M. and Nowey, T. 2013. "A Closer Look at Information Security Costs", *The Economics of Information Security and Privacy*, In Böhme R. (Ed.) Springer Berlin Heidelberg, pp 3-24

CSI, 2008. "The latest results from the longest-running project of its kind", Computer Crime & Security Survey, Available online at:
http://www.sis.pitt.edu/jjoshi/courses/IS2150/Fall11/CSIsurvey2008.pdf

CSI, 2009. "CSI Computer Crime and Security Survey", Available online at:
http://www.personal.utulsa.edu/~james-childress/cs5493/CSISurvey/CSISurvey2009.pdf

Dierickx, I. and Cool, K., 1989. "Asset stock accumulation and sustainability of competitive advantage". *Management Science*, 35(12), pp.1504-1511.

E&Y, 2012. "Fighting to close the gap Ernst & Young's 2012 Global Information Security Survey", Available online at:
http://www.ey.com/Publication/vwLUAssets/GISS2012/$FILE/EY_GISS_2012.pdf

E&Y, 2014. "Get ahead of cybercrime EY s Global Information Security Survey" 2014, Available online at: http://www.ey.com/Publication/vwLUAssets/EY-global-information-security-survey-2014/%24FILE/EY-global-information-security-survey-2014.pdf

Gordon, L.A. and Loeb, M. 2002. "The economics of information security investment", *ACM Transactions on Information and System Security*, 5 (4), pp. 438–457

Grant, R.M., 1991. "The resource-based theory of competitive advantage: implications for strategy formulation". *California Management Review*, 33(3), pp.114-135.

Greene, W. H., 2011. "Econometric Analysis", New Jersey: Prentice Hall Inc.

Gu, J.W. and Jung, H.W., 2013. "The effects of IS resources, capabilities, and qualities on organizational performance: An integrated approach". *Information & Management*, 50(2), pp.87-97.

Gujarati, D. N., 2008. "Basic Econometrics", New York: Mc-Graw Hill Higher Education.

Huang, S., Lee, C. and Kao, A., 2006. "Balancing performance measures for information security management - A balanced scorecard framework", *Industrial Management & Data Systems*, 106 (2), pp. 242 – 255

ISACA, 2015. "State of Cybersecurity: Implications for 2015 An ISACA and RSA Conference Survey", Available online at:
http://www.isaca.org/cyber/documents/state-of-cybersecurity_res_eng_0415.pdf

ISO 27000, 2016. "Information technology — Security techniques — Information security management systems — Overview and vocabulary, International Standardisation Organization"

ISO 27001, 2013. "Information technology – Security techniques – Information security management systems – Requirements, International Standardisation Organization"

Johnson, M.A., 2014. "Business and security executives views of information security investment drivers: Results from a Delphi study*", Journal of Information Privacy and Security*, 5 (1), pp. 3-27

Landesmann, M.A., 2015. "The New North–South Divide in Europe: Can the European Convergence Model be Resuscitated?" The Triple Challenge for Europe: Economic Development, Climate Change, and Governance, p.60.

Laudon K. and Laudon, J. P., 2016. *Management Information Systems: Managing the Digital Firm*, Pearson, 16th Edition

Law, K.S., Wong, C.S. and Mobley, W.M., 1998. "Toward a taxonomy of multidimensional constructs". *Academy of Management Review*, 23(4), pp.741-755.

Liang, T.P., You, J.J. and Liu, C.C., 2010. "A resource-based perspective on information technology and firm performance: a meta analysis". *Industrial Management & Data Systems*, 110(8), pp.1138-1158.

Longstaff, T. A., Chittister, C., Pethia, R. and Haimes, Y. Y., 2000. "Are we forgetting the risks of information technology?" *IEEE Computing*, 33 (12), pp. 43–51.

Mata, F.J., Fuerst, W.L. and Barney, J.B., 1995. "Information technology and sustained competitive advantage: A resource-based analysis". *MIS Quarterly*, pp.487-505.

Melville, N., Kraemer, K. and Gurbaxani, V., 2004. "Review: Information technology and organizational performance: An integrative model of IT business value". *MIS Quarterly*, 28(2), pp.283-322.

Nevo, S. and Wade, M.R., 2010. "The formation and value of IT-enabled resources: antecedents and consequences of synergistic relationships". *MIS Quarterly*, pp.163-183.

NIST, 2008. "Performance Measurement Guide for Information Security", NIST Special Publication 800-55 Revision 1, Available online at:
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-55r1.pdf(Accessed 26/02/2017)

PWC Survey, 2016. "Turnaround and transformation in cybersecurity, The Global State of Information Security®", Available online at: http://www.pwc.com/sg/en/publications/assets/pwc-global-state-of-information-security-survey-2016.pdf

PWC Survey, 2017. "Moving forward with cybersecurity and privacy – How organizations are adopting innovative safeguards to manage threats and achieve competitive advantages in a digital era, Key findings from The Global State of Information Security", Available online at: https://www.pwc.com/gx/en/information-security-survey/assets/gsiss-report-cybersecurity-privacy-safeguards.pdf

Ravichandran, T. and Rai, A., 2000. "Quality management in systems development: an organizational system perspective". *MIS Quarterly*, pp.381-415.

Ravichandran, T., Lertwongsatien, C. and LERTWONGSATIEN, C., 2005. "Effect of information systems resources and capabilities on firm performance: A resource-based perspective". *Journal of Management Information Systems*, 21(4), pp.237-276.

Ross, J.W., Beath, C.M. and Goodhue, D.L., 1996. "Develop long-term competitiveness through IT assets". *Sloan Management Review*, 38(1), p.31.

Sans Institute, 2010. "Measuring effectiveness in Information Security Controls", SANS Institute InfoSec Reading Room, Available at: https://www.sans.org/reading-room/whitepapers/basics/measuring-effectiveness-information-security-controls-33398 (Accessed 26/02/2017)

Schumacker, R.E and Lomax, R. G., 2016. *A beginner's guide to structural equation modeling*, Fourth Edition. New York, NY: Routledge Academic

Skaggs, B.C. and Youndt, M., 2004. "Strategic positioning, human capital, and performance in service organizations: A customer interaction approach". *Strategic Management Journal*, 25(1), pp.85-99.

Sun, Y., Fang, Y., Lim, H.K. and Straub, D., 2012. "User Satisfaction with Information Technology Service Delivery: A Social Capital Perspective", *Information Systems Research* 23(4), pp. 1195-1211

Torres, J. M., Sarriegui, J.M., Santos, J. and Serrano, N., 2006. "Managing Information Systems Security: Critical Success Factors and Indicators to Measure Effectiveness", in *Proceedings of the 9th International Conference* Katsikas, S., López, J., Backes, M., Gritzalis, S. and Preneel, B. (Eds.), ISC 2006, Samos Island, Greece, pp 530-545

Wade, M. and Hulland, J., 2004. "Review: The resource-based view and information systems research: Review, extension, and suggestions for future research". *MIS Quarterly*, 28(1), pp.107-142.

Wang, J., Chaudhury, A. and Rao, H.R., 2006. "A Value-at-Risk Approach to Information Security Investment", Information Systems Research, Vol. 19 (1), pp. 106 - 120

Wong, K.K.K., 2013. "Partial least squares structural equation modeling (PLS-SEM) techniques using SmartPLS". *Marketing Bulletin*, 24(1), pp.1-32.