Antecedents of Optimal Information Security Investment: IT Governance Mechanism and Organizational Digital Maturity

Samuel Okae, Francis Kofi Andoh-Baidoo, Emmanuel Ayaburi

Antecedents of Optimal Information Security Investment: IT Governance Mechanism and Organizational Digital Maturity

Samuel Okae[1], Francis Kofi Andoh Baidoo[2] and Emmanuel Ayaburi[2]

[1] Nobel International Business School, Accra, Ghana
[2] University of Texas Rio Grande Valley, 1201 W University Dr, Edinburg, TX, 78539, USA
[2]francis.andohbaidoo@utrgv.edu

Abstract. Information security risk is of concern to both researchers and practitioners. In this study, we investigate the antecedents of optimal information security investment from organizational perspective using the concept of information technology governance. Specifically, we examine how board attributes including IT savviness, board duality, experience, and functional debate along with an organizational attribute, digital maturity, influence optimal information security investments. Data was collected from board members in organization to test the research model. Our results offer both theoretical and practical implications.

Keywords: Digital-maturity, Board, Dysfunctional, Duality, IT-Savviness, Optimal security investment

1 Introduction

Information security incidents worldwide have attracted attention of organizations and researchers since the effects on the associated institutions are disastrous (Kozak, 2005). The 2014 JPMorgan Chase data breach is a classic case of a disastrous information security incident. This attack is believed to have compromised over 83 million of the bank's accounts affecting 76 million households and 7 million businesses in the United States (Ponemon Institute, 2015). Addressing information security risks demands making optimal security investments in key technologies to protect the organization. Prior studies that have examined optimal information security investments employed analytical methods (e.g., Gordon & Loeb 202; Huang, Hu, & Behara, (2006)) with little emphasis on how organizational factors such as governance culture may play a critical role. Specifically, little is known about which attributes of organization's governing board affect how funds are allocated for security investment.

Board IT governance has been found to be critical for the success of information security programs (FFIEC, 2017). Board IT governance involves the decision and strategy of board of directors in ensuring that they distribute firm resources judiciously (Heenetigala, 2011). Board of directors needs to ensure resources available to the firm are distributed in a manner that will yield optimal results to serve organizational aims and objectives. In deciding how firm's resources are to be distributed, the board must

consider the extent to which organizational resources should be invested in critical functions such as information security. Board with inadequate information security knowledge, may ask the wrong question about IT risks and expense (Nolan & McFarlan, 2005). This ultimately makes the board incapable of fulfilling their oversight responsibilities, exposing the firm to security threats. Given that the characteristics of the board are likely to affect the decisions they make, this issue bears an examination (Jensen 1995; Zahra and Pearce 1989). Thus, the purpose of the current study is to investigate which Board IT governance and organizational attributes influence optimal information security investment. We argue in this study that, having a well composed IT savvy board of directors could be one way to improve the board's decision-making regarding information security implication.

To investigate the research problem, we deploy the concept of Board IT governance (Jewer et al., 2012), to develop a model that explicates antecedents to optional IT security investment. Data was collected from the upper level managers in the banking industry in a developing country to test the model. The financial industry is a suitable target for most hackers and cyber criminals, and the industry has experienced increased average cost of information security data breach (Mohammed, 2017). The results of our analysis demonstrate that while digital maturity plays an important role in firms' decision to invest in optimal information systems not all characteristics of the board members are a good predictor of such a decision. Based on our results, we offer both theoretical and practical investments.

2 Theoretical Foundation and Hypotheses

Some scholars have studied information security investments with the focus on optimal investment. Gordon & Loeb (2002) address information security investments by building a model that helps to determine how much organizations must invest in information security. Huang, Hu, & Behara (2006) also developed a model for information security investments that deal with simultaneous attacks from multiple external sources. These studies employed analytical models. However, to make the necessary investment in IT, the board needs to be convinced. Several economic, strategic, technological, operational, and environmental factors inform firms' decision to invest in information security (Gordon & Loeb, 2002). The economic or financial factors consider the budgetary allocations firms are ready and are able to make considering the structures at risk of being corrupted or lost if such actions are not taken to protect them in the short to long term (Johnson, 2009). The organizational factors consider firms' contextual view prompting their investments in information security. The firm's organizational factors also consider operational factors that look at how existing and new IT structures will be used strategically, either exploratively or exploitatively in the protection of clients' and firms' information. The technological factors look at the technological capability of firms, the human resources available to operate and maintain information security structures when investments are made in this area (Tatsumi & Goto, 2010). The environmental factors affecting investment in information security include firms' identified strengths, weaknesses, threats and identified opportunities when investment is made in information security investment. However, the human factor is considered a critical

management input necessary for effective information security (Soomro et al., 2016; Chang and Ho 2006). This study investigates how a management factor, Board IT governance, influence optimal IT investment from governance perspective.

Board Information Technology Governance

Board governance makes up the integral part of corporate governance by implementing processes, relational mechanisms, and structures within the firm which allow individuals to execute their expectations in backing up IT business value (Wilkin & Chenhall, 2010). Most organizations have IT governance. However, institutions with efficient governance team have set of active IT structural mechanisms such as committees, procedures and plans which are consistent in promoting actions in line with the firms' strategies and values. Board Information Technology governance refers to current and formal frameworks which provide structures to ensure that IT investment strategy is aligned with organizational strategy (Pereira & Da Silva, 2012). IT governance is a structure of technologically based institutional arrangements that affects the decision-making and the framework adopted by the institutions. It emerged as a fundamental business imperative because it is key to realizing the value of IT in today's business. IT governance must consider and implement the most effective and secure structure for its effectiveness. It should adopt a defined process as any undefined actions lead to vulnerability of the system to attackers. Using Board IT governance as the theoretical basis, Jewer et al., (2012) examine how board attributes, a governance mechanism, influence organizational strategic choice. The board attributes investigated include proportion of insiders, board size and board IT competence. In this study, we use board composition (duality, dysfunctional level of debate, and experience of board members) and IT savviness to represent proportion of insiders and board IT competence respectively. Board IT governance is the system and procedure put in place to ensure that an organization is efficient in the application of IT, in achieving the set objectives of an organization OECD (2004). IT governance considers oversight processes and the responsibilities of the management (Brisebois, Boyd, & Shadid, 2007). Most organizations approach IT governance from the perspective of tool or procedures (Allen, 2005). Allen (2005) argues that the likelihood of the success of IT governance procedures largely depends on certain principles. One of these identified principles is executive support. The support of the board is fundamental to the success of launching an idea in the organization. The initiatives that are adopted are often because the board can relate the IT initiative to organizational goals and appreciate how such initiative will be beneficial to the organization (OECD, 2004). Another factor is the composition of the board which includes experience, duality and functional debate of the board members (Zahra and Pearce 1989).

Practical board IT governance sets apart unique assets in the firm for IT use and at the same time ensures that the organization complies with the overall principles of mission and vision. In this regard, a firm with efficient IT governance will ensure that its personnel have IT skills, IT processes, IT knowledge assets and experience. Though there is a strong argument for more board involvement in IT governance, Andriole (2009) found that boards of directors were alarmingly uninvolved in the planning or oversight of technological initiatives and were increasingly out of the loop with regards

to these initiatives. The study found that because of this the various boards included in the study were missing prospects to enhance and optimize their technological investments. For IT issues, boards should be involved in decision making especially on the systems that the company uses. This study seeks to determine how IT governance structures and processes influence the relationship between board composition and information security investments. Specifically, we investigate significant organizational strategic choice, optimal security investment decision which comprises economic or financial factors considered in the budgetary allocations firms make with regard to the structures at risk of being corrupted or lost if such actions are not taken to protect them in the short to long term (Johnson, 2009).Organizations with effective IT governance are likely to carve out competitive advantage regarding technological decisions (Allen, 2005). According to Weill (2004), most organizations have information Technology governance. However, institutions with efficient governance team have set of active information technology structural mechanisms such as committees, procedures and plans which are consistent in promoting actions in line with the firms' strategies and values (Weill, 2004).

Board's IT Savviness and Optimal Information Security Investment

Board IT savviness can be described as the level of IT knowledge possessed by board members. An IT-savvy board is considered to have enough technical knowledge regarding IT issues. This study proposes that more IT savviness of board members improves the board's understanding and appreciation of technological issue particularly in the domain of information security and would thus be able to make good information security investment decisions. Ensuring a more efficient and effective IT governance structures and information security investments would be easier if the board, who control the organization's resources and set policy, were IT savvy. Harrison et al. (1997) found that the executives' perceptions of the usefulness of IT initiatives was a major factor in their decision making. However, it can be argued that without enough level of literacy, it would be difficult for a board member to appreciate that usefulness or benefits of information security initiatives and how investing in them could assist in achieving the organizations' strategic goals. IT savviness, also referred to as IT competence (Jewer et al., 2012), can be considered as an attribute of board members that would impact their decision making particularly regarding IT related issues. IT experience at the board level can help guide management through changes in the business environment. It would be prudent for firms to have IT-savvy members on the board to enrich boardroom discussion on IT investments (Nolan & McFarlan, 2005). By asking the appropriate questions, directors can make the right decisions to improve their businesses and protect the company's integrity and brand. Thus, we posit that:

H_1: Board IT savviness has a positive effect on optimal information security investments.

Board Composition and Optimal Information Security Investment

Another board characteristic that could potentially influence members' decision making is the composition of the board. Board composition factors such as experience, duality and level of functional debate play a critical role in its governance culture (Zahra

& Pearce, 1989). Our first board composition factor, Board duality, is a corporate leadership structure that merges the position of board chair and CEO. A single person holding both the Chairman and CEO role improves the value of a firm as the agency cost between the two is eliminated (Alexander, Fennell and Halpern, 1993). However, CEO duality can lead to worse performance as the board cannot remove an underperforming CEO and can create an agency cost if the CEO pursues his own interest at the cost of the shareholders (White and Ingrassia, 1992). Hermalin & Weisbach (1988) argue that often the context or environment that the company finds itself in will determine the extent of board duality. Their findings showed that firms tended to recruit directors from within the firm when a CEO was nearing the end of his or her tenure and often chose a new CEO from the new batch of a board member. On the other hand, their study found that when a firm or organization had had to withdraw from a market or was performing poorly, board members tended to be recruited from outside the organization. There is still debate in the literature about the effectiveness of outsider-dominated boards against insider-dominated boards. This study examines the role that duality plays in influencing the optimal information security investment.

The second component of board composition that this study will considere is the level of debate which Forbes & Milliken, (1999) describe as board cohesiveness. The authors define this as the board members' ability to work with each other and their motivation to remain on the board. This refers to the level of affection or level of willingness to work together. For the purposes of this study, high levels of cohesiveness will be considered functional debate. Gabrielsson et al. (2007) argue that board members tend to make more meaningful contribution when in situations of high cohesion since they believe their inputs are valued than when faced with situations of low cohesion among the board members.

The final component of board composition considered in this study is experience. The literature generally agrees that the experience of board members is an important factor that influences the positions that board members take and the choices they make when faced with strategic and policy decisions (Westphal & Milton, 2000). The experience of individual board members acts as a mix of competencies and capabilities that help in executing the governance function. Therefore, putting together we posit that:

H_{2A}: The duality of the board members has a positive effect on optimal information security investments.

H_{2B}: The level of functional debate among board members has a positive effect on optimal information security investments.

H_{2C}: The experience of the board members has a positive effect on information security investments.

Digital Maturity and Optimal Information Security Investment

Digital maturity of a firm is the degree to which the firm has used technology and its capabilities to engage its employees, enhanced its operation and develop new business (Kane et al., 2017). Digital maturity enables an organization to deploy digital innovations and to achieve enterprise-wide transformation (Kane et al., 2015). Digital maturity measures the intensity at which digital technologies are deployed in an organization and how leadership and employees are transformed through the creation of

management capabilities that effectively facilitate digital transformation (Valentine & Stewart, 2015). Digital maturity dictates the need to invest in innovative information technologies and build competencies in IT skills, IT knowledge and to transform business processes. An organization's digital maturity will influence how information security risks are addressed through the right information security investments even as they continue to deploy innovative technologies. Hence considering digital maturity as a valuable resource it will influence the extent to which limited resources are dedicated to information security. Thus, we suggest that:

H3: The degree of digital maturity of the firm is positively related to optimal investments in information security positively.

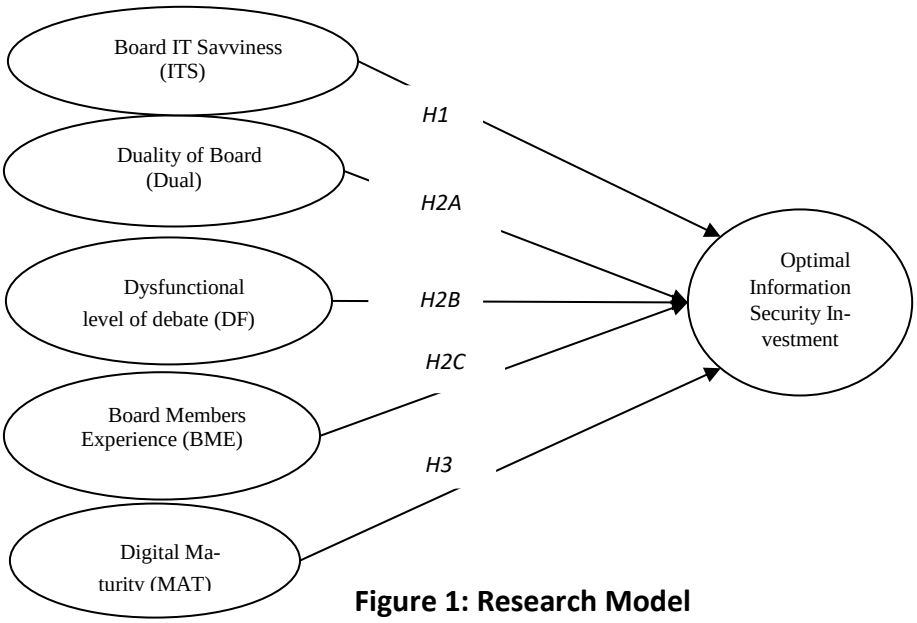

Figure 1: Research Model

3 Methodology

Measures and Sample

This study was conducted using a survey research design. The target population of the study comprises of individuals who are part of the top management team in their organization. The actions of top management are affected by decisions of board managements. These individuals have huge responsibilities in deciding how the firms' resources are utilized and are task with protecting investors. Our sample included 100 respondents. The sampling techniques used in this study are cluster sampling, convenient sampling, and snowball sampling approach. The current study used prior validated measures; Digital Maturity (MAT), Board Members Experience (BME), Dysfunctional level of debate (DF), Duality of Board (Dual), Board IT Savvi-ness (ITS) and optimal security investment (Huang, Behara and Goo, 2014: Massey and Dawes, 2007).

In this study, only the quantitative method was used to empirically test the relationship between the study constructs. We obtained 100 usable responses from our target population. Dawson (2002) noted that the use of a quantitative method and a case study ensure collection of rich data and provide the researcher with the opportunity to maintain a detached, objective view in order to understand the responses as the use of this method requires minimal contact with the respondents

Analysis

The Structural Equation Modeling (SEM) was used to investigate the casual paths hypothesized in this study. A two-step approach was used to analyze the data. In the first step, the covariance-based technique was used to assess the appropriateness of the measurement model. The covariance-based technique was used as it minimizes the differences between the covariance of the collected sample and that of the ones predicted by the model and reproduces the covariance matrix of the observable variable (Chin and Newsted, 1999). For testing the structural model, Variance based partial least square (PLS) SEM was used as it maximizes the variance of the dependent variable which is explained by the independent variables (Hair et al., 2014).

Results

We used the composite reliability and Average Variance Extracted (AVE) to test for reliability and validity of the constructs. Convergent validity was demonstrated by large factor loadings (0.70 or above) for all constructs (Hair et al., 2014). Discriminant validity of each latent construct was tested by the method recommended by (Fornell & Larcker, 1981). The square root of AVE of each construct (diagonal of Table 1) should be higher than the correlation between that construct and any other constructs. This criterion is satisfied by all latent constructs. The composite reliability was noted to be above 0.70 for most constructs. Therefore, our measurement model exhibits sound reliability and validity necessary for further testing of the research hypotheses.

Table 1. Construct Validity

	CR	AVE	(1)	(2)	(3)	(4)	(5)	(6)
BME(1)	0.71	0.58	0.76					
DF(2)	0.95	0.86	-0.43	0.93				
Dual(3)	0.75	0.51	-0.16	0.04	0.71			
ITS(4)	0.87	0.72	0.23	-0.20	-0.11	0.85		
Invest(5)	0.64	0.40	0.35	-0.17	-0.11	0.35	0.63	
MAT(6)	0.83	0.62	0.19	-0.17	-0.04	0.34	0.35	0.78

We conducted model robustness checks for multicollinearity. VIF values for BM (1.29), DF (1.24), Dual (1.04), ITS (1.18) and MAT (1.15) were much less than the threshold of (VIF < 10), indicating absence of multicollinearity problem. In assessment of the explanatory power, our model accounted for about 25% of variance ($R^2 = 0.248$) in explaining the likelihood of making optimal decision in investing in information security in the firm. The Adjusted- R^2 (0.2018) further strengthens the explanatory power

as it takes into account our sample size and number of variables in our model (Hair et al. 2010). Summary of the hypotheses testing are depicted in Table 2 and Figure 2.

Table 2. Results

Path	**Coef.**	**t-Stat**	***P* Values**	**Supported?**
BME -> Invest	0.271	1.988	0.047	Yes
DF -> Invest	0.031	0.247	0.805	No
Dual -> Invest	-0.035	0.246	0.806	No
ITS -> Invest	0.207	2.052	0.040	Yes
MAT -> Invest	0.234	2.093	0.037	Yes

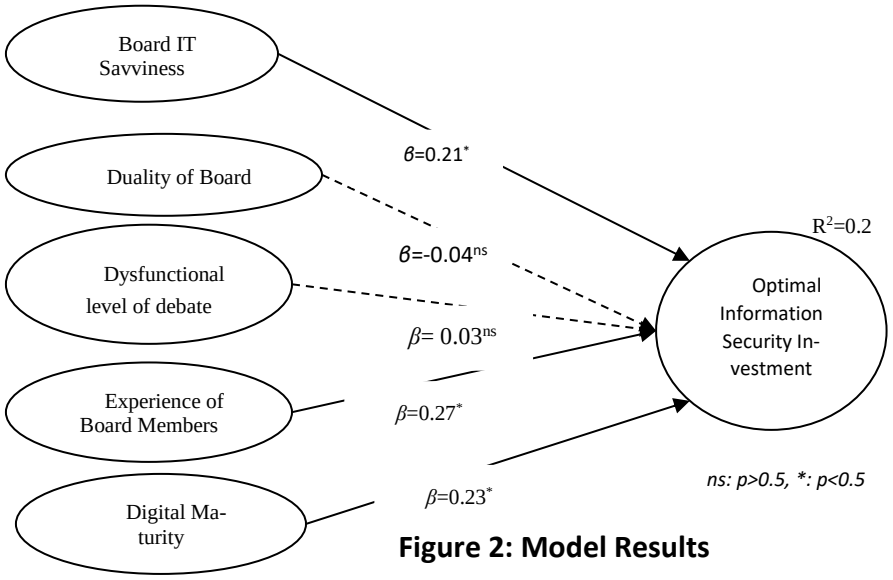

Figure 2: Model Results

As hypothesized, BME was shown to be a good predictor of optimal investment in information systems security (β=0.27*, $p < 0.05$; t= 1.99), as well as the hypothesized positive relationship between ITS and MAT and optimal investment in information systems security (β=0.21, $p < 0.05$; t=2.05 and β=0.23, $p < 0.05$; t=2.09 respectively). However, no support was found for the relationship between DF and Dual, and optimal investment in information security (β= 0.03, $p > 0.05$; t= 0.25 and β= 0.04, $p > 0.05$; t= 0.25 respectively).

Discussion and Future Research Direction

The advancement of information technology (IT) has brought about rapid changes in businesses operations. However, the use of IT is associated with information risks (Dangolani, 2011). Information security risk is defined in this study as the risk that arises when the firm's information assets and information systems are not protected

sufficiently against various kinds of damage or loss (Straub & Welke, 1998). Board of board have responsibility to provide resources to ensure that information security risks are minimized. However, to ensure the growth of businesses, corporate boards need to make concerted effort to distribute their resources judiciously. This calls for optimal information security investment. We argue that board characteristics (IT Savviness, composition) and organizational digital maturity will influence organization's optimal information security investments. Only one of the hypotheses relating the dimensions of board composition, i.e., experience was supported. Level of functional debate and duality of board members were not supported. Both IT savviness and digital maturity were also supported.

Implication

Our results offer several theoretical and practical implications. For theory, we have demonstrated how Board IT governance can enable optimal information security investment using the banking sector as a context. The proposed theoretical model or variant can be tested in other contexts to expand our understanding of IT governance and information security investments. We also demonstrated that the digital maturity of a firm influences board of directors' decision to optimally invest in information security. For managerial, since business executives are more likely than security executives to view information security as a cost center rather than a business enabler, our results indicate a greater need for board members with skills and knowledge in IT issues to better understand information security investments. This is important because according to the 2017 Cybercrime Report, Cybersecurity Ventures predicts cybercrime will cost the world in excess of $6 trillion annually by 2021 (Morgan, 2017). In 2017, cybercrime is estimated to have caused $450 billion in damages worldwide (Thornton, 2017). Businesses must protect their systems in order to avoid these damages by ensuring vulnerabilities are reduced (Gartner, 2016). Specifically, organizations must consciously invest in various security technologies such as data loss prevention, spyware detection, removal applications and cryptographic techniques to protect systems, data and processes against technical failure, damage or attacks (Gartner, 2016). Second, in general, the study highlights the need for more dialogue and information sharing between security executives, who are responsible for designing the organization's security infrastructure, and business executives who must allocate the funds to support that infrastructure. For example, in 2016, Thomson Reuters (2015) reported that the U.S. government had reserved $14 billion of its budget proposal for cybersecurity efforts to protect federal and private networks. Johnson (2009) affirms this and argues that firms invest in information security for different reasons.

4 REFERENCES

1. Allen, J. H. (2005). Governing for Enterprise Security (GES), Implementation Guide: Characteristics of Effective Security Governance1. USA: Carnegie Mellon University. 5-7.
2. Andriole, S. J. (2009). Boards of Directors and Technology Governance : The Surprising State of the Practice Boards of Directors and Technology Governance : The

Surprising State of the Practice I . Boards And Technology Governance. Fortune, 24(March), 373–394.
3. Brisebois, R., Boyd, G., & Shadid, Z. (2007). What is IT Governance and why is it important for the IS auditor. The INTOSAI IT Journal, (25), 30–35.
4. Chang, S. E., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. Industrial Management and Data Systems (Vol. 106).
5. Chin, W. W., Marcolin, B. L., & Newsted, P. R. (2003). A partial least squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation study and an electronic-mail emotion/adoption study. Information Systems Research, 14(2), 189–217.
6. Dangolani, S. K. (2011). The Impact of information technology in banking system (A case study in Bank Keshavarzi IRAN). Procedia-Social and Behavioral Sciences, 30, 13–16.
7. Daniel P . F. and Frances J . (1999). The Academy of Management Review, Vol . 24 , No . 3, pp . 489-505. The Academy of Management Review, 24(3), 489–505.
8. FFIEC. (2017). FFIEC Updates Cybersecurity Expectations for Boards. Retrieved December 25, 2017, from https://www.bankinfosecurity.com/ffiec-management-booklet-a-8683.
9. Forbes, D. P., & Milliken, F. J. (1999). Cognition and Corporate Governance : Understanding Boards of Directors as Strategic Decision-Making.
10. Fornell, C., & Larcker, D. F. (1981). Structural equation models with unobservable variables and measurement error: Algebra and statistics. Journal of Marketing Research, 382–388.
11. Gabrielsson, J., Huse, M., & Minichilli, A. (2007). Understanding the Leadership Role of the Board Chairperson Through a Team Production Approach. International Journal of Leadership Studies, 3(1), 21–39.
12. Gartner. (2016). Magic Quadrant for Content-Aware Data Loss Prevention. G00277564, (January 2016).
13. Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. ACM Transactions on Information and System Security, 5(4), 438–457.
14. Hair Jr, J. F., Anderson, R. E., Tatham, R. L., & William, C. (1995). Multivariate data analysis with readings. New Jersy: Prentice Hall.
15. Harrison, D. A, Mykytyn Jr., P. P., & Riemenschneider, C. K. (1997). Executive Decisions About Adoption of Information Technology in Small Business: Theory and Empirical Tests. Information Systems Research, 8(2), 171.
16. Heenetigala, K. (2011). Corporate Governance Practices and Firm Performance of Listed Companies in Sri Lanka. Corporate Governance, (April).
17. Hermalin, B. E., & Weisbach, M. S. (1988). The Determinants of Board Composition. RAND Journal of Economics, 19(4), 589–606.
18. Huang, C. D., Hu, Q., & Behara, R. S. (2006). Economics of Information Security Investment in the Case of Simultaneous Attacks Economics of Information Security Investment in the Case of Simultaneous Attacks. Information Security, (Weis 2006).
19. Jewer, J., & McKay, K. N. (2012). Antecedents and consequences of board IT governance: Institutional and strategic choice perspectives. Journal of the Association for Information Systems, 13(7), 581.

20. Johnson, A. M. (2009). Business and security executives views of information security investment drivers: Results from a Delphi study. Journal of Information Privacy & Security, 5(1), 3–27.
21. Kane, G. C., Palmer, D., Nguyen-Phillips, A., Kiron, D., & Buckley, N. (2017). Achieving digital maturity. MIT Sloan Management Review, 59(1).
22. Kane, G. C., Palmer, D., Phillips, A. N., & Kiron, D. (2015). Is Your Business Ready for a Digital Future? MIT Sloan Management Review, 56(4), 37–44.
23. Kozak, S. (2005). The role of information technology in the profit and cost efficiency improvements in the banking sector. Journal of Academy of Business and Economics, 2(1), 34–38.
24. Massey, G. R., & Dawes, P. L. (2007). The antecedents and consequence of functional and dysfunctional conflict between marketing managers and sales managers. Industrial marketing management, 36(8), 1118-1129
25. Mohammed, A. A. (2017). Ghanaian Banks Systems at Risk of Cybercrime—Cyber Security Expert.
26. Morgan, S. (2017). 2017 Cyber Ventures Cybercrime Report. Cybersecurity Ventures, 14.
27. Nolan, R., & McFarlan, F. (2005). Information technology and the board of directors. Harvard Business.
28. Pereira, R., & da Silva, M. M. (2012). IT governance implementation: The determinant factors. Communications of the IBIMA, 2012, 1.
29. Ponemon Institute. (2015). Cost of Data Breach. Ponemon Institute, (May), 1–30.
30. Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. International Journal of Information Management, 36(2), 215–225.
31. Straub, D. W., & Welke, R. J. (1998). Coping with Systems Risk: MIS Quarterly, (404), 441–469.
32. Tatsumi, K., & Goto, M. (2010). Optimal timing of information security investment: A real options approach. In Economics of Information Security and Privacy (pp. 211–228). Springer.
33. Thornton, G. (2017). Locking down the value of data Contents: Executive summary.
34. Valentine, E., & Stewart, G. (2015, January). Enterprise Business Technology Governance: Three competencies to build board digital leadership capability. In 2015 48th Hawaii International Conference on System Sciences (pp. 4513-4522). IEEE.
35. Westphal, J. D., & Milton, L. P. (2000). How Experience and Network Ties Affect the Influence of Demographic Minorities on Corporate Boards. Administrative Science Quarterly, 45(2), 366–398.
36. Zahra, S. A., & Pearce, J. A. (1989). Boards of Directors and Corporate Financial Performance: A Review and Integrative Model. Journal of Management, 15(2), 291–

Appendix: Crossloadings

	BM	DF	Dual	ITS	Invest	MAT
BME1	0.471	-0.404	-0.035	0.005	0.101	-0.020
BME2	0.969	-0.360	-0.168	0.246	0.361	0.212
DF1	-0.390	0.899	0.041	-0.201	-0.077	-0.088
DF2	-0.420	0.958	0.061	-0.215	-0.193	-0.226
DF3	-0.382	0.920	0.009	-0.132	-0.145	-0.093
DUAL1	-0.120	-0.013	0.755	-0.069	-0.078	-0.010
DUAL2	0.095	-0.136	0.557	-0.066	-0.039	0.042
DUAL4	-0.201	0.127	0.806	-0.106	-0.104	-0.076
INVEST1	0.233	-0.201	-0.128	0.309	0.778	0.286
INVEST3	0.180	-0.192	-0.275	0.031	0.310	-0.014
INVEST5	0.271	0.004	0.040	0.222	0.698	0.269
ITS2	0.166	-0.247	-0.097	0.862	0.294	0.285
ITS4	0.166	-0.194	-0.108	0.887	0.264	0.221
ITS6	0.233	-0.067	-0.090	0.797	0.314	0.342
MAT1	0.267	-0.138	-0.073	0.391	0.383	0.898
MAT3	0.105	-0.172	-0.072	0.181	0.186	0.732
MAT5	-0.045	-0.084	0.088	0.122	0.177	0.710