Six Board Roles for Information Security Governance

Sara Nodehi[a], Tim Huygh[b] and Laury Bollen[c]
Information Science, Open University, Heerlen, The Netherlands

Keywords: Information Security (InfoSec), Board of Directors, Governance, Accountability.

Abstract: As cyber threats evolve, board engagement is becoming increasingly essential to ensure Information Security (InfoSec) is integrated into an organization's strategic fabric, ensuring the protection of business value. Only through board-level active participation can the organization develop a security-conscious culture. Ultimately, board commitment to InfoSec helps reduce risks, maintain stakeholder trust, and ensure long-term success. However, little is yet known about the board's exact role in Infosec. Leveraging a framework from corporate governance literature identifying board roles, and drawing parallels with extant InfoSec literature, this paper explores board-level involvement in InfoSec in greater depth, leading to the identification and description of the board of directors' roles in this context. Moreover, the paper identifies a future research agenda to be pursued in an empirical setting to contribute to the growth of knowledge regarding board-level InfoSec governance.

1 INTRODUCTION

In this era of increasingly complex and interconnected technologies, addressing InfoSec issues requires more senior management and board involvement (Girn, 2022). The ability of senior managers and boards to assess a company holistically and implement new processes in a timely manner has led academics to advocate that effective security policies should be developed at the top rather than by the InfoSec department, typically spearheaded by a Chief Information Security Officer (CISO) (McFadzean et al., 2007). While several papers such as Bobbert and Mulder (2015); Larcker et al. (2017); McFadzean et al. (2007); Williams (2007) suggest that the involvement of the board of directors is necessary for adequate InfoSec governance, the literature regarding the role of the board of directors in InfoSec is limited and no literature to date explicitly discusses how the board of directors should act and what their exact roles are. While InfoSec literature does discuss board-level aspects, it is often passingly mentioned, leading to fragmented insights on board-level Infosec governance throughout the InfoSec literature. To understand the board's potential role in InfoSec theoretical pluralism is necessary, as this role may span technology, human behavior, legal and regulatory aspects, risk management, and more (Bolourian et al., 2021; Попов & Макеева, 2022). In other words, multiple theories may be relevant as a lens to develop a good and complete understanding of the multi-faceted concept of board-level InfoSec governance.

As opposed to InfoSec literature, corporate governance literature has put a significant emphasis on the role of the board of directors. According to Nicholson and Newton (2010), there is a wide range of ways in which researchers such as Mintzberg (1983), Hillman and Dalziel (2003), Zahra and Pearce (1989), and Hung (1998) conceptualize the board's role set in governance. Hence, in the first stage of this research, we explored existing models on the role of the board of directors that have been discussed in corporate governance literature and analyzed their suitability for defining and describing board roles in the context of InfoSec.

While discussing these competing models is out of scope for this short paper, we settled to draw on Hung (1998)'s model for two major reasons. First, it considers both an institutional and contingency

[a] https://orcid.org/0000-0002-2919-1336
[b] https://orcid.org/0000-0003-4564-7994
[c] https://orcid.org/0000-0001-6475-7561

Nodehi, S., Huygh, T. and Bollen, L.
Six Board Roles for Information Security Governance.
DOI: 10.5220/0012695900003690

In *Proceedings of the 26th International Conference on Enterprise Information Systems (ICEIS 2024) - Volume 2*, pages 713-720
ISBN: 978-989-758-692-7; ISSN: 2184-4992

perspective, which both are relevant in an InfoSec context, and second, the model satisfies the abovementioned need for theoretical pluralism by discussing the board roles using six well-known (managerial) theories (i.e., Resource Dependency Theory (RDT), Stakeholder Theory, Agency Theory, Stewardship Theory, Institutional Theory, and Managerial Hegemony). As such, this model creates a solid foundation for identifying six potential roles of the board of directors in the field of InfoSec, rigorously grounded in theory.

Drawing upon the seminal corporate governance model advanced by Hung (1998), our current scholarly inquiry undertakes a comprehensive exploration of the multifaceted dimensions of board involvement in InfoSec initiatives. Rooted in established managerial paradigms, the study delineates six distinct roles assumed by boards in the realm of InfoSec, leveraging insights gleaned from extant InfoSec literature. As a result of a systematic analysis based on theoretical foundations, each role is meticulously analyzed, revealing nuanced insights into the mechanisms boards can use to mitigate cyber threats and strengthen organizational resilience. Thus, this investigation endeavors to enrich our understanding of the intricate interplay between board dynamics and InfoSec governance, thereby furnishing a conceptual framework that elucidates the imperative of board engagement in safeguarding the digital infrastructure of modern enterprises.

The remainder of the paper successively discusses each of these roles as identified by Hung (1998)., This way, the paper explores board-level involvement in InfoSec in depth, leading to the identification and description of the board of directors' roles in this context.

2 LINKING ROLE AND RESOURCE DEPENDENCY THEORY (RDT)

The first board role is the linking role, which is underpinned by the RDT (Hung, 1998). RDT has primarily focused on how directors attract resources for their firms and how they interact with key stakeholders like policymakers and suppliers to create competitive advantages. In other words, RDT focuses on the relationship the company has with external resources, the board's contributions to the process, and the control and management of resources (Oliveira et al., 2022). According to Sánchez et al. (2017), a board's ability to understand and govern complex businesses is required to implement the linking role. This role requires a variety of backgrounds, either derived from board members' education and experience or from their analysis of the relationship between directors and external agents. In the context of InfoSec, the linking role of the board revolves around three issues: resource acquisition, Inter-Organizational Relationships (IOR), and regulatory compliance.

First, organizations may not always have the tools, resources, and capabilities to deal with complex security incidents or attacks. So, large corporations increasingly outsource core and non-core activities. Outsourcing can be challenging due to foreign employees' limited control and knowledge (Hamlen & Thuraisingham, 2013). According to Abawajy et al. (2008), global outsourcing (offshore) and using a third-party in-house organization to deliver InfoSec (onshore) has been cited as one of the main InfoSec challenges. As organizations rush to take advantage of outsourcing, they often underestimate the security challenges posed by a global sourcing environment. There will be laws, regulations, compliance issues, cultural differences, and perceptions about security, privacy, and network protection when outsourcing around the world. According to RDT, boards should maintain strong and consistent security programs regardless of ethos, legislation, or compliance requirements (Abawajy et al., 2008).

Second, the complexity of the IOR process makes it difficult to allocate accountability, responsibility, and decision rights across multiple owners of resources, systems, and processes as the organization engages in IOR. This also pertains to enhancing and safeguarding the quality and value of the services delivered (Grant & Tan, 2013). According to Carminati et al. (2018), although IOR collaboration can be beneficial, it can also pose serious privacy and security risks, primarily due to weak trust relationships among the collaborating parties, which could lead to a lack of trust in how data/operations are handled. InfoSec is often a collaborative process involving vendors, service providers, and government entities, not just internal operations. Taking into consideration RDT, it is imperative that boards identify their external dependencies to enhance cybersecurity by establishing, maintaining, and enhancing the IOR.

Third, compliance with regulatory requirements is often cited as an indicator of improved performance and accountability (Tashi, 2009). According to Haber et al. (2022), regulatory compliance measures enforce good cybersecurity hygiene, but without good processes, personnel, training, automation, and

diligence, an organization is vulnerable. External auditors provide assistance beyond certification to evaluate accounting procedures and assess internal controls (Chorafas, 2001). In corporate governance, Rubaya-Tolibas (2017) emphasizes the role of external auditors in verifying the fairness and reliability of financial statements and increasing transparency. This is why external auditors, consultants, and regulatory bodies may be needed by organizations. Following RDT, organizations should identify their dependencies in terms of InfoSec compliance, and should limit external dependency where critical resources are involved and manage external dependency when required (Straub et al., 2009).

3 COORDINATING ROLE AND STAKEHOLDER THEORY

The second board role is the coordinating role, which is underpinned by Stakeholder Theory (Hung, 1998). According to Stakeholder Theory, considering stakeholder relations at board level can better address the need to balance the demands and expectations of various stakeholders (Parmar et al., 2010). To create and distribute stakeholder value, executives must manage and shape these relationships. Executives are responsible for addressing stakeholder interests while creating more value for them. Managers must find ways to make trade-offs and then improve those trade-offs for all stakeholders. Even though stakeholder relationships are crucial to businesses' survival and growth in capitalist societies, they are also moral endeavours involving issues of choice, value, and harm. By emphasizing stakeholder relationships and the coordinating role, boards can better create value and avoid moral failures (Freeman et al., 2010). As Pavlović and Tot (2020) emphasize, among the stakeholders with the greatest influence over Infosec are shareholders, managers, employees, unions, and other internal stakeholders. There is growing conflict and increasing complexity in the current security environment, which implies that as there are more stakeholders, security concerns may emerge and grow (ŞENGÖZ, 2022). According to Seltsikas and Soyref (2013), engaging key stakeholders and understanding the organizational context are critical to effective InfoSec. Drawing on Stakeholder Theory, the board is responsible for ensuring transparency and accountability in InfoSec, including rigorous reporting of security-related matters and communicating the actions taken.

4 CONTROL ROLE AND AGENCY THEORY

The third board role is the control role, which is underpinned by Agency Theory (Hung, 1998). Agency Theory can be applied to understanding corporate governance phenomena and conflicts of interest between agents and principals, emphasizing monitoring and incentive alignment systems to curb opportunistic behavior costs (Payne & Petrenko, 2019). Musaali (2010) stresses the importance of addressing conflicts of interests among directors and managers, as well as clearly distinguishing chairman and chief executive duties. In InfoSec, a board's control role revolves around accountability and monitoring, contractual relationships, and designing effective governance mechanisms.

First, as cyberattacks become more sophisticated, boards need to oversee cyber risk management so that companies are protected (Al Balushi, 2017). By monitoring continuously, organizations can ensure continuity, prevent threats, respond to risks, and recover without disrupting their business operations (AlGhamdi et al., 2020). This involves tracking security incidents, audits, and determining security effectiveness through key performance indicators (KPIs). For instance, using a systematic mapping study, Cadena et al. (2020) identifies metrics and indicators related to security incident management costs, quality, and service. To enhance asset protection strategies, Tyson (2011) discusses process-oriented and outcome-oriented metrics that measure security performance and incident rates. An InfoSec measurement infrastructure for KPI visualization is proposed by Hajdarevic et al. (2012) for continuous improvement of an organization's InfoSec Management System.

Second, organizations increasingly hire outside firms to maintain their IT. It's often difficult for these organizations to monitor contracted services and software. Information systems and data of organizations are often at risk due to contractors' uncontrolled and insecure access. Thus, organizations must manage contractor access and secure it (Allen et al., 1988). To identify and manage third-party risks, Andress and Leary (2015) advocate integrating InfoSec into contract management processes. In particular, Franqueira et al. (2013) suggest that organizations must establish proper oversight, integrate InfoSec into contract management, evaluate and negotiate security agreements, and specify responsibilities and compliance measures when creating contracts. By defining the responsibilities

and expectations of third parties in an agency theory-based contract, boards can be more effective.

Third, in Corriss (2010)' view, InfoSec governance needs to be incorporated into the culture of the organization from top to bottom, resulting in overall alignment. A misalignment of top-level management's governance approach and lower-level employment relationships can lead to adverse consequences for employees (Franqueira et al., 2013). In board-level governance, Posthumus and von Solms (2008) proposes using Agency Theory as a theoretical framework to improve alignment between InfoSec and business users. To protect data and systems, executives and boards often need to take a top-down approach to InfoSec. Using Agency Theory and board control, security managers and employees can be guided by an effective governance mechanism to act in the organization's best interests.

5 STRATEGIC ROLE AND STEWARDSHIP THEORY

The fourth board role is the strategic role, which is underpinned by Stewardship Theory (Hung, 1998). While Agency Theory assumes agents and principals act in their own self-interests, Stewardship Theory assumes managers are committed to the organization's success (Antón, 2010). It believes that executives and managers share a common interest as stewards of a company's resources. According to Gelfond et al. (2017), companies, whether public or private, are stewarded by their boards of directors who are responsible for selecting and supervising management, setting company strategy, and identifying and monitoring risks. As per Stewardship Theory, boards must safeguard organization interests and information assets, and govern InfoSec effectively, transparently, ethically, and over the long term. The board's strategic role revolves around four issues in InfoSec: setting the tone for InfoSec, organizational culture, employee behaviour and motivation, and ethical considerations.

First, top executives should develop security policies since they can evaluate organizations holistically and ensure new systems and procedures are implemented on time (McFadzean et al., 2007). It is the board's responsibility to create an organization's security culture, to educate employees via e.g. SETA programs on InfoSec, and to empower them to protect assets. Kárász and Kollár (2020) emphasize the importance of leadership in developing InfoSec awareness, which includes commitment, example-setting, and responsible decision-making. Integrating security into the organization's culture starts with everyday security concerns, and gradually introduces more policies over time (Corriss, 2010). Creating a culture of data security and asset protection requires the board's strategic role.

Second, an organization's culture is also crucial to InfoSec's success, in addition to security awareness and controls (Koskosas et al., 2011). In order to ensure the correct attitude towards security responsibilities, Van Niekerk (2005) recommends educating employees and establishing a corporate subculture of InfoSec. A culture that fosters compliance with information policies leads to better InfoSec (Tang et al., 2016). Mahfuth et al. (2017) also believes that having a strong InfoSec culture can enable employees to act as "human firewalls" protecting the organization's information assets. Psychological ownership leads to more secure behaviour. Stewardship cultures promote employee ownership of assets and data, resulting in improved security compliance (Ogbanufe et al., 2021).

Third, people's behavior has been repeatedly identified as one of the primary causes of policy failure (Kappelman et al., 2021). In other words, end users are InfoSec's weakest link. Using Stewardship Theory, Ogbanufe (2018) explored empirically and theoretically how psychological ownership affects InfoSec Stewardship behavior. According to Son (2011), researchers have relied on extrinsic motivation to explain employee rule-following behavior related to security in the past, whereas intrinsic motivation is capable of explaining employee rule-following behavior related to security in their organizations. Organizations can motivate its employees by creating a supportive culture, providing training, and designing motivating jobs (Sikolia & Biros, 2016).

Fourth, the biggest challenge in Infosec is not making ethical decisions, but recognizing them (Fleischmann, 2010). Kaur et al. (2017) emphasizes the responsibility of company boards in implementing ethical behavior across policies and procedures. According to Kjaer (2021), to ensure a sound and healthy culture within the organization, the board is responsible for setting organizational values and ethical standards. Schwartz et al. (2005) also emphasizes that directors are responsible for oversight of an organization's ethics and compliance programs, and that their ethical role sets a high standard at the top.

6 MAINTENANCE ROLE AND INSTITUTIONAL THEORY

The fifth board role is the maintenance role, which is underpinned by Institutional Theory (Hung, 1998). The Institutional Theory assumes that human behavior shapes institutions (behavior, perceptions, power, policy preferences, decision-making processes), as well as influencing them. Organizations must adapt to their institutional environment, which consists of norms, rules, and understandings about acceptable or normal behavior (Diogo et al., 2015). The rules and structures within an institutional environment influence organizational practices. Organizations, in Institutional Theory, are seen as embedded within broader societal and industry contexts rather than being isolated (Najeeb, 2014). The board must protect the organization from external influences while keeping it legitimate and relevant. How formal organizational structures spread can be explained by Institutional Theory (David et al., 2019). In InfoSec, the board's maintenance role revolves around three issues: compliance and regulations, norms and standards, and legitimacy and reputation.

First, consumers, patients, and the general public are protected by InfoSec laws. Different laws and standards apply to organizations depending on their country and/or industry sector (Lincke, 2015). Baran (2021) discusses the principles of legal regulation concerning InfoSec, such as the presumption of security for critical infrastructures. Intellectual property, privacy, and investigations are included among the legal concepts discussed by Conrad et al. (2014). Thus, board members should follow security regulations, understand legal principles, and manage privacy concerns as part of their maintenance role.

Second, for guiding security strategies and ensuring compliance with regulations, Trinca (2015) emphasizes the importance of industry standards and guidelines. According to Solms (1999), InfoSec management standards play an important role in ensuring appropriate levels of InfoSec among business partners. Tofan (2011) points out that standards allow security systems to be compared internationally on the basis of a common reference. In Caldwell (2013)'s view, organizations often need to meet security standards, either to ensure compliance or to reassure partners and clients. The board determines and implements industry standards and best practices to guide security strategies and enforces them to maintain legitimacy. Drawing on Institutional Theory, organizations and their boards can understand why ISO 27001 and NIST guidelines shape their security policies.

Third, Infosec is often needed not just for protection but also to preserve an organization's legitimacy and reputation. InfoSec affects IT usability, and the experience users have with their systems. Having a non-functional InfoSec service can irreparably harm an organization's reputation (Naicker & Mafaiti, 2019). According to Syed and Dhillon (2015), the impact of data breaches is felt on multiple dimensions of organization's reputation related to InfoSec, varying attributions, and sentiments on social media. The consequences of data breaches can be severe, including reputational damage and financial losses (Ray, 2022; Sinanaj & Muntermann, 2013). Taking responsibility for reputation risk is a formal function of boards. For corporate boards to oversee reputation risk management, Tonello (2007) recommends having a program to address stakeholder relations issues. For the organization's reputation to be protected, the board must ensure the security practices are legitimate.

7 SUPPORT ROLE AND MANAGERIAL HEGEMONY

The sixth and final board role is the support role, which is underpinned by Managerial Hegemony (Hung, 1998). The board needs substantial security expertise to fulfil its various roles in InfoSec. Hartmann and Carmenate (2021), however, highlight a serious lack of IT expertise on boards that may result in inadequate InfoSec governance. In most of today's organizations, cyber security is recognized, and specialist skills are in demand (Furnell & Bishop, 2020). Thus, companies have appointed technology experts, created technology committees, and assigned audit responsibilities to deal with InfoSec issues (Hartmann & Carmenate, 2021). This creates a complex relationship between the board and the InfoSec specialists, particularly the CISO. In this context, Hooper and McKissack (2016) discuss the evolving role of the CISO and the necessity for effective communication between the CISO and the board of directors. In addition, Short and Carandang (2022) outline how CISOs have evolved into business leaders that are able to influence board members through marketing and communication skills. Cybersecurity guidance is often provided by CISOs since most board members lack cybersecurity expertise. In these cases, Sharpe (2012) argues,

governance issues may not be controlled by boards effectively, and management decisions will determine the outcomes of decisions at the corporate level. In other words, managerial hegemony exists, a situation in which board members are leaving decisions that should be made at the board level to specialists at the management level. Following the discussion as outlined in previous sections of this paper, boards, particularly in a highly complex and volatile environment like InfoSec, should be vigilant against managerial hegemony and take appropriate responsibility for InfoSec issues. As such, InfoSec board roles need to be better understood in the first place and even though this short paper provides an initial overview, more research is needed.

8 CONCLUSION & FUTURE EMPIRICAL WORK

The use of Hung (1998)'s model in InfoSec literature to outline the six board roles provides a valuable framework for understanding and improving InfoSec governance. Boards can use this approach to create a structured mental model that helps them navigate the complexities of InfoSec and take up accountability and responsibility in an environment characterized by evolving cybersecurity threats and regulations. The explicit definition of roles leads to a shared understanding among organizational leaders, fostering a collaborative culture around InfoSec. Furthermore, it allows for comparison and identification of best practices among organizations, which helps establish industry standards. In the end, these insights enhance both theoretical and practical knowledge, helping to strengthen InfoSec in a rapidly evolving digital landscape.

In future empirical work, we will validate and assess the accuracy of board members' roles through discussions with board members and (security) executives, including CISOs. By analyzing case studies from high-reliability organizations and critical infrastructure providers, we will gain insight into the practices of effective InfoSec governance and management in high-risk environments. Their importance for the national critical infrastructure is expected to provide valuable insights into how boards address security challenges in such a context. The reliability of these organizations will improve the credibility and applicability of findings, enhancing the overall validity and practical relevance of our research. As a continuation of the case studies, this study will use a contingency perspective to assess the importance of the board's role in InfoSec. Therefore, we will organize focus groups to explore organizational characteristics such as leadership style style (Turel et al., 2017) and IT's strategic role (Turel & Bart, 2014) to understand their influence on board roles. The synthesis of findings derived from both case studies and focus groups is envisaged to culminate in a comprehensive understanding of the dynamic interplay and inherent significance associated with board-level involvement in InfoSec. With the integration of these diverse research streams, this work attempts to provide a nuanced perspective that enhances theoretical discourse and also provides practical insights that can help organizations improve strategic decision-making regarding InfoSec.

REFERENCES

Abawajy, J., Thatcher, K., & Kim, T.-h. (2008). Investigation of stakeholders commitment to information security awareness programs. 2008 International Conference on Information Security and Assurance (isa 2008),

Al Balushi, M. (2017). Regulating Cybersecurity in Corporate America. Specific Reference to Corporate Espionage. *Specific Reference to Corporate Espionage.(September 14, 2017)*.

AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. *Computers & security*, *99*, 102030.

Allen, J., Cunningham, L., Ford, G., Fraser, B., Kochmar, J., & INST, C.-M. U. P. P. S. E. (1988). *Security for information technology service contracts*.

Andress, J., & Leary, M. R. (2015). Manage the Security of Third Parties and Vendors.

Antón, F. (2010). Menuju Teori Stewardship Manajemen.

Baran, M. (2021). Principles of legal regulation of the institute of information security. *Uzhhorod National University Herald. Series: Law*.

Bobbert, Y., & Mulder, H. B. F. (2015). Governance Practices and Critical Success Factors Suitable for Business Information Security. *2015 International Conference on Computational Intelligence and Communication Networks (CICN)*, 1097-1104.

Bolourian, S., Angus, A., & Alinaghian, L. (2021). The impact of corporate governance on corporate social responsibility at the board-level: A critical assessment. *Journal of Cleaner Production*, *291*, 125752.

Cadena, A., Gualoto, F., Fuertes, W., Tello-Oquendo, L., Andrade, R., Tapia, F., & Torres, J. (2020). Metrics and indicators of information security incident management: A systematic mapping study. *Developments and Advances in Defense and Security: Proceedings of MICRADS 2019*, 507-519.

Caldwell, T. (2013). Setting the gold standard. *Computer fraud & security*, *2013*, 15-19.

Carminati, B., Ferrari, E., & Rondanini, C. (2018). Blockchain as a platform for secure inter-organizational business processes. 2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC),

Chorafas, D. N. (2001). The Contribution of External Auditors to the Internal Control System. *Implementing and Auditing the Internal Control System*, 314-336.

Conrad, E., Misenar, S., & Feldman, J. (2014). Domain 10: Legal, regulations, investigations, and compliance.

Corriss, L. (2010). Information security governance: Integrating security into the organizational culture. Proceedings of the 2010 Workshop on Governance of Technology, Information and Policies,

David, R. J., Tolbert, P. S., & Boghossian, J. (2019). Institutional Theory in Organization Studies. *Oxford Research Encyclopedia of Business and Management*.

Diogo, S. M., Carvalho, T., & Amaral, A. (2015). Institutionalism and Organizational Change.

Fleischmann, K. R. (2010). Preaching what we practice: Teaching ethical decision-making to computer security professionals. International Conference on Financial Cryptography and Data Security,

Franqueira, V. N., Van Cleeff, A., Van Eck, P., & Wieringa, R. J. (2013). Engineering security agreements against external insider threat. *Information Resources Management Journal (IRMJ)*, *26*(4), 66-91.

Freeman, R. E., Fairchild, G. B., Venkataraman, S., Mead, J., & Chen, M.-J. (2010). Creating Value for Stakeholders. *Stakeholder Management & Stakeholder Responsibilities eJournal*.

Furnell, S., & Bishop, M. (2020). Addressing cyber security skills: the spectrum, not the silo. *Computer fraud & security*, *2020*, 6-11.

Gelfond, S., Schwenkel, R. C., & Cohen, H. (2017). Private Company Boards.

Girn, S. (2022). A Data Driven Approach to Board Cybersecurity Governance. Pacific Asia Conference on Information Systems,

Grant, G., & Tan, F. B. (2013). Governing IT in inter-organizational relationships: Issues and future research. *European Journal of Information Systems*, *22*(5), 493-497. https://doi.org/10.1057/ejis.2013.21

Haber, M. J., Chappell, B., & Hills, C. (2022). Regulatory Compliance. In M. J. Haber, B. Chappell, & C. Hills (Eds.), *Cloud Attack Vectors: Building Effective Cyber-Defense Strategies to Protect Cloud Resources* (pp. 297-373). Apress. https://doi.org/10.1007/978-1-4842-8236-6_8

Hajdarevic, K., Pattinson, C., Kozaric, K., & Hadzic, A. (2012). Information security measurement infrastructure for KPI visualization. 2012 Proceedings of the 35th International Convention MIPRO,

Hamlen, K. W., & Thuraisingham, B. (2013). Data security services, solutions and standards for outsourcing. *Computer Standards & Interfaces*, *35*(1), 1-5.

Hartmann, C., & Carmenate, J. (2021). Academic Research on the Role of Corporate Governance and IT Expertise in Addressing Cybersecurity Breaches: Implications for Practice, Policy and Research. *Current Issues in Auditing*.

Hillman, A. J., & Dalziel, T. (2003). Boards of directors and firm performance: Integrating agency and resource dependence perspectives. *Academy of Management review*, *28*(3), 383-396.

Hooper, V. A., & McKissack, J. J. (2016). The emerging role of the CISO. *Business Horizons*, *59*, 585-591.

Hung, H. (1998). A typology of the theories of the roles of governing boards. *Corporate governance*, *6*(2), 101-111.

Kappelman, L., McLean, E. R., Johnson, V. L., Torres, R., Maurer, C., Kim, K., Guerra, K., & Snyder, M. (2021). The 2020 SIM IT Issues and Trends Study. *MIS Quarterly Executive*, *20*(1).

Kárász, B., & Kollár, C. (2020). Leadership Responsibilities in Information Security Awareness Development.

Kaur, K., Gupta, I., & Singh, A. K. (2017). A comparative study of the approach provided for preventing the data leakage. *International Journal of Network Security & Its Applications*, *9*(5), 21-33.

Kjaer, K. N. (2021). Ethics and why they matter. *Effective Directors*.

Koskosas, I., Kakoulidis, K., & Siomos, C. (2011). Information security: Corporate culture and organizational commitment. *International Journal of Humanities and Social Science*, *1*(3), 192-195.

Larcker, D. F., Reiss, P. C., & Tayan, B. (2017). Critical Update Needed: Cybersecurity Expertise in the Boardroom. *Cybersecurity*.

Lincke, S. (2015). Complying with Security Regulation and Standards. *Security Planning: An Applied Approach*, 39-58.

Mahfuth, A., Yussof, S., Baker, A. A., & Ali, N. a. (2017). A systematic literature review: Information security culture. 2017 International Conference on Research and Innovation in Information Systems (ICRIIS),

McFadzean, E., Ezingeard, J.-N., & Birchall, D. W. (2007). Perception of risk and the strategic impact of existing IT on information security strategy at board level. *Online Inf. Rev.*, *31*, 622-660.

Mintzberg, H. (1983). Power in and around organizations.

Musaali, M. (2010). The Board Managment Nexus in Corporate Governance. *Corporate Governance: Actors & Players eJournal*.

Naicker, V., & Mafaiti, M. (2019). The establishment of collaboration in managing information security through multisourcing. *Computers & Security*, *80*, 224-237.

Najeeb, A. (2014). Institutional theory and human resource management.

Nicholson, G., & Newton, C. (2010). The role of the board of directors: Perceptions of managerial elites. *Journal of Management & Organization*, *16*(2), 204-218.

Ogbanufe, O. (2018). The Mediating Role of Psychological Ownership in Increasing Information Security Stewardship Behaviors.

Ogbanufe, O., Crossler, R. E., & Biros, D. P. (2021). Exploring stewardship: A precursor to voluntary

security behaviors. *Comput. Secur.*, *109*, 102397.
Oliveira, F., Kakabadse, N., & Khan, N. (2022). Board engagement with digital technologies: A resource dependence framework. *Journal of Business Research*, *139*, 804-818.
Parmar, B. L., Freeman, R. E., Harrison, J. S., Wicks, A. C., Purnell, L., & De Colle, S. (2010). Stakeholder theory: The state of the art. *Academy of Management Annals*, *4*(1), 403-445.
Pavlović, D., & Tot, V. (2020). Economic security as a function of corporate security: A stakeholders' perspective. *Civitas*, *10*(1), 159-179.
Payne, G. T., & Petrenko, O. V. (2019). Agency Theory in Business and Management Research. *Oxford Research Encyclopedia of Business and Management*.
Posthumus, S., & von Solms, R. (2008). Agency theory: can it be used to strengthen IT governance? IFIP International Information Security Conference,
Ray, R. K. (2022). The Impact of Data Breach on Reputed Companies. *International Journal for Research in Applied Science and Engineering Technology*.
Rubaya-Tolibas, V. (2017). The Role and Responsibilities of External Auditor in Corporate Governance. Ascendens Asia Journal of Multidisciplinary Research Conference Proceedings,
Sánchez, L. P.-C., Guerrero-Villegas, J., & Hurtado Gonzalez, J. M. (2017). The influence of organizational factors on board roles. *Management Decision*, *55*(5), 842-871.
Schwartz, M. S., Dunfee, T. W., & Kline, M. J. (2005). Tone at the Top: An Ethics Code for Directors? *Journal of Business Ethics*, *58*, 79-100.
Seltsikas, P., & Soyref, M. (2013). Information security: a stakeholder network perspective. ACIS 2013: Information systems: Transforming the Future: Proceedings of the 24th Australasian Conference on Information Systems,
ŞENGÖZ, M. (2022). Türkiye'nin Ulusal Güvenlik Sınamaları Üzerine Aksiyolojik Bir Değerlendirme. *Takvim-i Vekayi*, *10*(2), 214-248.
Sharpe, N. F. (2012). Questioning Authority: The Critical Link between Board Power and Process. *The Journal of Corporation Law*, *38*, 1-51.
Short, A., & Carandang, R. (2022). The modern CISO: where marketing meets security. *Computer Fraud & Security*.
Sikolia, D., & Biros, D. (2016). Motivating employees to comply with information security policies. *Journal of the Midwest Association for Information Systems (JMWAIS)*, *2016*(2), 2.
Sinanaj, G., & Muntermann, J. (2013). Assessing Corporate Reputational Damage of Data Breaches: An Empirical Analysis. Bled eConference,
Solms, R. v. (1999). Information security management: why standards are important. *Inf. Manag. Comput. Secur.*, *7*, 50-58.
Son, J.-Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management*, *48*(7), 296-302.
Straub, D., Weill, P., & Schwaig, K. S. (2009). *Strategic on the IT resource and outsourcing: A test dependence of the strategic control model*. Springer.
Syed, R., & Dhillon, G. (2015). Dynamics of Data Breaches in Online Social Networks: Understanding Threats to Organizational Information Security Reputation. International Conference on Interaction Sciences,
Tang, M., Li, M. g., & Zhang, T. (2016). The impacts of organizational culture on information security culture: a case study. *Information Technology and Management*, *17*, 179-186.
Tashi, I. (2009, 16-19 March 2009). Regulatory Compliance and Information Security Assurance. 2009 International Conference on Availability, Reliability and Security,
Tofan, D. (2011). Information Security Standards. *Journal of Mobile, Embedded and Distributed Systems*, *3*, 128-135.
Tonello, M. (2007). Reputation Risk: A Corporate Governance Perspective. *Corporate Law: Corporate & Financial Law: Interdisciplinary Approaches eJournal*.
Trinca, A. Y. (2015). Standards, Guidelines, and Regulation for the Security Industry.
Turel, O., & Bart, C. (2014). Board-level IT governance and organizational performance. *European Journal of Information Systems*, *23*(2), 223-239.
Turel, O., Liu, P., & Bart, C. (2017). Board-level information technology governance effects on organizational performance: The roles of strategic alignment and authoritarian governance style. *Information Systems Management*, *34*(2), 117-136.
Tyson, D. (2011). *Security convergence: Managing enterprise security risk*. Elsevier.
Van Niekerk, J. F. (2005). *Establishing an information security culture in organizations: An Outcomes Based Education Approach* Nelson Mandela Metropolitan University Port Elizabeth].
Williams, P. (2007). Executive and board roles in information security. *Network Security*, *2007*(8), 11-14.
Zahra, S. A., & Pearce, J. A. (1989). Boards of directors and corporate financial performance: A review and integrative model. *Journal of management*, *15*(2), 291-334.
Попов, К., & Макеева, Е. (2022). Relationship between Board Characteristics, ESG and Corporate Performance: A Systematic Review. *Journal of Corporate Finance Research / Корпоративные Финансы | ISSN: 2073-0438*.