Information Securing in Organizations: A Dialectic Perspective

Yaojie Li
Management & Marketing
Columbus State University
Columbus, Georgia, USA
li_yaojie@columbusstate.edu

Bryan Fuller
Management
Louisiana Tech University
Ruston, Louisiana, USA
bfuller@latech.edu

Tom Stafford
Computer Information Systems
Louisiana Tech University
Ruston, Louisiana, USA
stafford@latech.edu

Selwyn Ellis
Computer Information Systems
Louisiana Tech University
Ruston, Louisiana, USA
ellis@latech.edu

ABSTRACT

Based on a field study of information security with two large corporations, we conjecture that information security should be aligned with varying organizational structures while adapted to environmental contingencies. We thus introduce a novel concept of information-securing – security-oriented actions-interactions in organizations to interpret the fit/misfit dilemma. Also, we suggest that conflicts can constantly exist between organizational security and business goals. To that end, from a dialectic perspective we elucidate how and why organizations act toward one direction first (e.g. business-oriented), then another (e.g. security-oriented), and eventually a synthesized one.

CCS CONCEPTS

• Security and privacy → Social aspects of security and privacy

KEYWORDS

Information Security, Organizational Structure, Dialectics

ACM Reference format:

Yaojie Li, Tom Stafford, Bryan Fuller, and Selwyn Ellis. 2019. Information Securing in Organizations: A Dialectic Perspective. In *Proceedings of ACM SIGMIS Computers & People Research Conference (SIGMIS-CPR'19), June 20-22, Nashville, TN, USA.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3322385.3322425

SIGMIS-CPR'19, June 20-22, 2019, Nashville, TN, USA.

ACM ISBN 978-1-4503-6088-3/19/06...$15.00.
DOI: http://dx.doi.org/10.1145/3322385.3322425

1. INTRODUCTION

To date, information security (for brevity, security) is a growing spending priority among contemporary companies as astute management appreciates that security failures can damage corporate reputations, deteriorating client trust and eroding market value [11, 15, 29]. Companies with fine-grained security programs, in contrast, are more likely to embrace opportunities in a market that demands security-embedded products and services. One can envisage that security and organizations are constantly coaligned, reshaping and reforming each other. Extensive security studies have enriched the understanding of security (1) actors (e.g. organizational insiders: [28, 39, 44]); (2) activities (e.g. information security compliance: [3, 13, 13]); and (3) approaches (e.g. deterrence: [6, 17, 37]; and protective-motivation: [2, 28]); while research concerning how information security fits into organizations has been elusive.

Information systems (IS) implementation literature [18, 20, 21], as reference, suggests that the match or "fit" between IS and organizational design determines the success of IS implementation. Similarly, in order to triumph in attaining and maintaining security, it would be intelligent to incorporate security into corporate design. Simply put, information security has to fit into diverse organizational structures. According to prior literature [32, 40], ignoring contingency factors, such as organizational strategy, structure, size, culture and environment, is likely to engender conflicts between security policy and an organizational system. The conflicts can cause a fallacy in security policy implementation, further posing severe security risks to an organization. Presumably, there is no panacea for formulating a set of universal security policies and procedures for all companies. Instead, companies have to figure out how to protect their own information assets and systems in turbulent security environments. However, research concerns about contingencies also tend to be sparse in current security literature.

To address the above research deficiencies, our first goal is to interpret organizational information security by mapping structural contingency theory into field interviews with two leading Fortune 500 companies. Even with many efforts to align security with organizational design, we conjecture that conflicts between security and business goals exist perceptually. To better understand the contraction that commonly occurs in organizations, we adopt a dialectic perspective that often applies in IS literature [1, 4, 33, 34, 35], on security-oriented (security model) and business-oriented (business model) organizational structures. Hence, the second objective is to advance knowledge in the evolution of security in organizations by progressing from seeming contradictions between the security and the business models. Rather than information security, information securing, a gerund, is conceptualized as a constellation of information security activities infused into organizational structure and structuring. Taken together, this research attempts to address two main research questions: (1) How organizational structure affects information security and (2) How we understand information securing in organizations in a dialectic perspective.

This research can make three possible contributions. First, it should contribute to information security research by introducing a contingence structure view of information security that has been elusive in previous literature. Adhering to the concept of "fit" in the spirit of the structural contingency theory, this study proposes that information security problems cannot be resolved without taking consideration of organizational structure. Second, the study invites a broad discussion about contradiction existing in security-oriented and business-oriented organizational structures. The research premise is that a company must ensure information security while also achieving business goals [15]. The thesis that corporate objectives are embodied in formal information security policies meets the antithesis of practical considerations at the workgroup level wherein practical and expedient "workarounds" contrasted against formal security policy meet in the synthesis of the merged consideration of company corporate imperatives balanced against practical workgroup consideration, insofar as secure organizational operations are considered.

Last, but not least, through an investigation of the "fit" and the "conflict" between security and practical operational considerations in organization, this research attempts to develop a theoretical framework of organizational information-securing. That is, corporate interests are protected at both corporate and workgroup levels, even though formal policies for security are not always observed in complete detail in all instances. To that end, the securing of an organization can be considered as independent from its formal organizational structure, and in that context a call is made for more research related to security contingency environments. The study asserts the notion of information securing as a dynamic process that evolves with the organization along with both its formal requirement and its pragmatic daily operational processes. The essence of an organization implies [12] that organizational information security objectives can be accomplished only when people pool their efforts, resources, knowledge, and/or identities.

This article is organized in the following manner: first, relevant literature is reviewed and theoretical development is conducted. Then, research methodologies and research are applications discussed. Specifically, it should be noted that in order to analyze the actuality of information securing in organizations, an initial study draws deductively from existing literature of structural contingency theory, then employs inductive analytical analysis exploring the initial conceptual framework in the context of two distinct research case scenarios, comparing a full range of organizational styles. In this way, an interactive data analysis is excised continually and interactively: data collection, data reduction, data display, and conclusion drawing [23].

2. LITERATURE REVIEW AND THEORETICAL DEVELOPMENT

In this section, two lines of theoretical foundations, structural contingency theory and dialectic theory, have been used to support studies of information security in organizations.

2.1 Information Securing in Organizations

In organizational theory literature, the debate concerning organizational structure traces back to Weber's [41, 42] ideal bureaucracy model of organization [12]. Organizational theorists summarize three core components from Weber's theory of organizational structure: division of labor, hierarchy of authority, and formalized rules and procedures. Through the lens of Weberian hierarchical structure, information security is "bolted-on" in organizations [15]. Information security tasks are assigned to candidates based on their relevant knowledge and expertise, therefore promoting information security professionalization and departmentalization (division of labor). In addition, information security professionals usually possess the authority in exercising security. For example, an employee who found security problems and issues is likely to report to a security authority (hierarchy of authority). Moreover, information security policies; standards, practices, guidelines, procedures derived from policies [43]; and strict security control dominate in many organizations (standardization). This ideal bureaucracy offers a way to turn employees with no more than average abilities into rational decision makers, serving clients with impartiality and efficiency [12]. In a sense, information security is provided in an independent fashion from organizational structure per se. The efficiency and effectiveness of information security can be ensured based on a constellation of qualified security professionals, security problems reporting and solving systems, and well-trained staff strictly complying with explicit security rules and policies. Based on the extent to which information security fits organizations, the study termed it security-affiliated in the bureaucratic organizational structure.

While Weber's bureaucracy provides a rationalized moral alternative to common practice nepotism and other power abuses, Weber's ideal concept has been criticized for two main drawbacks (1) its tendency to over-rationalize decision making to the point of turning people into unfeeling, unthinking automatons, and (2) its reliance on a fairly stable and reductionist assumption [12]. In security scenarios, even when information security policies are implemented seamlessly (a rare occurrence), it is impossible for the "rational" policy to outline every possible security behavior in anticipation of every possible threat eventuality [14, 19, 29]. Also, small organizations are unlikely to afford a sophisticated security system due to their boundary resources.

According to Donaldson [7], contingency factors reflect the influence of the environment in which an organization is located; an effective organization, therefore, has to fit its structure to the contingency factors and thus to the environment. According to Donaldson [8], contingency is defined as any variable that can moderate the effect of organizational characteristics on organizational performance, such as strategy, size, task uncertainty, and technology. Presumably, information security is another crucial contingency factor to consider in organizations. Facing rapidly changing and complex security environments, an organization has to change its structure to achieve a fit with information security. Information security, in turn, is reflected in the organization as one of its unique organizational characteristics. As a closer relationship between information security and organizational structure has thus been constituted, we term this security-contained. Based on the model, it can be illustrated that organizations have multiple security alternatives in varying contexts. For example, small organizations can utilize security technologies to fit their relatively simple organizational structure. In large organizations, despite "bureaucratic" security system aforementioned, one may attempt to break Weberian "iron cage" to motivate and empower even organizational insiders (security novices) to protect information assets and systems [3, 28, 30].

The last type of relationship between information security and organizational structure, security-infused, is derived beyond the security-contained relationship. The underlying rationale of security-infused model is dialectics between security and other contingencies. Intuitively, besides security contingency, an organization is likely to be influenced by institutional, strategic, size factors. Many contingency factors form contradictions and they interact. An effective set of organizational information security is attained by infusing it with other contingency factors in the organization. For example, investment in security may lead to a reduction of organizational resources allocated to the business goal. As such, an organization has to balance these two according its internal and external situations. For example, it can integrate information security training with routine work training, cutting high security risk business sectors or underserving security programs. Accordingly, the next session illuminates how the business and the security model discourse while bolstering organizational capability and adaptability.

To identify the fit between information security and organizational structures, we thus apply prescriptive theories of organizational structure. Mintzberg [24, 25] synthesized research on organizational design and thus developed five basic organizational structures from which management can adopt an appropriate one to meet organizational internal and external needs (Table 1). Hence, this study maps components of information ISO/IEC 17799 control objectives and Killmeyer's information security architecture [16] into Mintzberg's taxonomy of organizational structures.

2.2 Dialectics of Security and Business Goals in Organizations

Dialectic theory is rooted in the Hegelian assumption that organizations exist in a pluralistic world of colliding events, forces, or conflicting values that compete with each other for domination and control [5, 22, 38]. There are far-reaching studies using a dialectic approach in organizational change (e.g. [10, 36, 38] and information systems research (e.g. [1, 4, 33, 34, 35]). Nonetheless, there is limited information security research that leverages a dialectic analysis. In compliance literature, information security policy is widely presumed as unambiguous and stable. Following Mitroff and colleagues' [26], this research argues in support of dialectics applied in information security research in that: (1) a dialectic approach actively involves implementers who are no longer passive receptacles for security policies, but active creators of what they will actually use (new information security policies); (2) dialectics is a dramatic vehicle that induces implementers to take an active interest in enhancing the security system. In addition, using dialectics is consistent with the contingency view in discussions heretofore. This article focuses only on misalignments between security goal and business goal, and considers the "Thesis" of the conventional corporate Information Security Policy as contrasted against the "Antithesis" of workgroup contingencies, which may occasionally violate corporate ISP requirements in the interest of workgroup efficiency. While the resulting dialectic "Synthesis" is the merger of the overarching consideration of corporate policy requirements with workgroup efficacy needs.

While the two contingency factors can converge at some point, there are several reasons that make them compete with each other for domination in organizations. First, from an economic perspective, the goal of information security is to protect information assets and systems by investing in safeguard sanctions, such as monitoring technologies, security education, training, and awareness (SETA) programs, hiring security professionals. In other words, security investment is often categorized as direct and indirect expenses. The business goal, on the contrary, refers to how to maximize shareholders' interests, or to generate profits. Intuitively, boundary resources of an organization are likely to escalate conflicts between the two. Second, according to structure contingency theory, the

security and business strategy, the security and business environment, the security and the production technology can be emerging opposing forces to change an organizational structure to meet their needs. In this case, security and business are analyzed as the most salient dialectics in organizations. The business goal is defined as the thesis, i.e., a statement or theory put forward and supported by arguments [35], whereas an antithesis is formed as a security goal, containing the opposite to the business goal. Through an analysis of the debate of the business and the security goal, a synthesis is formed, reflecting which aspects of the two are the most plausible. The opposites of a contradiction are characterized by (1) the identity of the two opposing elements to explain their co-existence and (2) the struggles between the two elements that drive the change [4]. As such, one can argue that while a business and a security goal contradict each other, they can coexist when both are not powerful enough to outweigh the other; meanwhile, a "creative synthesis" [26] is likely to surface by incorporating elements from business and security goals, resulting in a dynamic change in an organization. In a further analysis of relevant contradictions, this research follows [1, 4] method of identifying and analyzing contradictions. To identify contradictions, conflicts as well as relevant interest groups, such as organizational politics, culture, learning and memory, and institutionalized patterns and practices will be considered [33, 34]. To analyze contradictions, three steps will be conducted: (1) define specific contradictions between the security and the business model; (2) analyze identity and struggles involving the two opposing elements; (3) synthesize by analyzing all contradictions involved in situations.

Despite the "triad of result" comprising thesis, antithesis, and synthesis, this research intends to explicate the dialectics between the business and the security model through the lens of "triad of method", including comparing, separating, and combining [9, 35]. According to Sabherwal and Newman [35], if a thesis dominates organizational activities, then the activities are identified and performed based on comparison with the thesis. Thus, constant comparison implies a continuation of the thesis. As new ideas appear to be distinct from the existing thesis, a separation of the antithesis form the thesis emerges. Lastly, to address the accelerating separation between the thesis and antithesis, a combination of the two or a synthesis is produced. In the business-security dialectics, it can be illustrated that business model usually governs organizational activities. As the thesis, the business goal is used to "benchmark" or standardize the activities. However, an emerging idea, such as updating an enterprise-wide information security system, adjusting strategy by emphasizing security embedded in products or services (e.g., social network companies, healthcare companies), is likely to separate a security model from the business model. Therefore, one has to stand out to address this division by combining a new alternative that may incorporate components of the business model, the security model, or both. Then, this synthesis will become a new thesis, performing the "benchmarking" role (Figure 3).

Table 1. Ideal types of organizational structure and associated information-securing mechanisms.

	Description of Characteristics	Associated Information-Security
Simple Structure	• Direct Supervision • Vertical and horizontal centralization • Low formalization	• Unsophisticated security infrastructure • Direct security problem reporting • Simple information security policies, standards, and procedures • Personal (managerial) monitoring
Machine Bureaucracy	• Standardization of work processes • Limited horizontal decentralization • High formalization • Automated and integrated technology	• Standard security infrastructure • Standard information security policies, standards, and procedures • Support from security department and experts • Security education, training, and awareness (SETA) programs
Professional Bureaucracy	• Standardization of skills • Vertical and horizontal decentralization • Highly skilled employees who value autonomy	• Standard security infrastructure • Standard information security policies, standards, and procedures • Support from security department and experts • SETA programs • Security culture in organizations
Divisionalized Structure	• Standardization of outputs • Limited vertical decentralization • Little interdependence or close coordination among divisions • Semiautonomous, loosely joined divisions	• Standard security infrastructure • Standard information security policies, standards, and procedures • Support from security department and experts • SETA programs • Security culture in departments/divisions
Adhocracy	• Mutual adjustment • Low formalization • Innovative • Selective decentralization • Cohesive workgroups	• Standard security infrastructure • Intelligent information security policies, standards, and procedures • Peer monitoring • SETA programs • Security culture in groups

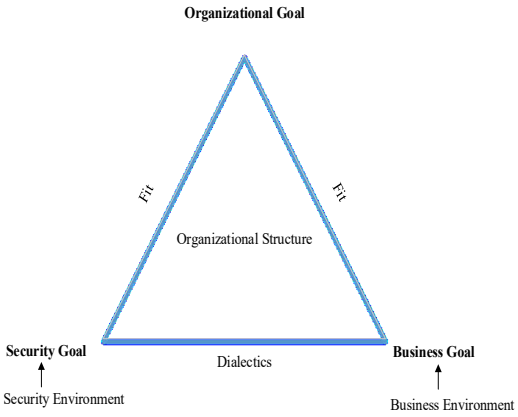

Figure 1. Alignment of security, business, & organizational goals

Figure 2. Fit security into organizational structures

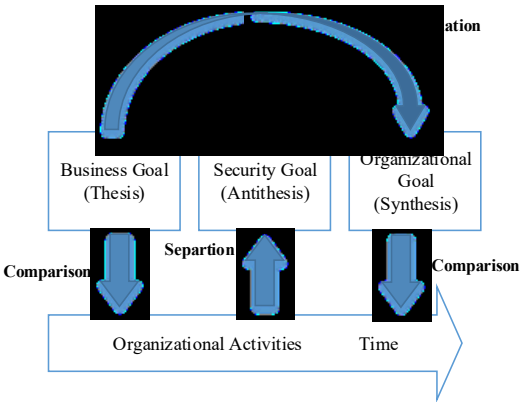

Figure 3. Dialectics of business and security models (adopted from Sabherwal & Newman 2003)

3. DISCUSSIONS

In this conceptual paper, we describe two important research questions: 1) how does information security into organizational structure and 2) how do organizations address the dilemma between business-oriented and security-oriented activities. In our further research, a case study and grounded theory method will be employed to analyze our qualitative data collected from two large companies.

REFERENCES

[1] Bjerknes, G., 1991. Dialectical reflection in information systems development. Scandinavian Journal of Information Systems. 3, 1, 55-77.

[2] Boss, S.R., Galletta, D.F., Lowry, P.B., Moody, G.D., and Polak, P. 2015.What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors. MIS Quarterly. 39, 4 (Apr. 2015), 837-864. DOI: https://doi.org/10.25300/misq/2015/39.4.5.

[3] Bulgurcu, B., Cavusoglu, H. and Benbasat, I. 2010. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Quarterly. 34, 3, 523-548. DOI: https://doi.org/10.2307/25750690.

[4] Cho, S., Mathiassen, L. and Robey, D., 2007. Dialectics of resilience: a multi-level analysis of a telehealth innovation. Journal of Information Technology. 22, 1 (Mar. 2007), 24-35. DOI: https://doi.org/10.1057/palgrave.jit.2000088.

[5] Churchman, C.W.1971. The Design of Inquiring System: basic Concepts of Systems and Organization. Basic Books, New York, NY.

[6] D'Arcy, J., Hovav, A. and Galletta, D. 2009. User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. Information Systems Research. 20, 1 (Mar. 2009), 79-98. DOI: https://doi.org/10.1287/isre.1070.0160.

[7] Donaldson, L. 1996. The normal science of structural contingency theory. In Handbook of Organization Studies. Clegg, S.R., Hardy, C., and Nord, W.R., Eds. Sage, London, U.K., 57-76,

[8] Donaldson, L. 2001. The Contingency Theory of Organizations. Sage, Thousand Oaks, CA.

[9] Findlay, J.N. 1958. Hegel: A Re-examination. Humanities Press, New York, NY.

[10] Ford, J.D. and Ford, L.W. 1994. Logics of identity, contradiction, and attraction in change. Academy of Management Review. 19, 4 (Oct. 1994), 756-785. DOI: https://doi.org/10.2307/258744.

[11] Gordon, L.A. and Loeb, M.P. 2002. The economics of information security investment. ACM Transactions on Information and System Security. 5, 4, 438-457.

[12] Hatch, M. J. and Cunliffe, A.L. 2013. Organization Theory: Modern, Symbolic, and Postmodern Perspectives, 3rd ed. Oxford University Press, Oxford, U.K.

[13] Herath, T. and Rao, H.R., 2009. Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems.18, 2 (Apr. 2009), 106-125. DOI: https://doi.org/10.1057/ejis.2009.6.

[14] Hsu, J.S., Shih, S., Hung, Y.W., and Lowry, P.B. 2015. The Role of Extra-Role Behaviors and Social Control in Information Security Policy Effectiveness. Information Systems Research. 26, 2 (June 2015), 282-300. DOI: https://doi.org/10.1287/isre.2015.0569.

[15] Johnson, M.E. and Goetz, E., 2007. Embedding information security into the organization. IEEE Security & Privacy. 5, 3 (May 2007), 16-24. DOI: https://doi.org/10.1109/msp.2007.59.

[16] Killmeyer, J. 2006. Information Security Architecture: An Integrated Approach to Security in the Organization, 2nd ed. CRC Press, Boca Raton, FL.

[17] Lee, S.M., Lee, S.G. and Yoo, S., 2004. An integrative model of computer abuse based on social control and general deterrence theories. Information & Management. 4, 16 (Jul. 2004), 707-718. DOI: https://doi.org/10.1016/j.im.2003.08.008.

[18] Leifer, Richard. 1988. Matching computer-based information systems with organizational structures. MIS Quarterly. 12, 1(Mar. 1988), 63-73. DOI: https://doi.org/10.2307/248805.

[19] Li, Y., Stafford, T., Fuller, B. and Ellis, S. 2017. Beyond Compliance: Empowering Employees' Extra-Role Security Behaviors in Dynamic Environments. In Proceedings of the 23rd America Conference on Information Systems (Boston, MA).

[20] Markus, M.L. and Robey, D. 1983.The organizational validity of management information systems. Human relations. 36, 3 (Mar. 1983), 203-225. DOI: https://doi.org/10.1177/001872678303600301.

[21] Markus, M.L. and Robey, D.1988. Information technology and organizational change: causal structure in theory and research. Management science. 34, 5 (May 1988), 583-598. DOI: https://doi.org/10.1287/mnsc.34.5.583.

[22] Mason, R.O. and Mitroff, I.I., 1981. Challenging Strategic Planning Assumptions: Theory, Cases, and Techniques. Wiley, New York, NY.

[23] Miles, M.B. and Huberman, A.M. 1994. Qualitative Data Analysis: An Expanded Sourcebook, 2e. Saga, Thousand Oaks, CA.

[24] Mintzberg, H. 1979. The Structuring of Organizations. Prentice Hall, Englewood Cliffs, NJ.

[25] Mintzberg, H. 1983. Structure in Fives: Designing Effective Organizations. Prentice Hall, Englewood Cliffs, NJ.

[26] Mitroff, I.I., Williams, J. and Rathswohl, E. 1972. Dialectical inquiring systems: a new methodology for information science. Journal of the American Society for Information Science. 23, 6 (Nov. 1972), 365-378. DOI: https://doi.org/10.1002/asi.4630230606.

[27] Morton, N.A. and Hu, Q. 2008. Implications of the fit between organizational structure and ERP: A structural contingency theory perspective. International Journal of Information Management. 28, 5 (Oct. 2008), 391-402. DOI: https://doi.org/10.1016/j.ijinfomgt.2008.01.008.

[28] Posey, C., Roberts, T., Lowry, P.B., Bennett, B. and Courtney, J., 2013. 'Insiders' protection of organizational information assets: Development of a systematic-based taxonomy and theory of diversity for protection-motivated behaviors. MIS Quarterly. 37, 4 (Apr. 2013), 1189-1210. DOI: https://doi.org/10.25300/misq/2013/37.4.09.

[29] Posey, C., Roberts, T.L., Lowry, P.B. and Hightower, R.T. 2014. Bridging the divide: a qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. Information & management. 51, 5, 551-567. DOI: https://doi.org/10.2139/ssrn.2418233.

[30] Posey, C., Roberts, T.L. and Lowry, P.B., 2015. The impact of organizational commitment on insiders' motivation to protect organizational information assets. Journal of Management Information Systems. 32, 4 (Oct. 2015), 179-214. DOI: https://doi.org/10.1080/07421222.2015.1138374.

[31] Puhakainen, P. and Siponen, M., 2010. Improving employees' compliance through information systems security training: an action research study. MIS Quarterly. 34, 4, 757-778. DOI: https://doi.org/10.2307/25750704.

[32] Raymond, L. 1990. Organizational context and information systems success: a contingency approach. Journal of Management Information Systems. 6, 4 (Mar. 1990), 5-20. DOI: https://doi.org/10.1080/07421222.1990.11517869.

[33] Robey, D. and Boudreau, M.C., 1999. Accounting for the contradictory organizational consequences of information technology: Theoretical directions and methodological implications. Information systems research. 10, 2 (June 1999), 167-185. DOI: https://doi.org/10.1287/isre.10.2.167.

[34] Robey, D., Ross, J.W. and Boudreau, M.C. 2002. Learning to implement enterprise systems: An exploratory study of the dialectics of change. Journal of Management Information Systems.19, 1 (Jul. 2002), 17-46. DOI: https://doi.org/10.1080/07421222.2002.11045713.

[35] Sabherwal, R. and Newman, M. 2003. Persistence and change in system development: a dialectical view. Journal of Information Technology. 18, 2 (Jun. 2003), 69-92. DOI: https://doi.org/10.1080/0268396032000101144.

[36] Seo, M.G. and Creed, W.D. 2002. Institutional contradictions, praxis, and institutional change: A dialectical perspective. Academy of Management Review. 27, 2 (Apr. 2002), 222-247. DOI: ttps://doi.org/10.5465/amr.2002.6588004.

[37] Straub, D.W., 1990. Effective IS security: An empirical study. Information Systems Research. 1, 3 (Sep. 1990), 255-276. DOI: https://doi.org/10.1287/isre.1.3.255.

[38] Van de Ven, A.H. and Poole, M.S. 1995. Explaining development and change in organizations. Academy of Management Review. 20, 3 (Jul. 1995), 510-540. DOI: https://doi.org/10.2307/258786.

[39] Warkentin, M. and Willison, R. 2009. Behavioral and policy issues in information systems security: the insider threat. European Journal of Information Systems. 18, 2 (Ap. 2009), 101-105. DOI: https://doi.org/10.1057/ejis.2009.12.

[40] Weill, P. and Olson, M.H. 1989. An assessment of the contingency theory of management information systems. Journal of Management Information Systems.6, 1 (Jun. 1989), 59-86. DOI: https://doi.org/10.1080/07421222.1989.11517849.

[41] Weber, M. 1946. From Max Weber: Essays in Sociology. Gerth, H. H. and Mills, C.W. Eds. Oxford University Press, New York, NY.

[42] Weber, M. 1947. The Theory of Social and Economic Organization. Oxford University Press, New York, NY.

[43] Whitman, M. and Mattord, H. 2016. Management of Information Security, 5th ed. Course Technology, Boston, MA.

[44] Willison, R. and Warkentin, M. 2013. Beyond deterrence: An expanded view of employee computer abuse. MIS Quarterly. 37, 1 (Jan. 2013), 1-20. DOI: https://doi.org/10.25300/misq/2013/37.1.01.