The Strategic JOURNAL of Business & Change MANAGEMENT

ISSN 2312-9492 (Online), ISSN 2414-8970 (Print)

www.strategicjournals.com

Volume 9, Issue 3, Article 034

STRATEGIC USE OF INFORMATION PRIVACY FOR ORGANIZATIONAL SUSTAINABILITY

Bestman, A. E., Chinyere, J. O., & Adebayo, A. A

The Strategic JOURNAL of Business & Change MANAGEMENT
ISSN: 2312-9492 www.strategicjournals.com

Vol. 9, Iss. 3, pp 517 – 527. September 27, 2022. www.strategicjournals.com, ©Strategic Journals

STRATEGIC USE OF INFORMATION PRIVACY FOR ORGANIZATIONAL SUSTAINABILITY

[1] Bestman, A. E., [2] Chinyere, J. O., & [3] Adebayo, A. A.

[1, 2, 3] Department of Office and Information Management, Faculty of Management Sciences, Rivers State University, Nkpolu-Oroworukwo, PMB, 5080, Port Harcourt, Nigeria.

Accepted: September 21, 2022

ABSTRACT

The purpose of this paper was to provide understanding about the strategic use of information privacy for organizational sustainability and also examine the relationship between information privacy and organizational sustainability. The baseline theory for this study was the restricted access and limited control theory (RALC), while the method used was the secondary methods where literatures were reviewed. The study findings revealed that, the strategic use of information privacy is vital for organizational sustainability as it protect individual's personal information from malicious users and boosts the confidence and trust the customers have for the organization. The study also found that administrative control and technical control have huge impact on building information privacy protection to achieve organizations sustainability that was measured by corporate reputation and stakeholder's satisfaction. The study concluded that there is a significant relationship between information privacy and organizational sustainability as well as the dimensions to the measures of the study. Based on the findings and conclusion, the study suggested that organizations and business firms should adopt strong administrative control and technical control as their strategies of ensuring information privacy protection in organization as it positively influence organizational sustainability, which can enable them achieved corporate reputation and stakeholder satisfaction.

Keywords: *Information privacy, organizational sustainability, administrative control, technical control, policy implementation, training, use of contract, access control, authentication, authorization, encryption, corporate reputation and stakeholder's satisfaction.*

CITATION: Bestman, A. E., Chinyere, J. O., & Adebayo, A. A. (2022). Strategic use of information privacy for organizational sustainability. *The Strategic Journal of Business & Change Management,* 9 (3), 517 - 527.

INTRODUCTION

Information is a vital asset to any organization as it enables them to make effective decisions that are needed to carry out their daily operations. Hence, the sustainability of any organization depends on how successfully the information in the organizations is managed. Some information is considered more susceptible than the other. Hence, organizations should be able to independently determine the mode of access to information in the organizations and also to protect individual's personal information in the organizations from unauthorized intrusion. The rapid growth of technology has made it possible for information to be collected and analyzed as quickly as possible without the knowledge of the organizations. Therefore, how organizations managed their information can influence how the organizations are perceived by stakeholder and the general public.

The merriam webster dictionary (n.d.) defined privacy "as freedom from unauthorized intrusion". Pelteret and Ophoff (2016), stated that "Privacy is a multi-disciplinary issue and therefore has a variety of definitions". However, Westin (1967, as in Pelteret & Ophoff, 2016) defines privacy as the "claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others". He also posits that personal autonomy, emotional release, self-evaluation, and protected communication are the purpose of privacy. Furthermore, Travani and Moor (2001), defined privacy "as the fundamental about protection from intrusion and information gatherings by others. However, information privacy according to Serohin (2021), "as the ability of an individual to independently determine the scope and mode of access to information about the way of his private life". Therefore, information privacy can also be defined as the capability or capacity of an individual, organization and institution to be able to protect their information from unauthorized intrusion. Hence, information privacy involved the capacity to decide how information should be used and collected as well as how information about the organization is communicated to the public. Many organizations have over the years experienced customer loss to their competitors as a result of many factors, such as speed of service delivery, and quality of service provided (Bestman & Chinyere, 2021). Hence, organizations are looking for ways to keep the business going and achieve sustainability. Privacy breaches in organizations are one of the major challenges for organizations that want to survive in business or have an edge over its competitors. Hence, there is need for them to be strategic in other for them to achieve this goal. Therefore, the strategic use of information privacy is a necessity for organizational sustainability as it can affect the ultimate success of the organizations.

Studies have explored a conceptual approach of information privacy, privacy in the digital age; others have focused on importance of information privacy to consumers, individual and organization. But just few have looked at the strategic use of information privacy for organizational sustainability and this study stand as one those few.

Problem

Information privacy involves the ability or capacity of an individual, organization and institution to protect their information from unauthorized intrusion. Information privacy is very essential as it enable organizations to protect their customers or client private information in the organizations. Thus, customers or client have this peace of mind knowing that their private information is safe with the organizations. Technological advancement has made it easy for large amount of data to be gathered and analyzed quickly. Therefore, organizations need to put measures in place to protect individual personal information stored in the organizations. Proliferation of problems may arise due to disclosure of individual vital information in the organization within the public space. These problems include inter-alia, loss of customers trust, reputational damage; reduce patronage, financial loss and loss of competitive advantage. Thus, the onus is on managers and business owners to provide strong information privacy protection to enable them to protect their information from unauthorized intrusion that can enable them achieve sustainability.

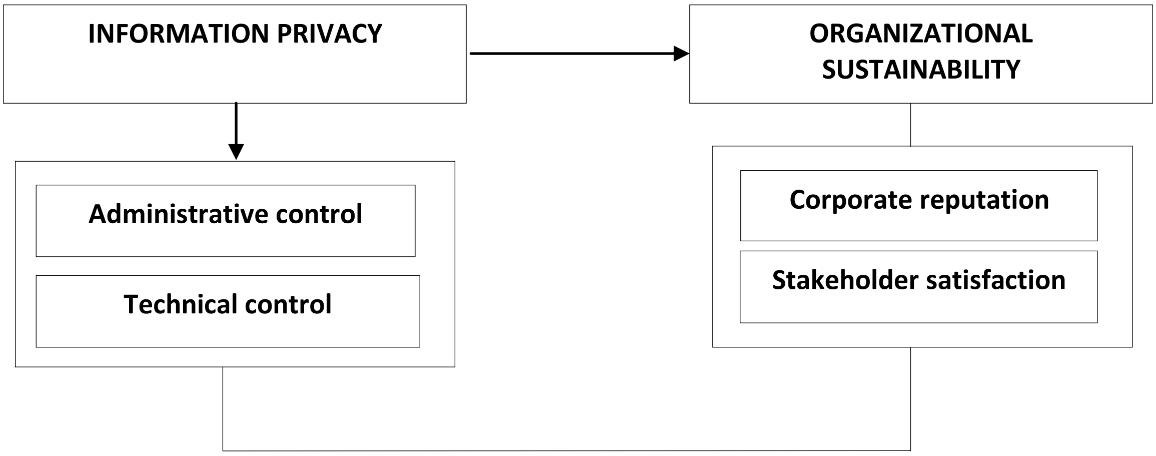

Figure 1: *Conceptual framework of information privacy and organizational sustainability*
Source*: *Research Desk, (2022).

Review of Relevant Literature

This literature attempts to discuss the various literature related to information privacy, its concept as a strategic means to achieve organization sustainability. Through this review, literature will be analyzed as a way of bringing new insights into the problem studied. The literature review will be done under the following headings

- Theoretical foundation
- Concept of Information privacy
  - Administrative control
  - Technical control
- Concept of organizational sustainability
  - Corporate reputation
  - Stakeholder's satisfaction
- Strategic use of information privacy for organizational sustainability

Theoretical foundation

The theoretical foundation of this study is hinged on restricted access limited control (RALC) theory propounded by Tavani and Moor (2001). This theory merged two important element of privacy which is restricted access and limited control into a single concept. Thus, the combination provides the necessary framework for privacy. The (RALC) theory defined privacy "in terms of protection from intrusion and information gathering by others (through situations or zones that are established to restrict access), not in terms of control over information". The RALC theory is a framework that recognized the importance of the restricted access theory which emphasizes the importance of using privacy policies and setting up zones that enable individuals to restrict others from accessing their information. The theory also recognized the importance of control theory in management of privacy which involves an individual not having absolute control over information about oneself, rather they need to have a level of control with respect to 3 key elements which are choice, consent and correction. Hence, individual need some control in their choice of actions that provide others the degree of access the person desired which can be from total privacy to total publicity (Tavani 2007). Therefore, individual can manage privacy if they can control the consent process, for example an individual can waive right to restrict others from accessing certain kinds of information about him or her, and lastly individual can managed privacy if they can be able to access their information and amend it if necessary. The RALC theory is used as the theoretical foundation of this study as it enables organization to understand how to manage information privacy in the organizations.

Concept of Information Privacy

Crossler (2011), posits that information privacy is a subgroup of the general concept of privacy, which has been studied and deliberated for centuries. Moore (2007), defined information privacy as “the right of a person to control their personal data”. On similar note, Serohin (2021), defined information privacy “as the ability of an individual to independently determine the scope and mode of access to information about the way of his private life”. Hence, information privacy can be defined as the capability or capacity of an individual, organization and institution to be able to protect their information from unauthorized intrusion. Information privacy involves the ability to decide how information should be used and collected as well as how information about individual is communicated to the public. However, Bélanger et al. (2002), specified that out of many definitions of information privacy there is only a little adjustment in the elements of the definitions, which typically include some form of control over the prospective secondary uses of one’s personal information. Serohin (2021), stated that Information privacy comprises of such control that enable a person to keep confidential information about those facts, phenomena and events that make up the content of all other aspects of the privacy.

Information privacy is considered as an element of the constitutional right to privacy, differentiated by the aspects of private life and the method of its objectification (Serohin, 2021). Information privacy is very essential to organization. Therefore, organizations need to put measures in place to protect customers and client personal information in the organizations. Technological advancement has forced organizations to adopt and increased their information privacy protections to enable them restrict access and also stop leakage of customers or client personal information that can lead to privacy breaches in organizations so as to avoid possible trouble in the organizations. Culnan and Williams (2009), stated that privacy issues can jeopardize the fiduciary relationship with shareholders if the bottom line is affected as a result of stock price declines, the loss of customers, fines, or other costs incurred in addressing the issues. Therefore, organizations need to be strategic with the use of information privacy in order to achieve organizational sustainability.

Administrative Control

Merriam-webster.com/dictionary (n.d.) defined control as an “exercise restraining or directing influence over”. Furthermore, Drucker (1974, as cited in (Hamilton &Jaja 2008), defined control as a function of management with the purpose of ensuring that the activities in organizations are engaged in such a way that desired results are achieved. Therefore, control can also be seen as the ability to decide how activities or actions are carried out. However, Simons (1999, as cited in (Hamilton &Jaja 2008), posits that administrative control involves some administrative practices which tend to set boundaries and guidelines for activities at the workplace. Merri (2013), suggested that administrative controls include; policies, awareness and training, on-screen wording that clearly describes to end users how applications work, suitable use agreements, and contracts. Hence, administrative controls are those exercise or practices carried out by managers of organizations that incline restrictions, boundaries, limitations and procedures for activities in the organizations. Administrative control is a necessity for information privacy in organizations; these controls include policies implementation, training and use of contract.

- **Policies Implementation:**

Merriam-webster.com/dictionary (n.d.) defined policy as “a set of guidelines or rules that determine a course of action”. Ansoff’s (1974, as cited in (Hamilton &Jaja 2008) defined policy as situational decision, because managers have specified a particular response to a defined set of conditions whose nature is well understood although their occurrence cannot be specified in advance. Furthermore, Urieto (1999, as cited in (Hamilton &Jaja 2008) stated that organization policies are statements that guide the activities or actions of members in specific situations. Therefore, policy can also be defined as set of rules or plans that pilot the activities of members in organizations. Organizations need to create policies to ensure that workers that have access to people personal information in the organizations do not disclose the information to third party or use the information for secondary purpose. Therefore, policies for information privacy should be created and also be implemented in organizations to ensure the effectiveness of the policy. Okoli and Onah (2003), suggested that policy implementation is the process of deciphering policy into actions and presupposition into results through various task and programs. Nwankwo and Apeh (2008), also asserts that the implementation of a policy is the most important phase in the policy process because this stage can determined the success or failure of a policy. Policy failures result from unsuccessful implementation (Nweke 2006).

- **Use of Contract**

Solan (2007), posits that contract is an obligation involved by the mere force of law to two or more parties, usually words, which usually accompany or represent a known intent. Furthermore, Genc (2002, as in Gagula & Lokovic 2017), stated that a contract is an agreed declaration, statement or speech of two or more parties with corresponding legal effects, which create or repeal the corresponding legal obligations. A contract can also be seen as an agreement between two or more parties that is to be bound by law. However, it should be noted that, for a contract to be valid, the following must be available, which are; offer, acceptance, consideration and an intention for the agreement to have a legal consequence in the case of a breach. This fact distinguishes a contract from a mere agreement. Hence, organization needs to adopt the use of contract and non-disclosure agreement for employees in organizations to agree not to disclose confidential information that they have access to or shared within the organization to anyone as an essential part of doing business, this methods of privacy protection is necessary for organizations that want ensure the protections of individual personal information in the hands of people that have access to the information not to use it for secondary purpose in order to achieve information privacy in the organizations.

Technical Control

These controls are executed into information technology infrastructure that are used to process personal data. Technical controls carry out several acute functions, which include preventing unauthorized persons from gaining access to the system and also been able to detect when a security violation has occurred on the system. The technical controls include; access control and encryption

- **Access control**

  Access control is used on systems or applications that are restricted to certain people. The access control consist of some attribute, information credentials, properties or privileges that may identify an entity in order to determine the access privileges of the system or entity (Mbanaso & Cooper, 2018). Access control include; authentication, authorization.

  Authentication:

  Mbanaso and Cooper (2018) posit that authentication addresses the concept of proving and confirming an identity claim by an entity. On a similar note, Singh and Manimegalai (2015), also stated that authentication "is the act of confirming the reality of an aspect of an entity". Authentication can also be seen as a process of endorsing the user's identity (Lal et al., 2016). It involves confirmation or verification of connection already established in the system. The authentication methods include; password, smart card and biometrics, all types of authentication mechanisms allows user to get access to the system however they all work differently.

Authorization:

Mbanaso and Cooper (2018), suggested that authorization is "the process of assigning privileges or credentials and the determination of whether the capabilities, privileges or credentials of an authenticated system are sufficient to perform certain actions or functions on a system". Authorization can also be seen as the process by which a system decides if the user has permission to use the system or access the system.

- **Encryption**

Olufohunsi (2019), defined encryption "as the process of converting information or a message which is referred to as plain text into a difficult unreadable form called cipher text by using an encryption algorithm (Bassel)". Furthermore, Singh and Manimegalai (2015), also defined encryption as the process of renewing or modernizing plan text into cipher text. Encryption was used up in communication among business partners to avoid third parties or spies from listening in the ancient days. Presently, encryption is used in organizations to help protect and secure their data from hackers. Encryptions and decryption are used in achieving privacy (Singh & Manimegalai, 2015).

The Concept of Organizational Sustainability

According to Colbert and Kurucz (2007), sustainability is the ability to "keep the business going", on a similar note Boudreau and Ramstad (2005), suggested that sustainability can be seen as the act of "achieving success today without compromising the needs of the future". However, Neubaum and Zahra (2006), defined organizational sustainability as the ability of an organization to encourage and support growth over time by successfully meeting the expectations of various stakeholders. Furthermore, Hart and Milstein (2003), referred organizational sustainability as the involvement of organizations in the process of accomplishing human development in an equitable, and secure manner by delivering simultaneously economic, social, and environmental benefits. Thus, organizational sustainability can also be seen as the ability of organizations to be consistent in their mode of operation in order to survive over a long period of time. Sustainable organizations are the ones whose attributes, activities and actions are projected to bring a desirable future-state for its stakeholders (Funk, 2003).

According to the Chartered Institute of Personnel and Development (CIPD, 2012), the goal of sustainability in an organizational context is "the principle of enhancing the societal, environmental and economic systems within which a business operates". Organizational sustainability is very necessary for organizations that want to survive on the long runs as it gives organizations a competitive advantage over their competitors. Organizations are looking for ways to remain in business. Hence they are adopting sustainable approaches or practice to their activities for them to last long in the business. White (2009), stated that depending on the condition, an organization might focus on the social or environmental aspects of sustainability. Furthermore, organizations must have a strategy prepared to encourage them carryout their activities responsibly. The strategy comprises of several aspect which include the ethical aspect and operational aspect (White, 2009).

Corporate Reputation

Pires and Trez (2018), defined corporate reputation "as a resource that generates competitive advantage". Corporate reputation reduces the risk of customers and investors leaving the organizations, rather it boosts the confidence of those partnering with the firm and encourages them to do more. Organizations with good corporate reputation are perceived to be the best in their services and product delivery in the industry, which increase the performance of the organizations. Corporate reputation is a very crucial factor for organizations aiming to build trust and win the heart of potential customers, client and the general public. Verhoeven et al. (2012), stated that corporate reputation can build the stakeholder trust as well as win the heart of a potential customers, or investor while introducing or a encouraging stakeholders to partner with the organizations or patronize the organization. Brammer and Pavelin (2004), posits that stakeholders make abnormal returns when purchasing stocks of organizations whose reputation has risen significantly. Hence, corporate reputation is a necessity for organizations that want to survive at the long run in business as it provides lots of patronage from customers as well as trust on their services and product delivery.

STAKEHOLDER' SATISFACTION

Bourne (2005), posits that stakeholders are individuals that are interested or have ownership in the project. Stakeholder can also be seen as individuals who have direct relationship with the organizations or individuals who are affected somehow by the organizations action. Huemann et al. (2013), suggested that project personnel, suppliers, partners, communities, as well as economic, social and ecological perspectives are considered stakeholders in the organization. Stakeholders of an organization contribute to the organization in the form financial support, knowledge, ideas and feedback and they include; employees, customers, suppliers, investors and community.

Stakeholder satisfaction refer to the feeling of excitement that stakeholder have about the realization of organizations goals and objective. Stakeholder satisfaction can also be seen as the happiness that stakeholders derived when organizations goals meet or exceed their expectation. Susnienė and Vanagas (2017), stated that stakeholder satisfaction is fundamental for organizations as it enable them get license to operate and produce output, to gain resources, build trust and become competitive and successful from the long-term perspective. Stakeholders' satisfaction is essential to organization as satisfied stakeholders expected to support the organizations in creating value. Ramaswamy and Ozcan (2014), stated that stakeholder's satisfaction has been identified as key to co-create value in the long term. They also noted that in any organizations the employees are very important as well as the customers. Beaulieu (2002), suggested organizations and business owners should see their stakeholders as an essential part of their business environment and should be given special attention so as to ensure benefit. Hence, stakeholder satisfaction is very necessary for organizations sustainability as it provide organizations with the ability to create new ideas as well as innovation for the organizations to keep going.

Strategic use of Information Privacy for Organizational Sustainability

Information policy is very vital to any organization that wants to survive at the long run in business; how a firm manages information can be determined how the firm is perceived by the public. Therefore, organization needs to ensure the use of information privacy protection to guarantee the safety of the information in their custody. Organizations need information privacy to protect the personal information of their employees, customers and stakeholder from intrusions and malicious users to avoid identity thief and been scammed. Pelteret and Ophoff (2016), stated that plenty issues can arise from the inappropriate use or poor protection of consumers' privacy and the concern about these issues can also affect their decisions about the organizations. Therefore, lack of information privacy in organization can makes the customers reduces patronage from the organization and also causes reputational damage that can affect the organization sustainability.

The rapid growth of information technology has made it easy for information to retrieved, assembled and scrutinized quickly without any permission or awareness of the organizations which can lead to breaches in privacy. Privacy breaches can lead to lower customer trust in a firm (Nofer et al., 2014).Thus, the strategic use of information privacy is very necessary in organization as it can make them to escape heavy fine attached to privacy breaches which can result to large amount of financial loss and also reputational damage that can affect the organizations survival. Hence, information privacy in an organizations can help organizations to build good reputation in the industry that can enable them have the ability to generate profit. Culnan and Williams (2009), also stated that privacy issues can jeopardize the fiduciary relationship with shareholders if bottom line is affected as a result of stock price drop, the loss of customers, fines, and other costs incurred in addressing the issues. Hence, information privacy can contribute to the key performance indicator and is a necessity for organizations that want to achieve sustainability.

Strategic use of information privacy in organization can increase trust and also boost the confidence of the individuals whose private information is stored in the organization because they believe that their information is safe with the organization. Thus, it shows that the organizations are reliable and trust worthy and it will increase patronage and loyalty in the organizations that can help achieve sustainability in the organizations. Furthermore, Barney and Hansen (as in Pelteret & Ophoff, 2016), stated that "Building trust can lead to competitive advantage, particularly if competitors are not seen as being as trustworthy and the attributes that lead to trustworthiness are difficult to imitate".

METHODS

The method used in this paper is the secondary data collection method from the relevant sources of research, scholarly works, articles and government sources. This information was intensively reviewed to gather the needed information that will help to identify and provide solution to the problems of the study in order to achieve sustainability in organizations.

Discussion of findings

Based on the literature reviewed, the study findings revealed;

1. The strategic use information privacy for organizational sustainability is vital. This was confirmed by Pelteret and Ophoff (2016), stated that plenty issues can arise from the inappropriate use or poor protection of consumers' privacy and the concern about these issues can also affect their decisions about the organizations. Culnan and Williams (2009), also stated that privacy issues can jeopardize the fiduciary relationship with shareholders if bottom line is affected as a result of stock price drop, the loss of customers, fines, and other costs incurred in addressing the issues.
2. There is a significant relationship between administrative control and organizational sustainability. This was confirmed by Simons (1999, as in (Hamilton &Jaja 2008), posits that administrative control involves some administrative practices which tend to set boundaries and guidelines for activities at the workplace. Hence, administrative controls are those exercise or practices carried out by managers of organizations that incline restrictions, boundaries, limitations and procedures for activities in the organizations. Strong administrative control is a necessity for information privacy in organizations.
3. There is significant relationship between technical control and organization sustainability. This was confirmed by Mbanaso and Cooper (2018) posit that authentication addresses the concept of proving and confirming an identity claim by an entity. This control is a necessity for information privacy in organizations.

CONCLUSION AND RECOMMENDATIONS

This paper successfully established that information privacy is very essential in any organization as it protect individual personal information that are stored in the organizations. Information privacy protections help organizations restrict access and also stop leakage of customers or client personal information that can lead to privacy breaches in organizations so as to avoid possible trouble in the organizations. Hence, information privacy is a crucial factor for organizations sustainability. The study concluded that administrative control and technical control are vital ways of ensuring information privacy in organizations. Therefore they should be given significant attention by organizations. Based on the findings and conclusion, the study suggested the following;

1. Organizations are encourage to have strong administrative control in ensuring information privacy in the organizations such as; policy implementation, and use of contract such as non-disclosure agreement will go to a great length in ensuring that people that have access to individual personal information in the organizations do not use it for secondary purpose other than it main purpose for which it was collected.
2. Organizations are encouraged to have technical control in the organization to ensure privacy protection. Technical controls carry out several acute functions, which include preventing unauthorized persons from gaining access to the system and also been able to detect when a security violation has occurred on the system, technical controls such as access control and encryption.

Contribution to knowledge

The study based on reviews, authenticated the purpose of the study, which is the strategic use of information privacy for organization sustainability. The study also validated the dimensions of this study as confirmed drivers of information privacy as well as the measures of organizational sustainability which are corporate reputation and stakeholder's satisfaction.

REFERENCE

Ajaegbu, F.O. Andeze, E. (2010). *Public policy making and analysis* Enug: Spring Time Press.

Beaulieu, S. (2002). Reintroducing stakeholder dynamics in stakeholder thinking: a negotiated-order perspective /Unfolding stakeholder thinking, p. 93.

Belanger, F. & Crossler, R. E. (2011).Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly* 35(4), 1017-1042.

Bélanger, F., Hiller, J., & Smith, W. J. (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *Journal of Strategic Information Systems* 11(4), 245-270.

Bestman, A. E., & Chinyere, J. O. (2021). Decisions support systems and organizational efficiency of the deposit money banks in Port Harcourt, Rivers State. *The Strategic Journal of Business & Change Management,* 8 (1), 183 – 196

Boudreau, J. & Ramstad, P. (2005). Talentship, talent segmentation, and sustainability: a new HR decision science paradigm for a new strategy definition. *Human resource management*, 44(2), 129–136.

Bourne, L. (2005), *"Project relationship management and the stakeholder circle", research thesis,* RMIT, Melbourne.

Brammer, S. & Pavelin, S. (2004). *Corporate reputation and social performance*. Mimeo, University of Reading, Uk.

CIPD (2012). *Responsible and Sustainable Business: HR leading the way – A collection of "thought pieces"*. London: CIPD.

Colbert, B. & Kurucz, E. (2007). "Three conceptions of triple bottom line business sustainability and the role for HRM", *Human Resource Planning* 30(1) 21-29.

Culnan, M. J., & Williams, C. C. (2009). How ethics can enhance organizational privacy: lessons from the choice point and TJX data breaches. *Mis Quarterly*, 33(4), 673–687.

Fassin, Y. (2009), "The stakeholder model refined", *Journal of Business Ethics,* 84(1), 113-135.

Funk, K. (2003). Sustainability and performance: companies that actively manage a wide range of sustainability indicators are better able to create long-term value for all stakeholders. *MIT Sloan manag. Rev*. (44), 65–70.

Gagular, A., & Lokovic, V. (2007). Interpretation of contract. *see law journal,* 1-28.

Grosu, V., Socoliuc, M., (2016). Discrimănări contabile privind tratarea fondului comercial, article *published in the international conference"paradigm of accounting and auditing: national realities, regional and international trends*". 71-72.

Hamilton, D. I. & Jaja, S. A.(2008). Strategies of administrative control: A study of business organizations in Nigeria. *European Journal of Scientific Research.* 19(3), 501-509

Hart, S. L. & Milstein, M. B. (2003). Creating sustainable value. *Acad. Manag. Perspect*. (17), 56–67.

Huemann, M., Weninger, C., Cardoso de Oliveira, J., Mendonça, B., Filho, L. & Weitlaner, E. (2013). Experimenting with project stakeholder analysis: a case study", in Silvius, G. and Tharp, J. (Eds), Sustainability Integration for effective Project Management. *IGI Global, Hershey*. 380-393

Lal, N. A., Prasad, S., & Farik, M. (2016). A review of authentication methods. *International Journal of Scientific & Technology Research 5*(11), 246–249.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (iuipc): the construct, the scale, and a causal model," *Information Systems Research.* 15(4), 336-355.

Mbanaso, U. M., & Cooper, P. G. S. (2018). *Privacy Characteristics Of Access Control Systems*. *September*. information Research Institute (IRIS).

Merri, B. L. (2013). *Information Privacy Revealed*. Educause Review.

Milhem, W., Abushamsieh, K. & Arostegui, M. N. P. (2014). Training strategies , theories and types training strategies , theories and types. *Journal of Accounting- Business & Management.* 21(1), 12-26.

Moore, A. D. (2007). Toward informational privacy rights. *San Diego Law Review*. (44), 809-846.

Neubaum, D. O. & Zahra, S. A. (2006) Institutional ownership and corporate social performance: the moderating effects of investment horizon, activism, and coordination. J. Manag. 32, 108–131. 26.

Nofer, D. K. M., Hinz, O., Muntermann, J., & Rossnagel, H. (2014). The economic impact of privacy violations and security breaches. *Business & Information Systems Engineering*. 6(6), 339-348

Nweke, E. (2006). *Public policy analysis: a strategic approach*. Enugu: John Jacobs Publishers

Okoli, F. C. & Onah, F. O. (2002). *Public administration in Nigeria: nature, principles and applications.* Enugu: John Jacobs Classic Publishers.

Olufohunsi, T. (2019). *Data Encryption*. University of Salford, Manchester

Pelteret, M., & Ophoff, J. (2016). A review of information privacy and its importance to consumers and organizations. *International Journal of an Emerging Transdiscipline*. (19), 277–301.

Pires, V. & Trez G. (2018). Corporate reputation: a discussion on construct definition and measurement and its relation to performance. *Emerald Publishing Limited*. (25) 1, 47-64

Ramaswamy V, Ozcan K (2014). The co-creation paradigm. *Stanford University Press,* P333.

Roberts, P. W., & Dowling, G. R. (2002). Corporate reputation and sustained superior financial performance. *Strategic Management Journal,* 23 (12), 1077-1093.

Satt, H., Chetioui, Y. (2017). Does goodwill improve firm performance? Evidence from the mena region. *Risk Governance & Control; Financial Markets & Institutions,* 7(2), 108-115.

Serohin, V. (2021). Information Privacy: A conceptual approach. *Constitutional And Legal Academic Studies*, *2*, 52–60.

Singh, K. J., & Manimegalai, R. (2015). Evolution of encryption techniques and data security mechanisms. *Word Applied Sciences Journal*. 33(10), 1597–1613.

Solan, L. (2007). Contract As Agreement. *Brooklynworks*, *353*.

Susnienė, D., & Vanagas, P. (2007). Means for satisfaction of stakeholders' needs and interests means for satisfaction of stakeholders needs and interests. *Engineering Economics.* 5 (55).

Tavani, H. T. (2007). Philosophical theories of privacy: Implications for an adequate online privacy policy. *Metaphilosophy,* 38(1), 1-22.

Tavani, H. T., & Moor, J. H. (2001). Privacy protection, control of information, and privacy enhancing technologies. *ACM SIGCAS Computers and Society,* 31(1), 6-11.

Verhoeven, J. W. M., Van Hoof, J. J., Keurs, V. T., & Van Vuuren, M. (2012). Effects of apologies and crisis responsibility on corporate and spokesperson reputation. *Public Relations Review,* 38, 501–504.

White, P. (2009). Building a sustainability strategy into business. *Corporate governance,* 9(4) 386-94.