STRATEGIES FOR INFORMATION SYSTEMS SECURITY IN ORGANISATIONS:

Strategies for security challenges in pre-adoption and post-adoption phase of Information systems

Research paper

Conerlious Zechariah Sagandira, Lund University, Lund, Sweden, co3720sa-s@student.lu.se

Abstract

As organisations and societies have been developing larger through the use of technologies. Forbes estimates that the use of emerging technology in organisations has boosted operating performance by 40%, increased time on the market by 36% and increased the opportunity to fulfil consumer needs by 35%. This ignited competition among organizations and to be able to compete, organisations have been using information technologies (IT) as a tool for competitive advantage. However, to use these technologies, organisation's choices during pre-adoption and post-adoption of information systems have been leading to more information systems security challenges. With the use of literature review and analysing solutions to these challenges, this paper suggests four different strategies which are: layering, response, deterrence and prevention. Organisation might need to consider the use of these strategies to ward off possible information systems security challenges as they try to adopt information systems to remain competitive in the industry.

Keywords: Security, Information systems, strategy, outsourcing, Centralised IS, Decentralised IS

Table of Contents

1 Introduction

Technology has become a driving force for the development of society and organisations. Forbes reports that the use of digital technologies in organisations has improved operational efficiency by 40%, faster time to market by 36% and the ability to meet customer expectations by 35%. As the majority of organisations, international corporations and some of the world's biggest institutions have expanded rapidly, every organisation wants to improve their efficiency. This ignited competition among organisations and to be able to compete, organisations have been using information technologies (IT) as a tool for competitive advantage. This made organisations depend much on the information systems to thrive in their respective sectors. However, the use of information systems in organisation has since raised some security concerns to both internal and external stakeholders. The issue of information security has caused some drawbacks in many organisations as they fail to balance efficiency and stakeholder trust. Hence, the use of information systems became one of the most important driver for any organisation's success. Although information security system remain a significant problem for many organisations. It is still a challenge for most of them to implement a strategy to secure their information systems.

This paper aims to suggest strategies that can be used to tackle information security challenges that might be experienced by organisations when adopting information systems to remain competitive in the industry. To come up with these strategies, challenges and solutions of pre-adoption and post-adoption will be used together with literature review.

1.1 Information systems in organisations

"Information systems (IS) are combinations of hardware, software and telecommunications networks that people build and use to collect, create and distribute useful data, typically in organizational settings" (Valacich & schneider 2009). As a discipline, information systems has become a driving force in successful organisations as well as improving our day-to-day life. Since most organisations have been relying much on information systems as a competitive tool, this led to the adoption of different organisational information systems structures and sourcing of powerful IS resources from other organisations to become more competitive in the industry (Lazarus, 2017).

There are two stages when an organisation will need to decide before the adoption of any IS. Firstly an organisation will need to choose an IS structure to rely on and secondly decide on how they can implement or adopt IS structure of their choice. According to Hsieh and Zmud (2019), these two stages can be referred to as pre-adoption and post-adoption of IS. During the pre-adoption stage, an organisation will be choosing on they type IS structure to use. An organisation may choose to go for a centralised, decentralised or federal IS structure. During the post-adoption stage, an organisation will be deciding whether to insource or outsource IS resources.

However, this paper will only focus on IS security implications of each IS structure in the pre-adoption stage and outsourcing as a way to implement IS in the post-adoption stage.

According to the book by Pearlson and Saunders (2013) organisations' IS structures can be either centralized at one end of the spectrum and decentralized at the other end of the spectrum. Centralised information systems (IS) organisations are those with all their employees, software, data, hardware and processing at one single location. On the other end of the spectrum, decentralised IS organisations are those with all their employees and components scattered everywhere. In decentralised IS organisations, their components are scattered so that they can meet their local user's or business needs. On the other hand, there are organisations with business needs that can be found in both ends of the spectrum. Normally these organisations want to archive advantages derived from both ends of organisational paradigms hence, they use the hybrid approach.

Most organisations thrive to archive the federal IS structure as it provides an organisation with more advantages (Pearlson & Saunders 2013). Overall, the use of either centralised or decentralised IS structure comes with its own information security challenges in an organisation. These challenges will be highlighted, and solutions will be suggested in the discussion part of this paper.

Implementing certain IS in organisations might be challenging due to lake of employees' expertise or IS knowledge (Wagnera et al. 2018). To solve this problem, organisations resorted to souring IS. Information systems sourcing is a process whereby an organisation hires another organisation which specialises in information technology to help them deploy desired IS into their organisation (Hirschheim et al. 2014). There are two types of sourcing IS which are: outsourcing and insourcing. In this paper, only outsourcing IS will be discussed in this paper. Outsourcing is an arrangement in which one organization employs another organization to be responsible for a scheduled or ongoing operation that is or may be carried out internally, and often includes the transition of staff and equipment from one organisation to another (Gorla & Somers 2013). Although organisations can get cheap services like data storage when outsourcing. There are security weaknesses that comes along with outsourcing (Ashcroft, 2018). These weaknesses will be discussed and solutions suggested in the discussion chapter of this paper.

1.2 Information security systems in organisations

Although information technology has rapidly created a range of innovation opportunities in organisations, these opportunities have created significant information-related risks which lead to an increase of data breaches in organisations. As a result of this, information security systems became the most vital part of IS process in an organisation. According to Moon, Choi and Armstrong (2018), information security systems refers methods and processes on how confidential information is kept, its availability and integrity. This is whereby access controls are used to detect, prevent and protect information systems from unauthorised personnel's, and data breaches. For the information security systems to be efficient and effective, a combination of processes, technology and people should be considered as main drivers (Whhitman & Mattord 2013).

Information security system of an organisation can be compared to the nervous system of an organisation. Organisations have been a target for cyber attackers which made more companies to invest more into information security systems. According to an information security breaches survey, at least 69 per cent of large organisations were attacked by an unauthorised outsider in 2014 (Nel & Drevin, 2015). Statista estimates that 33% of small organisations where attacked in 2014 with a decrease of 10% the previous year (2013). This shows how common large organisations' IS are attacked.

This raises a question to why more large organisations are attacked than small organisations?. According to Warkentin and Johnston (2006), poor IS governance in large organisations may lead to poor choice of IS structure which may lead to IS attacks. On the other hand, according to Ashcroft, (2018) most organisations risk their information security systems during outsourcing in the need for cheap services. This leads the discussion of outsourcing and the use of either centralised or decentralised IS structure security weaknesses. An example below explains how both the type of IS structure an organisation chooses and outsourcing can have IS challenges.

Forbes reported that an Indian outsourcing information technology (IT) giant Wipro Ltd was hacked in 2018. The company's IT systems was hacked and it was used to launch attacks against Wipro's customers such as RHT Health Trust. Wipro ended up paying $75 million to settle a lawsuit after it botched an SAP implementation on US National Grid. Wipro's attack shows how risky it can be for an organisation to rely much on an outsourcing company and employees. According to Threat Post, there are more Wipro's customers who also became victims after Wipro was attacked. Depending on their IS structure, some managed to recover their IS and some didn't. The company noticed an attack after noticing some unusual activities on some of its employee accounts due to an advanced phishing

campaign (Nandikotkur, 2019). The organisation was attacked through an employee's account which raised some questions on how the company monitors its employees' online activities as it uses a decentralised IS structure. This leads to a discussion on the security challenges that can be faced by an organisations in either decentralised or centralised IS through their employees. This example shows how outsourcing and the choice of IS structure can lead to a serious IS attacks that may lead to loss of confidentiality, information availability and organisation's integrity. With use of Confidentiality, Integrity and Availability (CIA) triad shown in Fig.1, security challenges of information systems will be explained how it affects the CIA of an organisation.

Fig. 1. The CIA triad

Source: Tierpoint.com

1.2.1 Security challenges of outsourcing information systems

In information systems, outsourcing can be an advantage to organisations by cutting costs and maintaining organisations' functionality in the event of IS failure. On the other hand, outsourcing can open doors to IS security attacks in an organisation (Savii, Neidenbach & Wolf 2008). This paper will only highlight three flaws of outsourcing that can cause IS security attacks in an organisation which are: less control, compatibility and data or information sharing. Due to the limited amount of time to write this paper, flaws will be explained in an author-centric rather than concept-centric.

Less control
When an organisation outsources, it has limited control over its systems as it places its trust in a third-party relying on their services and expertise. Because of this, organisation's information confidentiality will be no longer guaranteed since they do not have control over how their IS tasks are monitored and performed (Nassimbeni, Sartor & Dus 2012).

Compatibility
When an organisation outsources IS experts in a long term project, this means in-house Information technology employees will be replaced. To avoid this, an organisation will end up merging both in-house and outsourced employees as one team which where their level expertise might not be compatible might cause compatibility which lead poor IS services. As a result of this, an organisation might loose its integrity since poor IS services might lead to poor reputation of an organisation.

Data/information sharing
During outsourcing, there will be data or information sharing between two parties. This may lead to man-in-the-middle (MitM) attacks since it will be easy for an attacker to intercept and use personality impersonation to deceive the third-party to share information intercept during information sharing by using impersonation of the third-party. This affects the availability of information to the other partner and intended audience.

1.2.2 Security disadvantages of a decentralised IS structure.

In a decentralised IS structure, there are a number of security disadvantages which might lead to data breaches attacks in the IS of an organisation. Some of the disadvantages are: *Multiple identities per user, mischaracterised risk and new decision points.* Wipro Ltd will be used as an example to explain how outsourcing can be a security risk to IS of an organisation. Disadvantages of outsourcing will be explained with the use of diagram below (fig.2).

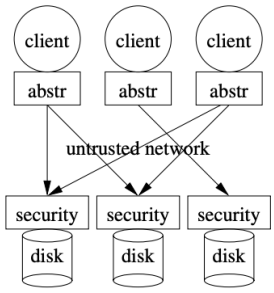

Fig. 2. Decentralised security
Source: (Thain et al. 2006)

Multiple identities per user

Based on the skill and ability of both the user and the system to execute the required authentication technique. In the diagram fig. 2 shows that a single user (client) might need to have multiple different identities in a decentralised security system to be able to have access to different security servers of an organisation . According to Dunphy, Garratt and Petitcolas (2018), multiple identities per user leads to identity fraud whereby an attack can be executed by deceiving the third party through user impersonation. As a result of this, it is difficult to maintain information confidentiality. Coinbase statistics states that, in 2016 15.6 million U.S consumers experienced identity frauds leading to the lose of $16 billion.

Risk can be mischaracterised

From fig. 2. It is shown that primary security mechanism in a decentralised system is moved closer to the storage device. This means employees of an organisation can have direct access to security servers as the organisation relies on its employees' decisions from decentralised locations. Due to the lack of employee expertise in decentralised locations, risks can be underestimated leading which might lead to intruder penetration as employees might not be competent enough for vulnerability testing of the system (Thain et al. 2006). Once the intruder or attacker penetrates the security system servers, the organisation might suffer loss of data. Mischaracterising risks by employees leads to inconsistency of information availability.

New decision points

In a decentralised security system, organisation's storage system may have several servers and each server might have a separate duty to execute authentication and authorisation. This means employees might have several decision points on both authentication and authorisation. This is a security risk because such decisions might execute well on one access control and fail at the other one. An organisation might experience an attack in their IS during the process of debugging a system because of new decision points (Thain et al. 2006).

1.2.3 Security disadvantages of a centralised IS structure.

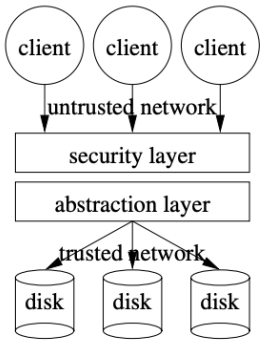

Fig. 3. Centralised security
Source: (Thain et al. 2006)[1]

Less security responsibility
As a result of depending much on IS experts, employees in centralised IS structure might end up being not responsible enough on how they interact with organisation's IS. Since it will be difficult to monitor or track which employee caused the IS failure. Knowing that chances are low to be hold accountable of their actions, employees might be reckless with their online behaviour as well. This makes it hard for an organisation to control and manage the security of their leading to poor services and well as tarnishing organisation's reputation (integrity).

Total IS failure
Once a single point of IS fails in a centralised IS, the rest of the security systems which depends on that point will as well have an access denial. An organisation might as well have time to recover or take security measures in the event of an attack as the whole IS would have been already captured. This prevents the organisation to have access to its information affecting one of the IS security component (availability).

Employee unresponsiveness
Since all systems will be centralised in a centralised IS organisation, it is difficult for the IS management to monitor every security control of an organisation. This might lead to inefficiency of IS security checks since each security decision has to be made by the managerial board of the organisation. This causes employees to be reluctant on security issues that may arise as they will be bored to wait for a decision to be made for each security failure check. Because of this attitude, employees might ignore to report security issues which they might think is small enough to affect organisation's IS.

Overall, it might not be enough for an organisation to rely on a centralised IS only especially for large and international organisations. Not only does the use of centralised IS affects the security of IS of an organisation but affects its performance and competence.
To be able to overcome possible security challenges that may come through one of the IS structures it is essential for an organisation to come up with information systems security strategies (Horne, Ahmad & Maynad 2015).

[1] Fig. 3. Centralised security
Source: (Thain et al. 2006)

1.3 Information systems security strategy

As a result of an increase in the number of organisations growing fast and larger, there are more reports of information security systems (ISSS) attacks in organisations (Garret, 2019). According to Beebe and Rao (2010) information security strategy is defined as "the pattern or plan that integrates the organisation's major IS security goals, policies, and action sequences into a cohesive whole". Information security systems strategies are mainly used to tackle or avoid possible security attacks to avoid data breaches (Jeonga et al 2019). For an organisation to know which security strategy to use, they need to know their IS security weaknesses. With the help of literature review, strategies will be suggested based on the aforementioned security weaknesses of outsourcing and organisation's choice of IS structure.

2 Discussion

Possible challenges associated with each type of IS structure and outsourcing where highlighted prior. In this chapter, solutions and a strategy will be discussed and suggested on how organisations can protect their information systems despite of the possible weaknesses and challenges associated with their type of IS structure or during outsourcing in the pre-adoption and post-adoption stages.

2.1.1 Solutions for outsourcing challenges

Table 1: solutions for outsourcing

Challenge	Defence	Key Actions
Compatability	Employee cautious	Employees should try to understand how the organisation proving IS services prepares and supervises its employess in order to monitor, handle and secure classified information.
Less control	Specify boundaries	The organisation must remind the organisation providing IS services of the position of its data at all times and must not delegate any of the deliveries to another group or third-party. Signing a non-disclosure agreement is also essential.
Compatability	Observe intently	Observe the provider's approach to early-stage threats and attacks in depth. Evaluate the consistency and depth of the solution of the provider.
Data/information sharing	Create a monitoring strategy	Monitoring the provider with continuous right-to-audit operations and the use of third-party monitoring beyond that of the outsourcing provider.

2.1.2 Solution for decentralised and centralised IS structure security challenges

As there are challenges associated with both centralised and decentralised IS organisational structures that can lead to information systems security attacks. Organisations might need to consider the adoption of a hybrid system (federal IT) structure. This is whereby an organisation uses both decentralised and centralised IS structures to benefit advantages from structures. With the help of a diagram *fig. 4.* Solutions to these challenges will be suggested.

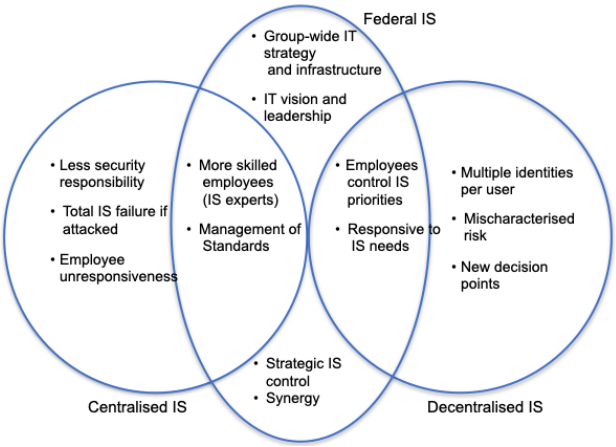

Fig. 4. Centralised security
Source: (Pearlson & Saunders 2013)[2]

By using a federal IS structure, organisations can ward off aforementioned security challenges of centralised and decentralised IS structures. Security challenges that are associated with a centralised system such as less security responsibility, total IS failure and employee unresponsiveness are solved by using strengths from a decentralise IS structure. For example, in a decentralised IS structure, employees control IS priorities which is a solution for less security responsibility in centralised IS. Security challenges of each IS structure are solved by implementing a federal IS as illustrated in the diagram *fig. 4.*

2.1.3 Strategies of securing Information systems of an organisation.

These strategies only focuses on tackling security challenges which are highlighted in this paper. Two strategies will be targeting IS structures (centralised & decentralised) security challenges in the pre-adoption phase of IS and the other two strategies will be targeting outsourcing security challenges in the post adoption phase. With the help of literature review, strategies presented in *Table 2.* shown below.

Security Challenges	Solutions	Strategy	Adoption phase	Literature and definitions
Compatability	Employee cautious	Layering (LAYER)	Post-adoption	This is a network security strategy which makes use of a variety components to protect activities by using various security controls. This type of strategy is mainly used by organisations with the goal to ensure that any single defense feature of their system has a backup to fix or recover any flaws or gaps in other security defenses Aydos, Vural and Tekerek (2019) (Deep 2020; Rizk et al. 2019; Anand 2020; Aydos et al. 2019; Hong & Kim 2016; Alberts 1996; Anderson 2001; Butler 2002; Byrne
Data/information sharing	Create a monitoring strategy			

[2] Fig. 4. Centralised security
Pearlson and Saunders (2013)[2]

				2006; Dasgupta 2004; Gandotra et al. 2009; Hitchins 1995; Hunter 2003; Jones 2005; Kewley and Lowry 2001; Lester and Smith 2002; McGuiness 2001; McHugh et al. 2000; Peterson 2007; Price 2010; Rosenquist 2008; Rubel et al. 2005; Runnels 2002; Sharlun ; Smith 2002; Stytz 2004; Burnburg 2003)
Multiple identities per user	Strategic IS control	Response (RESP)	Pre-adoption	Response takes appropriate corrective actions against identified attacks. (Armstrong et al. 2004; Beauregard 2001; Cahill 2003; Hamill et al. 2005; Grance et al. 2004; Saydjari 2004; Williamson 2004)
New decision points	Management of standards			
Employee unresponsiveness	Responsive to IS needs			
Less control	Specify boundaries	Deterrence (DETER)	Post-adoption	Deterrence employs disciplinary action to influence human behavior and attitude. (Agrell 1987; Blumstein et al. 1978; D'Arcy et al. 2009; Dunn 1982; Forcht 1994; Hu et al. 2011; Huth 1999; Kankanhalli et al. 2003; Klete 1975; Park et al. 2011; Parker 1981, 1983; Siponen and Vance 2010; Straub 1990; Straub and Nance 1990; Straub and Welke 1998; Waterman 2009)
compatibility	Observe intently			
Risk can be mischaracterised	More skilled employees (IS experts)	Prevention (PREV)	Pre-adoption phase	Prevention aims to protect information assets prior to an attack by prohibiting unauthorized access, modification, destruction, or disclosure. (Arce and McGraw 2004; Brand 1990; Browne 1972; Brykczynski and Small 2003; Evans et al. 2004; Graham 2003; Humphries et al. 2000; Lampson 2004; Lippmann et al. 2002; McDermott 2000; Ray et al. 2005; Schudel and Wood 2001; Virta 2005; Wood and Duggan 2000; Zalenski 2002)
Less security responsibility	Synergy			
Total IS failure	Groupwide IT strategy and infrastructure			

3 Conclusion

This paper highlights possible security challenges that organisations may encounter during their pre-adoption and post-adoption of their IS. In the pre-adoption phase organisations might chose to adopt centralised or decentralised IS structures however, each structure comes with its own security challenges that might affect confidentiality, integrity and availability of organisation's information. Security challenges in the pre-adoption phase like multiple identity user, less security responsibility, total IS failure, employee unresponsiveness and new decision points have been highlighted and solutions to these challenges were also drawn. With the use of

literature review and suggested solutions, organisations are advised to used prevention and response strategies as tools to tackle each security challenge in the pre-adoption phase of IS. Moreover, organisations might also encounter security challenges in the post-adoption phase of the IS. This might happen when organisations try to adopt IS by outsourcing. This paper highlights security challenges of outsourcing such as less control, compatibility and information sharing and possible solution to these challenges have been suggested. By using literature review and analysing possible solutions of these challenges, this paper suggests that organisations might need to consider the use of deterrence and layering strategies to ward off possible challenges that may come when outsourcing.

References

Keri E. Pearlson, Carol S. Saunders (2013) *Strategic Management of Information Systems, 5th Edition International Student Version*, 5th edn., online : Wiley.

Kate O'Flaherty (2019) *Breaking Down The Wipro Breach -- And What It Means For Supply Chain Security,* Available at: *https://www.forbes.com/sites/kateoflahertyuk/2019/04/16/breaking-down-the-wipro-breach-and-what-it-means-for-supply-chain-security/#540e49e35259* [Accessed: 28 October 2020].

Joseph Valacich, Christoph Schneider (2009) *Information Systems Today: Managing the Digital World*, 4th edn., Wales: Paperback.

Narasimhaiah Gorla, Toni. M. Somers (2014) 'The impact of IT outsourcing on information systems success', *Information & management ,* 51(3), pp. 320-335.

Yun Ji Moon, Myeongglil, Deborah J. Armstrong (2018) 'The impact of relational leadership and social alignment on information security system effectiveness in Korean governmental organizations', *International journal of Information & management ,* 40(), pp. 54-66.

Frans Nel, Lynette Drevin (2019) ' Key elements of an information security culture in organisations', *Information and Computer Security,* 27(2056-4961), pp. 146-164 [Online]. Available at: *https://www.emerald.com/insight/content/doi/10.1108/ics-12-2016-0095/full/html* [Accessed: 28 October 2020].

Merrill Warkentin, Allen C. Johnston, (2006) 'IT governance and centralised security controls ', *IT security ,* 40(), pp. 1-8.

Geetha Nandikotkur (2019) *Wipro's Breach Incident Raises Questions,* Available at: *https://www.bankinfosecurity.asia/wipros-breach-incident-raises-questions-a-12391* [Accessed: 28 October 2020].

Guido Nassimbeni, Marco Sartor, Daiana Dus (2012) 'Security risks in service offshoring and outsourcing', *Industrial Management & Data Systems,* 112(3), pp. 1-36 [Online]. Available at: *https://www.emerald.com/insight/content/doi/10.1108/02635571211210059/full/html* [Accessed: 28 October 2020].

Douglas Thain, Christopher Moretti, Paul Madrid, Philip Snowberger, and Jeffrey Hemmes (2006) 'The Consequences of Decentralized Security in a Cooperative Storage System', *Department of Computer Science and Engineering,* 22(), pp. 1-12.

Gregory Garrett (2020) *Cyberattacks Skyrocketed in 2018. Are You Ready for 2019?,* Available at: *https://www.industryweek.com/technology-and-iiot/article/22026828/cyberattacks-skyrocketed-in-2018-are-you-ready-for-*

2019#:~:text=During%202018%2C%20we%20have%20seen.phishing%20attacks%20in%20companies%20overall.[Accessed: 28 October 2020].

George Gustav, Savii Norbert, Neidenbach Edwin Wolf (2008) 'Mastering IT Security Issues in Outsourcing', *IT Security,* (), pp. 1225-1226.

JJ Po-An Hsieh, Robert W. Zmud (2019) 'UNDERSTANDING POST-ADOPTIVE USAGE BEHAVIORS: ', *A Two-Dimensional View ,* 2(), pp. 1-12.

(Valacich & schneider 2009)

Real

UKEssays. November 2018. Management Challenges with Information Systems. [online]. Available from:https://www.ukessays.com/essays/management/management-challenges-information-systems.php?vref=1 [Accessed 24 October 2020].

Sydney (2017) *Centralized, Decentralized or Hybrid Sourcing Structure: How Do We Decide?,* Available at: *https://spendmatters.com/2017/08/01/centralized-decentralized-hybrid-sourcing-structure-decide/* (Accessed: 28 October 2020).

Paul A. Ashcroft (2018) 'Reducing Outsourcing Cyber Risks', *TECHNOLOGY ISSUES,* 2(), pp. 1-15.

Stephan M.Wagnera, Pan Theo, Grosse-Ruykenb & Feryal Erhunc (2018) 'Determinants of sourcing flexibility and its impact on performance', *International Journal of Production Economics ,* 205(), pp. 329-341.

Rudy Hirschheim, Armin Heinzl &Jens Dibbern (2014) *Information Systems Outsourcing. The Era of Digital Transformation* [Online]. Available at: *https://books.google.se/books?hl=en&lr=&id=vXHpDwAAQBAJ&oi=fnd&pg=PR5&dq=IT+sourcing+information+systems&ots=yPESfWn-g4&sig=GqwvyhNWKFT-L_NO5hJB2Bne_Ss&redir_esc=y#v=onepage&q=IT%20sourcing%20information%20systems&f=false*[Accessed: 28 October 2020].

Dominick Rizk; Rodrigue Rizk &Sonya Hsu (2019) ' Applied Layered-Security Model to IoMT', *IEEE International Conference on Intelligence and Security Informatics (ISI),* 1(), pp. 1-277 [Online]. Available at: *https://ieeexplore.ieee.org/abstract/document/8823430* [Accessed: 28 October 2020].

Samundra Deep, Xi Zheng, Alireza, Jolfaei Dongjin, Yu Pouya, Ostovari Ali & Kashif Bashir (2020) 'A survey of security and privacy issues in the Internet of Things from the layered context', *Emerging telecomunications technologies ,* 1(), pp. 1-300 [Online]. Available at: *https://onlinelibrary.wiley.com/doi/full/10.1002/ett.3935* [Accessed: 28 October 2020].

Atif AhmadSean B. MaynardSean B. & MaynardSangseo Park (2014) 'Information security strategies: ', *Towards an organizational multi-strategy perspective,* 1(3), pp. 1-18.

Christina Y jeonga, Sang-Yong, Tom Leeb, & Jee-Hae Limc (2019) 'Information security breaches and IT security investments: ', *Impacts on competitors,* 56(5), pp. 681-695.

Michael E. Whitman, Herbert J. Mattord (2013) *Management of Information Security*, 5th edn., online : Wiley.

Paul Dunphy, Luke Garratt, Fabien Petitcolas (2018) 'Decentralizing Digital Identity: ', *Open Challenges for Distributed Ledgers,* 1(), pp. 1-4.

.