Available online at www.sciencedirect.com

ScienceDirect

IFAC Papers Online CONFERENCE PAPER ARCHIVE

IFAC-PapersOnLine 48-3 (2015) 1846–1852

The effectiveness of COBIT 5 Information Security Framework for reducing Cyber Attacks on Supply Chain Management System

Mark Wolden*, Raul Valverde, Malleswara Talla****

* BAE System, Saudi Arabia.
**John Molson School of Business, Concordia University, Montreal.,

(e-mail: mark.wolden@baesystems.com, rvalverde@jmsb.concordia.ca, mrtalla@jmsb.concordia.ca)

Abstract: Cyber espionage and malware attacks pose a great danger to many organisations, particularly those that embrace the use of modern technology to enhance efficiency. Although new off-the-shelf applications for enterprise resources planning (ERP) and management provide higher availability and better service, they are often customised, that can leave some scope for security gaps. While organisations have put in place tight security measures, malicious end users use security loopholes found in various systems to commit common cybercrimes such as denial of services, web hacking and defacement, malware, spam and phishing. The Supply Chain Management System (SCMS) is no stranger to such cybercrimes and certainly requires an Information Systems (IS) Security Framework in fighting off malware attacks. This paper investigates the effectiveness of the implementation of the COBIT 5 Information Security Framework in the reduction of risk of Cyber Attacks on SCMS. In this effort, qualitative data was gathered for a comprehensive security questionnaire targeted to IS administrators and managers responsible for Supply Chain organizations that use COBIT 5 framework for security. The results indicated that COBIT 5 added a new dimension for IS security governance via strict policies and rule set that further strengthened enterprise applications security. Overall, we found that organization benefited from implementing the COBIT 5 framework security measures in SCMS and ERP systems.

Keywords: Enterprise Resources Planning, Supply Chain Management Systems, COBIT 5 Information Security Framework.

1. INTRODUCTION

In today's increasingly competitive market place, demand information is no longer a secret among the supply chain partners; however it is important to share information in a secured manner. It is proven fact that a supply chain functions effectively with information exchange (Valverde & Saade 2015). Several supply chains are often managed by business that holds strong hierarchical relationships with other partners in the chain (Valverde & Saade 2015). However, as a system, Supply Chain Management System SCMS has become highly susceptible to malicious attacks, an aspect that warrants for confidentiality to guarantee the security required for its operations. SCMS vendors at large have already rolled out their security measures, which might work rather well from within; whereas in an open backdrop, contemporary methods that are technically enhanced are needed to assure the safety of SCMS systems. The focus of this paper is on vulnerabilities and pliability of supply chains and the effectiveness of COBIT 5 as a security framework to reduce cyberattacks.

2. SUPPLY CHAIN SECURITY MANAGEMENT

2.1 The Framework

The security of a supply chain can be divided into design, security, and structure. These two sections influence the vulnerability and the disruption probability. In a supply chain, security framework businesses or companies can decide on a certain balance between design and structure as well as security enhancing measures (Boyson, et al, 2009). These will enable them to understand the supply chain. The balance can be easily decided on once the companies integrate supply chain security to their business strategy. Although these approaches are effective in these categories, they can be discussed in a larger perspective in the management of a supply chain framework.

2.2 Supply Chain Design and Structure Risk Mitigation

This strategy can be approached in the following two categories: Resilience and Agile.

2.2.1 Resilience

10.1016/j.ifacol.2015.06.355

The term "resilience" refers to the physical feature of a property that helps it to return to the original formation after a deformation that is not beyond its elasticity. In a business perspective, it is the responsibility of an organization to react to business disruptions (Valverde and Talla 2012a). Some of these disruptions are not expected to happen, for example disruptions caused by natural disaster. Resilience can be either proactive or reactive risk management. Consequently, it refers to the ability of any system to return to the desired or original state. On the other hand, to restore once a disruption has occurred, plans are put in place on the supply chain to its original design and structure. Resilience can be achieved either through flexibility or redundancy. Flexibility in the context is possible for a business to switch to other suppliers in case of disruptions while redundancy is reassignments to other industries due to underutilization. It can be achieved through infrastructure and resources investment, for example, multi-skilled work force, which is a system that can be able to accommodate multiple products, which has the capacity of a real change and number of suppliers.

2.2.2 Agile

Agility refers to the ability to react to short-term changes that takes place in a supply chain as well as the ability to respond to external disruptions smoothly. It also means the ability to respond to short-term changes in demand or supply quickly (Grittner and Valverde 2012). In this case there are back-ups that are set aside to deal with disruptions and other suppliers can be selected as solutions to a disruption. This is a proactive measure because actions have been taken in advance. In agility, aspects such as visibility, velocity, and acceleration are important. In order for a company to be able to respond to sudden and market changes, unexpected agility should be used. Moreover, agility can be important in dealing with demand and supply fluctuations although it is an important remedy in increasing the supply chain. Agility can be increased in the following ways. Promotion of information flow between suppliers and customers is important. The collaborative relationship within suppliers, postponing design, coming up with inventory buffers, and having a dependable logistic system are all-important factors to consider. As mentioned in the redundancy context, working with known suppliers is emphasized (Valverde, d Saade 2015).

2.3 Enhancing Security Measures

These measures enable companies to cope with vulnerabilities resulting from the supply chain design and sources of risk exposure. To have a clear analysis of this section it can be divided into: measures and visibility via audits.

2.3.1 Measures

A company can implement these security measures with an aim of curbing insecurity within the supply chain. Some of these aspects are use of closed circuit TV, perimeter fencing, among others. In addition, gaining admittance to larger corporate locations requires a prearranged appointment and an employee escort while on the premises. Some of these measures include; information, personnel, physical, security managers, and security plan. Analysis, this is an important approach in assessing the current state and impending dangers that are prone to risk sources. The final measure is on the pillar of security enhancing measures and is based on visibility, which can generate information that is more accurate in helping and mitigating vulnerability (Stephens and Valverde 2013)

2.3.2 Preventive and Reactive

Most of the measures that have been discussed can fall under the category of preventive measures. For example, the physical, personnel, security managers among others. On the other hand, security plans are under the reactive nature.

2.3.2 Audits

It is an important strategy to conduct an audit in a company with an aim of identifying security measures. The audit result will help define whether they are adequate for the circumstances. The main goal of an audit is to make sure that the right measures are adopted to prevent vulnerabilities. Conducting an audit is a preventive measure and can be deployed after something has happened (Almadhoob & Valverde 2014).

2.4 Vulnerability in the Supply Chain

After discussing supply chain management design and structure, it is important to discuss on the vulnerability, which is potential susceptibility to sources of risk. The interaction of structures and measures determines the potentials of vulnerabilities. Vulnerabilities can be dealt with by the design and structure of the supply chain; alternatively, higher dependencies have resulted from changing trends in supply chain management. These vulnerabilities can be dealt with by security measures that can be created via structure and design. It is important to note that, the better the balance between supply chain and the security tools the lower the vulnerability. Another important aspect to note is that the business disruption cannot be fully eliminated as some risk sources cannot be eliminated. The following are some of the underlying reasons for vulnerability, reduction in inventory, reducing the number of subcontractors, research, and development of new materials.

Research has shown that current principles used in supply chains have resulted in very vulnerable chains (Stephens and Valverde 2013). For example, the drive towards efficient supply networks has amounted into those networks becoming more vulnerable to business disruptions. Some supply chains aim at reducing vulnerability, but there remain chances that can result into disruption escalation. Therefore, it is easy to deal with the internal sources more than the external ones. This is true because despite all the security measures that are put in place, chances of a terrorist attack to take place are still

there. Human factors can also cause vulnerabilities in the supply chain. For example, cargo can be stolen despite all the security measures set aside.

There are different ways that have been adopted by companies in reducing vulnerabilities, for example reengineering or decreasing vulnerability by adjusting the structure and design within supply chains (Talla and Valverde 2012) (Valverde, Saade and Talla 2014)(Valverde and Talla 2012b). Introduction of analysis tools can act as answers to the drastic supply chain disruption. The analysis application can help in handling incidents in an adequate manner in the future. Kraus & Valverde (2014) developed a tool for the detection of fraud in supply chain, this tool analyses supply chain transactions in order to reduce the risk of fraud in the supply chains. Vulnerabilities in the supply chain can be mitigated with the help of supply chain tools.

2.5 COBIT Framework

Wiesmann A. et al. eds., 2005) illustrated the objective and functionality of several frameworks. COBIT, for example, is a risk-management based framework. It is classified as an IT governance framework that consists of four domains which are Plan and Organize (PO), Acquire and Implement (AI), Deliver and Support (DS), and Monitor and Evaluate (ME). Each domain has different controls. Organizations can consider using the full COBIT framework or adopt specific controls which can fulfil their needs. Because COBIT controls, mainly, take into account the governance of business objectives, organizations usually map standards such as ISO 27000 to integrate it along with COBIT and maximize security controls.

The policy components deal with the guidelines that must be in place that will ensure there is management and enforcement of security. COBIT provides procedures on how the software should be implemented and instructions to the Supplier Relationship Management (SRM) on how security must be managed with a consumer.

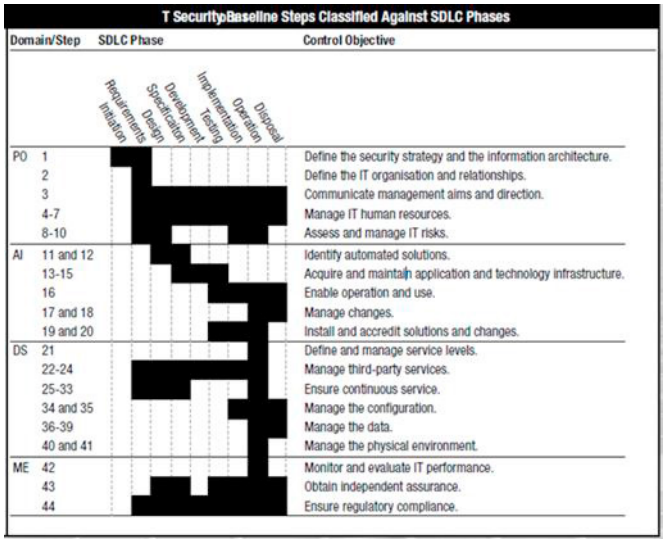

Fig. 1. Mapping the COBIT controls against SDLC phases (Watson C., 2009)

Watson C. (2009) proposed COBIT security baseline which involve several controls in each of the four domains. They presented the minimum security controls to verify compliance with web application security. The paper also provides an example for mapping the COBIT controls against SDLC phases. Steps are shown in figure 1.

3. RESEARCH METHODS

The basis of this study is to determine how effective the implementation of COBIT 5 Information Systems (IS) Security Framework for Information Security is in preventing and mitigating the risk of a cyber-attack on a SCMS. This incorporates the qualitative approach alongside quantitative which is better in this context so as to determine the perceptions and views on issues to do with System Network Integrity, Intrusion Detection & Monitoring, and Physical Security. More so, the issues concerning Management Overhead for Third Party ERP Toolsets, Relationship & Integration of the ERP-Role-Based Architecture was investigated at a corporate level. Consequently, the research would also check at the reliability of the Security Framework Management System (COBIT 5), Data Audit Trails and Process Documentation. The scholars used deductive and inductive strategy respectively to implement and structure the goals and objectives of the study. The scholars navigate through triangulation method by using various methods of study as Gratton & Jones, (2004), emphasizes using various design philosophies and approaches helps to enhance the depth of comprehension that a survey can yield. As such, study follows a technique that includes a questionnaire survey. The accuracy of qualitative and quantitative techniques is anchored on questions being surveyed or issues being asked. A researcher will use both methods as this offers wide-ranging experience and comprehensive understanding on the aim and objectives of a study (Hussey & Hussey 1997) have affirmed on preference between quantitative and qualitative techniques in the fieldwork study. Different experts have attempted to differentiate quantitative and qualitative study methods: Quantitative study techniques were evolved originally in natural sciences to research on natural occurrence. Examples of triangulation methods are well established now in social sciences. They constitute survey techniques, formal techniques (e.g. econometrics) arithmetical methods like mathematical modelling and experimentations.

The research used the case study approach, a single company with worldwide presence and headquarters in the United Kingdom. The researchers limited the study to one company mainly to improve response rates given the fact that people invited to complete the surveys were informed about the use of this survey in measuring the security effectiveness of the corporation. The other reason is because the scope of the research is in COBIT 5 and the case study satisfies the criteria. Although there are generalizability limitations by using a single case study, there is evidence of good results for information systems research with a single study as indicate

by Valverde, Toleman and Cater-Steel (2011) and Valverde (2008). The research was done using a pragmatist approach. Qualitative data was gathered through questionnaires. The selection for target audience is from group of employees, managers of various Supply Chain organizations that use COBIT 5 technology to assure the security of their enterprises. There are various methods that are used to evaluate captured data. The research sample included the 115 respondents randomly selected from various locations of the case study organisation. The respondents were selected mainly because they used systems for supply chain management purposes. The process of selecting a sample is normally continued until your required sample size is met. The sample of 115 respondents provided the views by filling questionnaires in how to determine how effective the implementation of COBIT 5 Information Systems (IS) Security Framework for Information Security is in preventing and mitigating the risk of a cyber-attack on a SCMS. These questionnaires were clustered in six categories, and then used for evaluating the opinion of respondents on the efficacy of the COBIT framework. The survey is structured in such a way as to get the most information about the work environment concerning implementation of the IS Security Framework. Therefore, the survey instrument comprised of logically structured questions, whose aims were clear to the researcher. The questions were categorized as Group 1, Group 2, Group 3, Group 4, Group 5, and Group 6. In Group 1, the focus was on Management of Rules, Responsibilities, and Policy. Here, the subtopics were Education & Training, and Change Control Management. Group 2 was about Addressing Security Implications of Role-Based Systems. The areas covered in this part of the survey questions were System Network Integrity, Intrusion Detection & Monitoring, and Physical Security. In Group 3, the questions were about Management Overhead for Third Party ERP Toolsets. Then in Group 4, the survey questions dwelt on Relationship & Integration of the ERP Role-Based Architecture and the Organization's Security Framework Management System (COBIT 5). Group 5 was on Data Audit Trails, while Group 6 covered Process Documentation. A comprehensive set of questions for a security survey has been presented in Table 1. The questionnaire was forwarded to groups of respondents. In each of these questions, the respondents have the choice of responding with a "True", "False", "Mostly True", and "Don't Know" responses. This was important since the study needed to sort the respondents according to their responses to questions in this section.

Table 1. ERP Security Survey Questionnaire

The following questions are concerned with Rules & Procedures:	
Q1	Are there appropriate Security Policy, Guidelines or Procedures established?
Q2	Do the existing Security/Guidelines/Procedures adequately state what is or is not allowed?
Q3	Are users informed of their obligation with regard to the relevant laws, security policy and procedures before being granted access rights?
Q4	Are you aware whether there is an Information Technology 'Acceptable Use Policy' within your organization?
The following questions address the ease of establishing role-based access to data, thus indicate the management overhead associated with that particular ERP's role-based access:	
Q5	Roles can be tied to position categories.
Q6	Default roles can be established
Q7	A report is provided that gives information on the implications of providing a role with access to a particular field, table or form (e.g. 'giving permission to access this form will allow the user to navigate to another form and change grades even though the grade field is not visible on this form').
The following questions address the security implications of the role-based.	
Q8	Role-based access is sufficiently granular that one can be sure than only those with a need to access certain data will be able to access that data.
Q9	It is relatively easy to deactivate access for a user.
Q10	Users are not required to have access privileges to the underlying database in order to run workflow processes.
Q11	Context sensitive roles can be defined (e.g. a user can perform function/s for specified records only at a specified point in the processing cycle).
Q12	Roles can be established that allow a user to process sensitive data in the ERP but restrict that user from downloading the data.
The following are for third party products, such as Business Intelligence Tools like Vision Waves, Portal Access Requirements, Reporting Tools, etc.	
Q13	Vendor recommended third party products and reporting tools are part of an integrated package have a role based architecture that is aligned to the ERP rather than being standalone role based architecture.
Q14	Is there a web-based tool that provides administrators with the ability to view the access that users have been granted, e.g. fields/tables/forms etc., within the ERP?
Q15	Is there a tool that provides a 'one stop' to manage access and deactivation from the ERP?
Q16	Password change policies and timelines for the ERP system and associated third party products can be managed from the organization's security management system?
The following questions assess the security of the ERP password and PIN authentication.	
Q17	Is the use of strong/complex password policy enforced?
Q18	Is the use of two-factor authentication enforced, e.g. RSA tokens?
The following questions are concerned with documentation related ERP Governance.	
Q19	Are there visual representations available that demonstrated processes, role approvals, dataflow, security checkpoints & database table touch tables?
Q20	Are workflow diagrams available to support process

	operations?
Q21	Is Process Documentation available that supports critical functions, e.g. Purchasing conditions, Invoicing, Credit Adjustments, Purchase Order creation?

Nevertheless, qualitative study, sampling aspect is also important such as how many and who should be included. Here, the best approach will be non-probability as a method as the sector involved limited number of chosen samples for research whereby there is no justification for numbers and results to random approach until a requirement is satisfied.

4. RESULTS AND FINDINGS

The main goal of this paper was to conduct an investigation into how effective the implementation of the COBIT Information Systems (IS) Security Framework for Information Security is in preventing and mitigating the risk of a cyber-attack on a SCMS. Furthermore, the findings in this section are derived from a survey conducted on case participants. The paper managed to meet this objective. As a demonstration of the possibility of merging practice and theory, the findings of the research are presented here. The researcher sent 200 surveys to key stakeholders connected with both the Supply Chain and Information Systems Management and Security who were identified in the case study. Only 115 surveys were responded to. Therefore, the study considered the survey questionnaires usable. There were surveys that were partially filled, and these had a note from the respondents explaining why they were unable to complete some of the sections. Despite this, all the surveys were considered usable because only 1 or 2 questions were unfilled in such instances.

The selection of participants for this case study depended on their ability to provide relevant information about the topic as the key factor. The 115 respondents were all from the same organization. For a clear understanding of how effective the implementation of an Information Systems (IS) Security Framework such as COBIT 5 for Information Security is in preventing and mitigating the risk of a cyber-attack on a SCMS, it is necessary get a glimpse of the practices and environment surrounding the information security. The following segment of the section gives and results from the survey interviews.

4.1 Results

The results are categorized as follows:

4.1.1 Management of Rules, Responsibilities, and Policy

This section covers the results for management of rules, responsibilities, and policy about implementation of the COBIT 5 Information Systems (IS) Security Framework such in preventing and mitigating the risk of a cyber attack on a SCMS. As indicated from related literature presented in this paper, there are various factors and activities of an organization's management that influence the effectiveness of an IS security framework. In addition, the case study survey gave views on this issue. Questions 1 to 7 provide the respondents view on Management of Rules, Responsibilities, and Policy concerning the case study topic. On "Q1: Are there appropriate security policy, guidelines, or procedures established?" the respondents answered predominantly "True". Q2 asked, "Do the existing security policy/guidelines/procedures adequately state what is or is not allowed?" On this one, 60% of the responses were "Mostly True". On Q3, the answers from the 115 respondents were predominantly "True" while Q4 gave a mostly "True" answer, this coming from 93.3% of the respondents. Q5 sought to establish from the respondents whether roles could be tied to position categories. Most (60%) of the 115 respondents indicated that this is "Mostly True." A further 33.33% of the respondents indicated this as "True." When it came to Q6: "Default roles can be established," the predominant answer was also "True" representing 66.7% of the respondents. Q7 read: "A report is provided that gives information on the implications of providing a role with access to a particular field, table or form (e.g. 'giving permission to access this form will allow the user to navigate to another form and change grades even though the grade field is not visible on this form)." The answer from the respondents was also predominantly "Mostly True."

4.1.2 Addressing Security Implications of Role-Based Systems

This segment of the section looks into responses concerning System Network Integrity, Intrusion Detection & Monitoring, and Physical Security. Responses to Q8 were 50% for "mostly true", while "true" respondents were 42.8% of the total. Q9 posed the following statement to the respondents "it is relatively easy to deactivate access for a user" to which the majority gave a "True" answer. A predominantly "true" answer was also given for Q10, Q11, and Q12.

4.1.3 Management Overhead for Third Party ERP Toolsets

The questions in this part concerned third-party ERP toolsets, for example Business Intelligence Tools such as Portal Access Requirements, VisionWaves, and Reporting Tools. Q13 had "Mostly True" and "Don't Know" as the most popular answers from the respondents. Q14 was dominated by "True", Q15 by don't know, while both False and Don't Know answers were indicated by 21.43% of the respondents in Q16.

4.1.4 Password and PIN Authentication 17, 18

This segment of the survey questions featured questions Q17 and Q18. For the two questions, most of the respondents (64.29% and 42.86% respectively) gave a "True" response.

4.1.5 Governance Documentation 19, 20, 21

This segment gives the results for governance documentation. This involved questions 19, 20, and 21 on the survey questionnaire. The responses were predominantly "Mostly True" for all three questions, although there was a tie between "Mostly True" and "True" responses in Q21.

4.2 Findings

The core objective of the paper was to identify how effective the implementation of the COBIT 5 Information Systems (IS) Security Framework is in preventing and mitigating the risk of a cyber-attack on a SCMS system. The case study explored the different aspects of implementation of an information security framework and tried to give an understanding about the influence of various aspects of an organization (Ramachandran, 2008). Moreover, the case had an obligation of giving relevant implications of the findings on how to make an Information System (IS) Security Framework successful. Case study findings indicate that with proper management of rules, responsibilities and policy, an organisation is able to enjoy effective implementation of the COBIT 5 Information Systems (IS) Security Framework that prevents and mitigates the risk of a cyber-attack on a SCMS. Effective management is seen in various activities including improved Education & Training, and Change Control Management. The literature indicates that security management tools are very essential for a supply chain. This is because the supply management runs through a myriad of risks.

This study reveals that management has influence on the effectiveness of a security system for an SCMS. Top management is responsible for channelling the necessary resources towards COBIT 5. Approval of decisions related to Information security also emanates from the management.

Further, the present study demonstrates that the willingness of administrators to back up an information security program through enforcement of rules and consistency has direct influence on the Effectiveness of the Implementation of an Information Security Framework in the prevention of Cyber Attacks on a SCMS. Employees and such managers have constant direct interaction hence this scenario plays out. These findings are in line with the study findings from Ramachandran et al (2008) who reiterated that mid-level management has the greatest influence on the effectiveness of an Information Security Framework.

The study data implies that the hierarchies existing within an organization are very important in determining how effective the information security system is in the face of risks of Attacks on the SCMS. The hierarchical level within the organization was very significant for a factor such as responsibility. Several studies have also developed similar findings, where the system structure is seen as a core contributor to effectiveness of the system. Siponen, (2000) who demonstrated that the dispersal and structure of a system has an impact on its effectiveness, conducted one such study.

The effectiveness of an ERP information security system in a way depends on awareness within the organization's members. Nowadays, most organizations have established Information system security systems whose capabilities are dependent on various factors. While appreciating the various scenarios, it is upon management to inform individuals about the limitations, capabilities, and countermeasures it has put in place to counter threats. The present literature has emphasised on the importance of employees understanding the Information System (IS) security framework in their company. It is also important for the employees to know the repercussions of their actions as they implement and use the information system. All this is part of an effective system, and as Siponen (2000) says, awareness of the information security is essential for use and interpretation of system procedures, technologies, and policies.

There is another aspect to information awareness; that of varying compliance to procedures and rules. As the findings show most of the employees are aware of the IS programs. However, the user's beliefs and assumptions are also instrumental in making the program successful. The level of security awareness may influence the way members behave when handling security programs. From the case study data, it is evident that some members are not exposed to IS programs. In addition, other members are completely aware of the programs. However, the question of whether the security programs are in line with the members' beliefs and understanding surfaces. The organization must dig deeper to understand such factors for the effective Implementation of an Information Security Framework in the prevention of Cyber Attacks on the ERP system.

5. CONCLUSIONS

This study demonstrated several things that contribute to the effectiveness of the Implementation of a COBIT 5 Information Security Framework in the prevention of Cyber Attacks on SCMS. Firstly, there is the issue of management of rules, responsibilities, and policies. Secondly, the hierarchical structure within the organization played a crucial role in the effectiveness of the IS system. This is because this factor determined how much and which personnel are involved in decisions related to IS. This structure seemed to define the roles played by managers, whether at the top or mid-level. Employee awareness about the working and importance of the system is also critical for an effective COBIT 5 IS security system. The related themes as indicated in the current study have an effect on the deployment and maintenance of a healthy IS security system in this organization. The role managers play in the effectiveness of the IS security system is highlighted as this looks at the people component within the organization. Managers belong to the category that sets up the IS security framework.

Generally, the results in this study suggest that managers are very instrumental in the overall security of information system, since they influence the approach taken by other employees. These findings are consistent with what Ramachandran et al (2008) found on the development of an information security environment within an organization.

The overall perspective from this study is that a conglomeration of factors, which are interrelated, influences IS management. The findings showed that management practices might have a positive impact on the effectiveness of the Implementation of the COBIT 5 Information Security Framework in the prevention of Cyber Attacks on the SCMS. Good management ensures a safe working environment where users are discouraged from information disclosure, sharing of passwords, and other negative behaviours.

Looking at the countermeasures put in place by the organization, it was evident that this aspect also plays a significant role ensuring effectiveness of the system. Management and technological initiatives are used to control access to the information system. Technological measures such as access controls and intrusion detection are a key feature of the organization IS security framework. Considering the initiatives mentioned here, information security management becomes very effective if technical countermeasures supplement management actions. For such a scenario to prevail there must be a workable relationship between decision makers, employees, relevant standards, technical aspects, and policy frameworks.

The research shows that SCMS are a vital tool in the modern business world. This technology is one of the engines that keep the market economy pulsating, while positively impacting on people's lives. Irrespective of the system's sophistication, the SCMS has become a target of cyber threats, stemming from malicious hackers, who use deadly malwares to achieve their goals. However, the findings in this paper set out to validate the effectiveness of the implementation of the COBIT 5 information (IS) security framework in the prevention of Cyber Attacks on SCMS.

REFERENCES

Almadhoob A and Valverde R (2014), A cybercrime prevention in the kingdom of Bahrain via IT security audit plans, *Journal of Theoretical and Applied Information Technology*, 65(1) pp 274-292

Boyson, Sandor; Corsi, Thomas; & Rossman, Hart. Building a Cyber Supply Chain Assurance Reference Model. Science Applications International Corporation (SAIC), 2009.

Gratton, C. and Jones, I. (2004), "*Research Methods for Sport Studies"*, Routledge and Taylor.

Grittner Detlef and Valverde Raul (2012), An object oriented supply chain simulation for products with high service level requirements in the embedded devices industry, International Journal of Business Performance and Supply Chain Modelling, 2012 Vol.4, No.3/4, pp.246 - 270.

Kraus C. and Valverde R. (2014), A data warehouse design for the detection of fraud in the supply chain by using the Bendford's law, *American Journal of Applied Science*, pp 1507-1518.

Ramachandran, S. (2008). Information security cultures of four professions. Hawaii internationalconference on system sciences, proceedings of the 41st annual, Hawaii.

Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*,*8*(1), 197-210.

Stephens, J., and Valverde, R. (2013), Security of E-Procurement Transactions in Supply Chain Reengineering. Computer and Information Science, Volume *6* No. 3, p1.

Talla M. and Valverde R. (2012), Data oriented and Process oriented Strategies for Legacy Information Systems Reengineering, ACEEE International Journal on Information Technology, Volume 2 No. 1.

Valverde, R. (2008). The ontological evaluation of the requirements model when shifting from a traditional to a component-based paradigm in inform ation systems re-engineering. DBA Thesis, University of Southern Queensland.

Valverde R and Saade R. (2015), The Effect of E-Supply Chain Management Systems in the North American Electronic Manufacturing Services Industry, *Journal of Theoretical and Applied Electronic Commerce Research*, Volume 9, Number 3.

Valverde, R., Saade, R. and Talla, M. (2014). ITIL-based IT service support process reengineering. *Intelligent Decision Technologies*, 8(2), pp.111-130.

Valverde R. and Talla M. (2012)a Risk Reduction of the Supply Chain Through Pooling Losses in Case of Bankruptcy of Suppliers Using the Black–Scholes–Merton Pricing Model: In: Chaubey P. Yogendra (ed) Some Recent Advances in Mathematics and Statistics, World Scientific.

Valverde, R and Talla Ma. (Editors) (2012)b Information Systems Reengineering for modern business systems: ERP, SCM and E-commerce management solutions. Information Science Reference (IGI Global), Hershey PA, USA.

Valverde, R. Toleman, Mark and Cater-Steel, A. (2011) A method for comparing traditional and component-based models in information systems re-engineering. Information Systems and e-Business Management, 9 (1). pp. 89-107.

Watson C. (2009) ' CobiT Security Baseline Applied to Business Web Applications, A Practical Approach for All Sizes of Organizations', *ISACA Journal, volume 4*.

Wiesmann A. et al. eds. (2005) A Guide to Building Secure Web Applications and Web Services, 2.0 Black Hat Edition, Free Software Foundation. [Online] Available: https://www.owasp.org/index.php/Category:OWASP_Guide_Project (Accessed: 23rd November 2013).