ISSN NO. 2320-5407

Journal homepage:http://www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH

RESEARCH ARTICLE

Risk Assessment & Mitigation Strategies of ERP Implementation for Supply Chain Management

Richie Das, Seema Kumpawat, Samrudhi Maknikar, Vivek Kumar, Ashish Lamba, Dr. PritiPuri
Symbiosis Centre for Information Technology, Pune India

Manuscript Info

Manuscript History:

Received: 18 September 2015
Final Accepted: 22 October 2015
Published Online: November 2015

Key words:

Enterprise Resource Planning (ERP), Supply Chain Management system (SCM), Main Frames (R/2), Risk Mitigation, Vulnerabilities

***Corresponding Author**

Richie Das

Abstract

This article is based on the Enterprise Resource Planning (ERP) implementation of Supply Chain Management system (SCM) that can help the enterprise to face the current challenges in global market efficiently and handling the issues. Companies implement ERP system to integrate their business process. This paper attempts to highlight different factors need to be addressed for implementing ERP system.

In this paper, we have tried to provide some vulnerability, risks due to those vulnerabilities, risk impact to the organizations and mitigation strategies in the process of ERP implementation.

INTRODUCTION

Why Enterprise Resource Planning (ERP)

ERP implementation helps to integrate various departments of an organization like HR finance, sales, Controlling and purchase; all the operations are integrated to centralized database which helps the organizations heads to take decision at right time. Enterprise usually wants to create such a tool and tailor it to the company’s precise needs without performing custom application development. Hence Enterprise need to approach for ERP implementation partner, that provides solution of composite Enterprise services which glue together to provide a sales order cockpit. (Derevensky, 2013)

By implementing ERP some advantages are as -cycle time of manufacturing will reduced , production cost and inventory overhead will also be reduced. Manpower reduction, procurements transparency increase, and supply chain process will be faster. According to market change response will be faster, better resources utilization, customer satisfaction and global reach are some other key benefits of using ERP. (Derevensky,2013)

Factors to be considered for an ERP implementation:-

Cost: ERP implementation require high budget to be implemented. If the requirements are not properly discussed and disclosed to the ERP implementation partner at planning phase then it may cause cost overheads.

Detailed analysis of an organisation’s vision and needs: A company should have clarity in understand its business process/requirements for implementing ERP. While implementing ERP the organization must understand if its Enterprise is flexible enough so that it can be mapped to Enterprise system. .

Appropriate and timely training and education of employees:-

Training/educating the user of the system/ Employees in an organization for how to use the system (ERP) on business process is essential.

Top management support: ERP implementations require full support of the management for sanctioning the budgets for procurement of ERP. They need to align the strategic business goals to the projects.

Effective communication:

For ERP implementation, communication is very critical feature. Communication of expectations at every level should be there. Expectations, education and communication management are critical features during the organization (Wee, S. 2000), (Fiona Fui-Hoon Nah and Janet Lee-Shang Lau,2001)

Main Frames (R/2) to Enterprise Central Component (ECC)

Earlier enterprises enable its production activity using a legacy system mainframe, but gradually due to increase in global competition R/2 system lacks. In providing integration and serving the customer at right time, it also creates delay in decision making. Enterprise Central Component (ECC) security parameters are also better than R/2 systems. ECC facilitates business planning, information sharing, and decision making on an enterprise-wide but R/2 were not supporting this features.

While implementing SCM using ERP some of the following Vulnerabilities, Threats, Risks and the Risk impact rating, we found: (We are referring NIST 800-30 for creating this table)

Risk No	Vulnerability	Threat	Risk Rating & Risk summary	Overall Impact	Risk Mitigation/Controls
(1)	Misrepresentation i.e. substandard electronic components The product received is of inferior quality compared to that quoted by the vendor.	Inexperienced employees (accidental)	**moderate** This includes misrepresentation of electronic parts. This is electronic component Counterfeiting which is kind genuine owner's trademark rights infringement. Due to lower quality and specifications, these parts can create hazard when used with critical machinery. (SAE,2013)	High	Ensure proper auditing of all the electronics component and machineries , appropriately checking all the representation numbers etc.
(2)	Insertion of Malicious code or components which can be replacement, modification and malware insertion on hardware, software or firmware level in Information and communications technology system. This insertion can be done on data which is the part of design, documentation (manuals),roadmaps and architectures. (John F. Miller ,2013)	Competitors, Hackers	**HIGH** Direct impact on production, loss of confidentiality, integrity and availability	High	The company should follow proper policies and procedures before acquisition of any new hardware or software. Also Intrusion Detection System and Intrusion Prevention System should be in place providing an efficient security check.
(3)	Ice Fog Attack This attack has a nature to store the victim's encrypted logs. These encrypted data can help to attacker to	Competitors, Hackers, Disgruntled employees	**MODERATE** Confidentiality and data loss	High	Encryption algorithm should be strong enough. All the devices PCs, laptops should be under network surveillance,24/7 monitoring should be

	find out his targets and victims. Hackers can also collect confidential data and hijack passwords to get in internal and external victim's network. Improper antivirus patch updates (Press Releases,2013) Kaspersky Lab)				there. Periodic OS patch update and antivirus update should be there. Also they should ensure secure firewall implementation.
(4)	Stuxnet virus Flaws in firewall implementation (Levi Ram,Dombe Ami Rojkes-2014)	Exploiters by outsiders and insiders	**MODERATE** Stuxnet virus are designed to attack the industrial programmable logic controllers, they have the capacity to disrupt the assembly lines ,machinery of factories It is possible that if a computer is connected to supply chain and it is not on network still stuxnet attack can be possible. (Levi Ram,Dombe Ami Rojkes-2014)	Moderate	Proper implementation of firewall and installation with appropriate guidelines. USB ports should be disabled to improve prevention of Stuxnet virus.
(5)	Improper Intermediate document(IDOC) creation	Exploitation by competitors and hackers	**MODERATE** Improper IDOC naming convention will cause ambiguity, and keep sender and receiver unidentified. In such cases someone who is familiar to this IDOC pattern can easily manipulate and redirect it towards the destination port of exploiter.	Moderate	While creation of IDOCs the ABAP code should go through adequate peer review process. Proper IDOC naming is required.
(6)	Intrusion Logic bombs in VPN algorithm.	Competitors and network hackers	**MODERATE** Competitors and hackers can enter into the network in the absence of proper Intrusion Detection System and Intrusion Prevention System and can exploit the algorithms according to their desires.	High	24/7 Monitoring by network team. Proper Intrusion Detection Systems and Intrusion Prevention Systems implementations should be there along with logs maintenance.

(7)	Improper ERP implementation	Disgruntled employee	**HIGH** ERP implementation procurement is time-consuming if the proper knowledge of requirement and there is absence of expertise then ERP implementation in worst situation may also lead to bankruptcy. There are many factors to implement ERP should be considered and if these factors are not taken care it can prove dangerous to organization.	High	Procuring an ERP system after considering all possible requirements and functionalities and then implementing it with full proof planning and under expert guidance.
(8)	Laying of Active key / digital token key	Competitor s	**MODERATE** Lying of Digital token in public place can easily theft by any person. Using of those token numbers can help the hacker to enter the organization network, thereby accessing the information asset.	Moderate	Organization should enforce mandatory security training to employees in order to make employees responsible and aware of the security issues.
(9)	Migration across platforms	Accidental or intentional exploitation	**MODERATE** When migration is done across cross platform, the existing applications should be coded in such a way that the new platform will support it. If this is not the case the real time users will not be able to access the information with additional functionalities that may lead to delay in decision making.	High	Selection of modules is to be done carefully so as to match with the required functionalities when migrating.
(10)	Spy satellite to monitor the system	Producers of same kind of consumer product, Hacker	**HIGH** • The hacker can reach out to the spy software and if he is well averse with the software he can manipulate to	High	All the functioning should be monitor through high end security satellite which provides proactive and reactive monitoring in case any issue happens, incident should be reported production support team.

			get the monitoring data. • He can also reach out to a supplier of the company there by negotiating for common interest to plant a spy satellite within the good when the supplier will transfer goods to the company		
(11)	Untrained access management team	Disgruntled employees	**LOW** If the access for the application is given to an employee's more than require for his role. E.g. Developer getting access to production environment.	Moderate	Appropriate and periodic training and learning Role based permission
(12)	Vendors Provider for different products and services (third party vendor) Multiple vendors	Disgruntled Vendor	**HIGH** Confidential data is hacked and it can be given to the competitor. And then company will face loss of trust of customers, loss in revenue and loss of reputation of company. Risk involved in IT Outsourcing	High	Best of Breed Selection :In multivendor environment organization should approach to such vendor which has on premise implementation of ERP and has adequate understanding of the organizational requirement
(13)	Communication gap between service provider representative and client side employees.	Disgruntled vendor	**HIGH** It can lead to failure of ERP implementation completely leading to heavy loss of business revenue. Delay in delivery Increase in Budget Risk involved in IT Outsourcing	High	Support vendor to conduct enough interviews with employees, interacting with department representative Requirement Clarity Through clients

Recommendations

1) Following proper policies, procedures and Master Services Agreement (MSA), timely Inspections, Internal/External Audits.

2) Implementing Intrusion Detection and Intrusion Prevention Systems.

3) 24/7 network and logs monitoring.

4) Adequate Training to staff/Users/Employees.
5) Implementing ERP after sufficient study about requirements and planning of proper procurement process.
6) Proper Communication with ERP service Provider and support from higher management

Conclusion

This paper provides knowledge about risk assessment and mitigation during ERP implementation for Supply Chain Management. Although ERP implementation incurs a lot of cost but wise analysis and step by step risk assessment and mitigation will help the organization in long run. In our paper, we have explained some challenges to ERP implementation to organizations. We have identified almost thirteen vulnerabilities, associated threats, risk, impact and mitigation plans for them. Although we have tried to cover some important risks but always there may be some more.

References

1. Seth Derevensky (2013): ERP implementation: Top 10 Critical Success Factors-Part One http://www.iracst.org/ijrmt/papers/Vol2no22012/14vol2no2.pdf
2. Press Releases(2013) Kaspersky Lab Exposes "Icefog": A New Cyber-Espionage Campaign Focusing on Supply Chain Attacks http://en.prnasia.com/story/86653-0.shtml
3. Levi Ram,Dombe Ami Rojkes-(2014)The Supply Chain Silent Threat – Cyber Attack http://www.supplychain247.com/article/the_supply_chain_silent_threat_cyber_attack/security
4. John F. Miller (2013)Supply Chain Attack Framework and Attack Patterns http://www.mitre.org/sites/default/files/publications/supply-chain-attack-framework-14-0228.pdf
5. SAE,(2013), Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition http://standards.sae.org/as5553a/
6. Fiona Fui-Hoon Nah and Janet Lee-Shang Lau,(2001),Critical factors for successful implementation of enterprise systems http://faculty.cbu.ca/pifinedo/NAH.pdf
7. Wee, S. (2000), ``Juggling toward ERP success: keep key success factors high'', ERP News, February, available http://www.erpnews.com/erpnews/erp904/02get.htm