academicJournals

Vol. 9(6), pp. 243-258, 28 March, 2015
DOI: 10.5897/AJBM2013.7308
Article Number: 60A7A0351964
ISSN 1993-8233

http://www.academicjournals.org/AJBM

African Journal of Business Management

Full Length Research Paper

Information technology and e-risk of supply chain management

T. N. Varma* and D.A. Khan

Department of Computer Applications, National Institute of Technology, Jamshedpur, India.

Received 6 December, 2013; Accepted 2 March, 2015

Application of information and communication technology (ICT) is exponentially growing in Supply Chain Management (SCM) for increasing productivity and profitability in business. This growth of Information Technology in SCM has changed the paper based environment to Virtual Supply Chain, which is also generating electronic risks (e-risks) in form of cybercrime or fraud. Although, reducing the e-risks from huge data generated in day to day operation of supply chain networks is a big challenge for decision makers, auditors, detecting and investigating agencies. We know that technology is always a double-edged sword which can be reciprocally used for prevention of e- risks in SCM. The purpose of these empirical studies is to discuss the IT application and trend to curb the supply chain's e-risks.

Key words: e-risk, information technology (IT), supply chain management (SCM)

INTRODUCTION

In the last decades, organizations were reluctant to share the data due to leakage of their trade secret of business. However, organizations are bound to rapidly adopt the use of the Information Technology in their Supply Chain Management for survival at global market place due to globalization. Supply chain management (SCM) is an integrated and complex network concept that refers to the sum of all the processes starting from the procurement of the raw material from the manufacturer/producer and ending with delivery of the end-product to the consumer (Silver et al., 1998). Due to increased complexity of data, uncertainty risk in supply chains is growing (Christopher and Peck, 2007; Hillman and Keltz, 2007), leading to an increasing vulnerability of electronic risks (e-risks). The IT enabled SCM can easily manage the flow of information with key business processes, materials, money within and outside the networks and contribute to firm profits by improving quality and by reducing coordination costs and transaction risks (Stroeken, 2000; Mabert et al., 2001; Sanders and Premus, 2002). Rigorous use of information technology in supply chain is also generating chance of cybercrime as "computer-assisted" such as hacking, phishing and "computer-focused" as hate crimes, telemarketing/internet fraud crimes. Widely used terms for crime involving computers are computer crime, computer related crime, computer misuse, cybercrime, digital crime, e-crime, internet crime, online crime etc. Therefore, IT is considered a critical prerequisite for managing supply chain (Davenport and Brooks, 2004).

According to the 2012 Report of the Nations

*Corresponding author. E-mail: tpverm@yahoo.com.

on Occupational Fraud and Abuse, published by the Association of Certified Fraud Examiners (ACFE), $3.5 trillion worth of fraud occurs every year. Organizations are spending money and time to detect, investigate, analyze and prevent it. Investigators and detecting agencies are forced to wade through massive amounts of data, which potential perpetrators count on to shield them from detection and prosecution. Many researchers discussed on the strategies, techniques and technologies for the design and development of SCM, survey papers on taxonomy of SCM, and modelling and analysis of SCM. There is a very few literature survey article that deals with generation and prevention of e-risks by IT in SCM. However, a comprehensive survey of IT in SCM will be useful to identify and prevent the e-risks. Also, some future research directions are indicated for developing IT embedded SCM system for fraud detection to reduce the e-risks. Section 2 discusses brief review of the literature. The details of the research methodology are presented in Section 3.Section 4 presents the classification of previous literature on the basis of different IT applications in SCM. A classification scheme for different type of e- risks (cyber crime) due to IT application and its detection and prevention through IT is presented in Section 5. In Section 6, a framework has been developed for the application of IT in SCM. Finally, discussion and conclusion are presented in Section 7.

BRIEF REVIEW OF LITERATURE

The development of information and communication technologies (ICT) that include Electronic Data Exchange (EDI), Radio Frequency Identification (RFID), Bar Code, Electronic Commerce, Decision Support system, Enterprises Resource Planning (ERP) package, the Internet and World Wide Web etc. had developed the complex and dynamic SCM. Researchers comment on this phenomena as beginning of an evolution in supply chain towards online business communities (Armstrong and Hagel, 1996), internet as the foundation for new business models, process and new ways of knowledge distribution (Laudon and Laudon, 2000).This arose for the application of IT in SCM. However, relation between IT and SCM was discussed as internet increases the richness of communications through greater interactivity between the firm and the customer (Watson et al., 1998), IT as cures for Bullwhip effect in Supply Chains (Lee et al., 1997), internet as the foundation for new business models, process and new ways of knowledge distribution (Laudon and Laudon, 2000), applications of radio frequency identification (RFID) in supply chain (Gould, 2000), electronic data interchange (EDI) (Ngai and Gunasekaran, 2004), inadequate enterprise without IT systems (Davenport and Brooks, 2004), e-commerce applications (Chou et al., 2004), enterprise resource planning (ERP) (Davenport and Brooks, 2004), mobile agent technology, as applied in an E-commerce application (Patel and Garg, 2004), online ordering (Kull et al., 2007),SCM and IT (van Donk, et al., 2008), spread sheet based vendor (Mahamani and Rao, 2010) , role of IT in SCM environment (Prasad et al., 2010), importance of e-procurement for an information technology chain (Ronchi et al., 2010), SCRM approach for risk mitigations (Tummala and Schoenherr, 2011), e-commerce depending on information infrastructures and telecommunications for its development (Gilaninia et al., 2011), RFID for SCM (Nair, 2012), e-supply chain and software agents (Nair, 2013), excel function as supply chain fraud detector (Varma and Khan, 2014) etc. The literature survey was primarily aimed to help researchers and practitioners in implementing a successful IT system for achieving an e-risk free SCM.

RESEARCH METHODOLOGY

Random data have been collected primarily through e-journals search engines available in intranet or organisational library that are in the areas of general, IT, fraud, cyber crime and supply chain management as shown in Table 1. The study was conducted for a review of e-risks (Cybercrime or fraud) which has been generated due to the application of IT tools and technique. Further, journal articles related to detection and prevention of e-risks in IT enabled SCM were reviewed.

Review of previous research on IT in SCM

Different IT applications in SCM have been reviewed based on the available literature in this area (Table 2).

Classification of cyber crimes and its causes, prevention

The aim of classification of literature is to identify different types of e-risks (Cyber crime) generation cause related to IT enabled SCM (Table 3). Further classification was related to IT tools and technique for detection and prevention of cyber crime and suggestion for future research directions was also aimed.

Electronic records management (ERM)

Virtual business transactions through Automatic identification (Auto ID), Electronic Data Interchange (EDI) and Enterprises Resource Planning (ERP) Systems are collectively known as Electronic Records Management (ERM).The objective of ERM implementation in SCM is to ensure the accountability of process flow, which is fruitful to reduce cybercrime risks (e-risks) generate during the e-communication.

Table 1. Random data on e-journals search engines.

Name of journal	No of article reviewed
African Journal of Business Management	1
Automotive Manufacturing & Production	1
Artificial Intelligence Review	1
Business Horizons	1
Business Process Management Journal	1
Computers and Electronics in Agriculture	1
CSI Communications	2
European Accounting Review	1
European Journal of Operational Research	1
Expert Systems with Applications	1
Industrial Management & Data Systems	1
Information Management	1
Integrated Manufacturing Systems	1
International Journal of Business Performance and Supply Chain Modelling	1
International Journal Of Computational Engineering Research	1
International Journal of Management and Enterprise Development	1
International Journal of Flexible Manufacturing Systems	1
International Journal of Operations & Production Management	3
International Journal of Physical Distribution & Logistics Management	2
/nternational Journal of Production Economics	1
International Journal of Production Research	1
International Journal of Research in Management	1
International Journal of Security and Networks	1
Int J. Technology Management	1
Interdisciplinary journal of contemporary research in business	1
IUP Journal of Supply Chain Management	1
Journal of Business Logistics	2
Journal of Enterprise Information Management	1
Journal of Operations Management	1
Journal of Purchasing and Supply Management	1
Managerial Auditing Journal	2
Management Science	1
Serbian Journal of Management	1
Supply Chain Management: An International Journal	1

Bar code and scanner

Since many decades, the use of barcode for item-level identification, verification of orders at receiving and shipping etc in SCM is a mature automatic identification (auto-ID) technology. Barcode has become the "ubiquitous standard for identifying and tracking products" (Wyld, 2006). This is commonly used in product identification, speeds data entry, enhances data accuracy, minimizes on-hand inventory, improves customer service, reduces product recall, reduces work-in-process idle time, monitors and controls shop floor activity, improves shop floor scheduling, optimizes floor space, improves product yield, reduces scrap, attendance recording, ATM card, debit and credit cards in banking organizations. Bar code helps us to reduce risk in supply chain which is rising due to manual oversight or fraudulent data entry by insider. Bar codes duplicity in process generate e-risks, which can be eliminated by application of biometric authenticity and authorizations. But there is a risk of data diddling which is performed by unauthorized modifications of data prior or adding fraudulent data during input or altering/omitting the desired input data or wrongly posting a transaction, making alterations or additions in the master file records, posting the transactions partially, destroying the output and substituting the counterfeit output or entry of a virus that changes data, the program, the database or application, exchanging valid disks and

Table 2. Different IT applications in SCM.

Criteria	Reference
Electronic Records Management (ERM) in SCM	Mount and Caulfield (2001), Graham (2002), Sanchez and Perez, 2003, Coronado , et al. , 2004, D'Avanzo et al.,2004, Michael et al., 2005, Wyld, 2006, Attaran, 2007,Garcia-Dastuge and Lambert,2007,Sabbaghi et al., 2008,Chandan et al., 2009,Jedermann et al. 2009, Fosso Wamba, S,2012
Enterprises Resource Planning	Sandhu et al., 1996, Van deRiet et al. , 1998, Coderre (1999), Little et al., 2003, Kuhlmann et al., 2003, Boyle, 2004, Davenport and Brooks, 2004,Gara,2004, Schlegelmilch and Steffens, 2005, Panigrahi (2006), Vaidya et al., 2006, Moon, 2007, Zhang et al., 2007AICPA,2008, Huang et al., 2008, Vaidya et al., 2008; Albrecht et al., 2009, Kuhn et al. 2010, ISO17799
E-business	Bauer et al., 2001,Geoffrion and Krishnan ,2001,Boone and Ganeshan 2007
Electronic Supply Chains (ESC)	Gunasekharan et al, 2004,Sammon et al, 2007
Electronic Commerce	Ramya S. Gowda,2013
Mobile agent	G. P. Picco 2001, Patel R.B. and Garg K. 2004
Spread Sheet, data mining	Ghosh and Reilly ,1994, L. Delamaire, H. Abdou, and J. Pointon,2009, Varma, T.N. and Khan , D.A.,2014
XML (extensible markup language)	Ameron,2000,Nurmilaakso et al. ,2002,Simchi-Levi et al., 2003W3C, XML Schema Part 0, 2004; W3C, XML Schema Part 1, 2004; W3C, XML Schema Part 2, 2004,
Computer Assisted Auditing Tools and Techniques (CAATTs)	ACL,2006, C. Dowling and S. Leech,2007, D. Janvrin, J. Bierstaker & D. J. Love 2008

tapes with modified replacements into a computer or computer system by anyone associated with the process of creating, recording, encoding, examining, checking, converting and transporting data into a computer.

Radio frequency identification (RFID)

Radio frequency identification (RFID) is an IT revolution in which information exchange system that can create an environment in every object can be automatically recognized, tracked, and traced from factory to shelf only using a single tag on each product item or pallet (Jones et al., 2004; Jones, Clarke-Hill et al., 2005; Lai et al., 2005; Ranky, 2006; Sellitto et al., 2007). By adopting RFID technology, supply chain can be enhanced by visibility into customer needs, efficient business process, reliable and accurate order forecasts, productivity improvement, operating cost reduction, better tracking, counterfeit identification and theft predication (Attaran, 2007). RFID includes authentication (Coronado et al 2004), reducing channel volume and enhancing forecasting and planning capabilities (D'Avanzo et al., 2004) of the next revolution in supply chain (Srivastava, 2004). Amcor uses RFID for managing the warehouses (Michael et al., 2005); Wal-Mart began setting deadlines for suppliers to start using RFID tags on their shipments in 2003 (Coronado et al., 2004). Suppliers are able to manage product recalls and return of faulty and defective materials by using RFID through its Electronic Security Marker (ESM) (Sabbaghi et al., 2008), wireless automatic identification and data capture (AIDC) technology (Fosso Wamba et al., 2008) that allows end-to-end supply chain item level tracking and tracing, adoption by Indian Retailers (Chandan et al., 2009). RFID is an emerging technology that is being increasingly used in logistics and supply chain management in recent years (Jedermann et al., 2009), reduce the risk of counterfeiting (Gao et al., 2004), products anti counterfeiting strategies, enhanced product recall, reverse logistics, and total inventory management (Bardaki, C., K. Pramatari and Oukidis,2007), technology in the supply chain (Sarac et al., 2010), internet of things (Calia, 2010), support of intra- and inter organizational business transactions (Wamba, 2012). There is different attacks as skimming attack (when RFID tag are read directly without anyone knowledge), eavesdropping

Table 3. Classification of cyber crimes.

Cyber crime*	Cause due to IT in SCM	Detection and prevention through IT
ATM/EDI/ Credit Card fraud	Bar code, Electronic Data Interchange, RFID,ERP, e-mail, Internet	Bar code, RFID, Data Mining, Cryptography, Biometric, GPS , EMV card standard or PIN technology
Cyber terrorism	Internet, e-SCM, Web application	ERM, Data mining
Criminal breach of trust/Fraud	All application of IT	Excel sheet, ERP, Data mining
Data Diddling	ERM,ERP, Database of SCM, Web application	Bar Code,
Denial of Service attacks, Web-jacking	Internet, ERP	Antivirus, auto-analysis of legitimate usage patterns, Firewall and intrusion Detection system
Destruction of electronic evidence	Internet, ERP	Antivirus, auto-analysis of legitimate usage patterns, Firewall and intrusion Detection system
Cyber Stalking	Internet, ERP	Antivirus, auto-analysis of legitimate usage patterns, Firewall and intrusion Detection system
E-mail bombing, spoofing , Phishing ,Spam	Internet, e-SCM	Anti-virus, auto-analysis of legitimate usage patterns
False electronic evidence	EDI, e-commerce	Firewall and intrusion Detection system
Forgery of electronic records	EDI,RFID, ERP	Cryptography, computer forensics
Identity theft	Internet, ERP	Authentication and authorization check, Firewall and intrusion Detection system
Illegal Access (Hacking, Cracking)	Internet, ERP	intrusion detection and risk mitigation, authentication and authorization check
Illegal data acquisition (Data Theft or Alteration)	Internet, ERP	data integrity verification,
Intellectual Property theft	Internet, ERP	data integrity verification, authentication and authorization check

Table 3. Contd.

Logic Bomb	Internet, Web application	Firewall and intrusion Detection system, authentication and authorization check
Money-laundering	e-commerce, Web application	Data mining
Privacy violation	Internet, Web application	Firewall and intrusion Detection system, authentication and authorization check
Salami attacks	Internet, Web application, RFID	RFID, Firewall and intrusion Detection system, authentication and authorization check
Sending threatening/ defamatory messages by e-mail	Internet, Web application	Mobile agent, Firewall and intrusion Detection system, authentication and authorization check
Spreading or Dissemination of Malicious Software (Malware), Virus attacks	Internet, ERP	Mobile agent, Firewall and intrusion Detection system, authentication and authorization check

* Terms explained in Appendix I

attack (attacker sniffs the transmission between the tag and reader to capture tags data) man-in-the-middle attack (a fake reader is used to trick the genuine tags and readers) and physical attack which requires expertise and expensive equipment takes places in laboratory on expensive RFID tags and security embedded tags (Mahinderjit-Singh and Li, 2009, 2010).The RFID tags play a significant role, as the latest form of artificial security tags, which can easily be integrated with existing chains and reduce counterfeiting. RFID helps the organization to avoid duplication of items, as the tags are unique and authenticated. It can also reduce the chances of fraud generated by manipulation in entry, authorization from the supplier to customer because of cloning become non existence. Cost and implementation constraints secure RFID tags and smart cards require specialized cryptographic implementations with Global Position System (GPS).

Electronic data interchange (EDI)

Electronic Data Interchange (EDI) is also called "paperless exchange" (Nagpalet al., 1999), in which there is computer to computer interchange of business documents and/or information in standard, structured, machine retrievable data format (computer can process the information without human assistance) (Sanchez and Perez, 2003) between separate computer systems, using a standard structured format (ANSI ASC X.12 in the late 1970s and EDIFACT in the 1980s). It was the replacement of the traditional forms of mail, courier, or fax. SAP's exchange infrastructure (White Paper, SAP Exchange Infrastructure 2.0, 2002; White Paper, SAP R/3 Enterprise, 2002; White Paper, SAP Exchange Infrastructure 2.0 Technical Infrastructure, 2002) has been in place for many years as the footstone of all ERP technologies. It was used for the paperless communication within supply chain network to share transactional data (Garcia-Dastuge and Lambert, 2007), order processing, inventory controlling, accounting, transportation, quick access to information, better customer service, increased productivity, improved tracing and expediting, etc. EDI is also tremendously beneficial in counteracting the Bull Whip effect and supply chain organizations can overcome the distortions and exaggerations in supply and demand information by using technology to facilitate real-time sharing of actual demand and supply information.

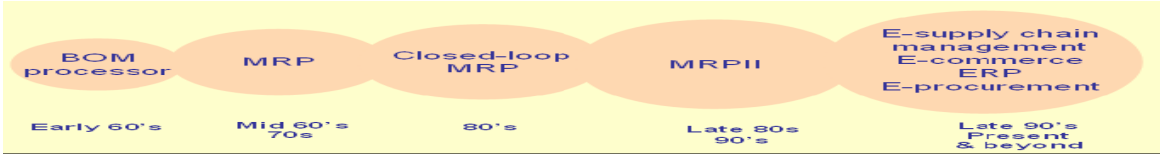

Figure 1. Evolution of e-supply chain.

Smart card

A smart card can generally be defined as a plastic card with dimensions similar to traditional credit/debit cards, into which an electronic device has been incorporated to allow information storage. Frequently, it also has an integrated circuit with data processing capacity.

E-business

e-business is "the use of the Internet or any digitally enabled inter- or intra-organizational information technology to accomplish business processes" (Boone and Ganeshan, 2007). As classified by Geoffrion and Krishnan (2001), e-business consists of three areas: (1) consumer oriented activity i.e business-to-consumer, consumer-to-consumer, and government-to-consumer activities, (2) business-oriented activity i.e; business-to-business, business-to-government and government-to-business activities and supported by (3) the e-business technology infrastructure i.e; network infrastructure, network applications, and respective software tools and applications. The key tools and methods of e-business include EDI (electronic data interchange) and XML (extensible markup language), buy-side e-business applications, sell-side e-business applications, digital market places, Item identification and Content management (Bauer et al., 2001). If e-business is not properly secured then illegal data acquisition is performed by cyber criminals. There is law for copyright protection or protection from data or intellectual property theft in every country.

Electronic supply chains

Electronic Supply Chain (ESC) is a supply chain that is electronically managed in form of EDI-based or Internet based between or among participating organization. Basically it is a virtual supply chain, which links organizations to allow them to buy, sell and move products, services and cash by using internet-based applications to transact and exchange information with their downstream or upstream. American-On-Line and lastminute.com have achieved innovative results using ESCs (Gunasekharan et al., 2004). In this collaborative planning, forecasting and replenishment (CPFR), Vendor Managed Inventory (VMI), Efficient Customer Response (ECR) and Quick Response have been easily managed. Intel began to recognise the power of the internet as a corporate communication channel by using the internet as "brochureware", to share technical information and market the Pentium processors (Sammon et al, 2007) (Figure 1).

e- procurement

An e-procurement is expected to be integrated into the wider purchase-to-pay (P2P) value chain with the trend toward computerized supply chain management. An e-procurement is done with a software application that includes features for supplier management and complex auctions with value chain consist of Indent Management, e-Tendering. e-Auctioning (The electronic auction (e Auction) is carried out in real time, where participants log in to an auction site using a browser at a specified time and bid for an article as conventional auctions. This is a transparent process and reduces malpractices, Vendor Management, Catalogue Management, and Contract Management. The forms of e-procurement are Web-based ERP (Enterprise Resource Planning): Creating and approving purchasing requisitions, placing purchase orders and receiving goods and services by using a software system based on Internet technology, e-MRO (Maintenance, Repair and Overhaul). It is the same as web-based ERP except that the goods and services ordered are non-product related MRO supplies, e-sourcing; identifying new suppliers for a specific category of purchasing requirements using Internet technology, e-tendering; sending requests for information and prices to suppliers and receiving the responses of suppliers using Internet technology, e-reverse auctioning; using Internet technology to buy goods and services from a number of known or unknown suppliers and e-informing; gathering and distributing purchasing information both from and to internal and external parties using Internet technology. In 1998, Intel launched a global online ordering system that reached a record US$1bn in product orders in the first month of operation. Today, Intel generates over 85 per cent of revenue from online orders and virtually all Intel customers are transacting business with Intel over the internet. Intel is aggressively moving towards paperless

purchase orders, shipment notification and deployment processes. Digital signatures on the documents submitted in electronic form in order to ensure the security and authenticity of the documents filed electronically. This is the only secure and authentic way that a document can be submitted electronically.

Secure electronic transaction/trading/technology (SET)

It is a proposed industry standard for payment card acceptance over the Internet. At the system heart is a pair of digital keys, one public and one private, held by each party to a transaction. In practice, banks will give both keys to a customer together with a digital certificate for authenticity. When customers wish to purchase over the Internet, they firstly give the public key to the merchant along with the certificate to prove its authenticity. Likewise, the merchant provides its own public key and certificates to prove its own bona fides to allow the transaction to proceed. Problems may arise in key distribution and customer identification in order to ensure that accounts and clients match.

Enterprise resource planning (ERP) systems (e.g., SAP, Oracle, Peoplesoft)

Enterprise Resource Planning systems are the IT revolution that emerged in the 1990s. This system is a common term for a co-operating software that manages and co-ordinates much of a company's resources, assets and activities (Boyle, 2004). It includes cost cutting in internal operations, efficiency across the extended supply chain, enhanced customer service and network relationships (Davenport and Brooks, 2004), an enterprise information system designed to integrate and optimise the business processes and transactions in a corporation (Moon, 2007), provides the critical infrastructure necessary for the effective evolution of the assurance function from a periodic event to an ongoing process through the integration of continuous auditing applications (Kuhn et al. 2010). The security aspects in an ERP system are security policy and administrator, user authentication, authorization, time restriction, log and trace, database security etc. (Van deRiet et al. , 1998),role-based access control, segregation of duties, encryption, username and passwords, etc. (Huang et al., 2008; Vaidya et al., 2008; Albrecht et al., 2009) .Fraud can be prevented in ERP system as role based access control, segregation of duties, username and passwords, etc. (Little et al., 2003; Gara,2004), a labor-intensive task requiring time, effort and resources (Wells, 2008) role mining techniques to automatically identify roles from existing permissions assigned to users within an organization (Sandhu et al., 1996; Kuhlmann et al., 2003; Schlegelmilch and Steffens, 2005; Vaidya et al., 2006; Zhang et al., 2007) proactively searching for or finding the indicators (also called symptoms or red flags), suggesting that fraud may be occurring (Albrecht et al., 2006). ERP with cloud computing, mobility and analytics is the next generation.ERP systems are integrated within the core functional modules (e.g., Material Management, Financial and Accounting, Human Resources, Production Planning, Sales and Distribution, Supplier Relationship Management, Customer Relationship Management , Supply Chain Management, etc.). The implementation of ERP in any organisations may create e-risks through failure of proper IT controls over critical application programs, data files /tables, failure to manage privileged user access and default system user accounts (e.g. SAP_ALL), exposure of business sensitive information, lack of segregation of duties, etc. The security issue of ERP system is a challenge for each organization. The different controls in ERP system for any organizations suggested by system implementers are a) IT general controls – access restriction and separation of responsibility to modify/change/delete system parameters, configurations, customizations, and/or master data etc., b) Automated Application Controls – approval of transactions workflow , encrypted data, validation of data upon entry using edits, unique transactions numbers of each process etc, c) Manual Controls – defined segregation of duties, reconciliations of materials and accounts, etc. and d) Hybrid or Computer-Dependent Application Controls – generation of MIS reports, review of audit logs, etc. Organisations are implementing NIST Federal information systems standards, COBIT®, Val IT, Risk IT, ITIL, and ISO17799 to control e-risks in there SCM.

SAP, Oracle and Baan are the market player in ERP systems package with high level of integration by utilizing a single data model, developing a common understanding of what the shared data represent and establishing a set of rules for accessing data. These ERP packages are playing a vital role in organisation to reducing the fraud or e-risks from their Supply Chains.

SAP

Organisations are using SAP solutions for purchase-to-pay, order-to-cash, or HR processes and using third-party tools for fraud detection or using proprietary relational databases. In either case, the need to export data out of the SAP system compromises both data security and governance which limit the amount of data that can be analyzed. SAP announced SAP Fraud Management in year 2013 with HANA platform. This is part of SAP's Governance, Risk and Compliance (GRC) product portfolio, along with Process Control, Access Control,

Risk Management and Global Trade Management, Business Objects and Business Intelligence. These solutions enhanced real-time fraud analysis. SAP HANA detects, investigates, analyzes, and prevents irregularrities or fraud in even ultra-high-volume environments. Some application of SAP is used to detect and prevent fraud in e- environment as false vendor Payment. This is created due to lack of segregation of duties, where vendor creation or modification in bank account number in vendor master , Good receipt notes/ Service Entry Sheet and invoice creation and approval be performed by the same user. It can be easily detected and prevented by defining proper segregation of duties logic.

Web services

The phages of ERP are a) manufacturing applications, b) specialized applications such as supply chain management and c) application of Web services (Thuraisingham, 2006). ERP vendors are introducing the Web scenarios broker hub that will act as a broker between Web services and the ERP software. SAP offers this hub through mySAP and Oracle via its e-business suite.

Electronic commerce (e-Commerce)

Electronic commerce is tool and technique for managing business in a paperless environment. E-commerce includes electronic data interchange (EDI), e-mail, electronic founds transfers, electronic publishing, image processing, electronic bulletin boards, shared databases, and magnetic/optical data capture (such as bar coding), the Internet, and Web sites in form of B2B (Business to Business) as Covisint,B2C (Business to Customer) as Amazon.com, Wal-mart.com, C2B (Customer to Business) as priceline.com, C2C (Customer to Customer) as e-Bay auction, P2P(Peer to Peer) and Mobile, or m-Commerce. In 1995, Intel formed the Internet Marketing and E-Commerce Group (IM&E) to centralize online marketing efforts. In year 2013, Filpkart becomes net Rs. 1200 crores in single largest funding for an e-commerce company in India. Hence it is playing a major role for integrating supply chain management (SCM) and changing the dynamics of business. E-commerce deals with business online; security plays the heart of business. Business needs lots of communication skills which are provided by software agents. Software agents are responsible for customer satisfaction in terms of B2B E-commerce. Software agents can be thus proved as an important entity with respect to E-Commerce. Without Software agents E-Commerce is like “a man having his leg cut” (Ramya, 2013). A software agent is a software system, which has attributes of intelligence, autonomy, adaptability, perception or acting on behalf of a user proactively. The intelligence of an agent refers to its ability of performing tasks or actions using relevant information gathered as buyer agents or shopping bots (retrieving information about goods and services from networks), monitoring and surveillance agents (used to observe and report on equipment, usually computer Systems), user agents or personal agents and data mining agents (finding trends and patterns from information gather from many different sources). Software agents provide security to the information.

XML (extensible markup language)

Structured information contains words, pictures, etc. which play an important role in Supply Chain Networks data flow and a markup language is a mechanism for identifying structures in a document. XML (extensible markup language) is simplification of Standard Generalized Markup Language (SGML) for originally large-scale electronic publishing and standard for exchanging various data over the Web, which is a flexible text format standard developed by the World Wide Web Consortium (W3C). It is useful over other description languages (e.g., HTML) to represent the data format using Document Type Declaration (DTD) schema or XML schema (W3C, XML Schema Part 0, 2004; W3C, XML Schema Part 1, 2004; W3C, XML Schema Part 2, 2004); hence it is applied in many ERP applications. The numbers of applications based on XML documents are large and e-business transactions are only one application area (Ameron, 2000). XML-based solutions provide a significant alternative to traditional EDI and lower the entry barrier to e-business because of the lower investment costs compared to EDI (Nurmilaakso et al., 2002), a cost-effective method of information exchange from system to system between organizations (Simchi-Levi et al., 2003). Initially ERP system was data or information based, which is now transforming into knowledge based system with various representations. Hence there is a requirement of description language, where XML is best choice.

Spread Sheet (Microsoft Excel)

Organizations are using Microsoft Excel as standard desktop software and decision making tools in their Supply Chains, because in comparison of total cost of ownership with commercial software based decision making supporting tool is less. It is also useful to apply in Supply Chain Networks (SCN), because it has many build-in capabilities to perform and execute quantitative modeling techniques. Microsoft Excel is an ever-present tool and easily use for data analysis because spreadsheets are easy to navigate and flexible enough. Excel allows users for applying analytical test (Horizontal and Vertical Analysis, Ratios and Trend Analysis, Performance Measures, Statistics , Stratifications, Aging, Application of

Benford's Law, Regression, Monte Carlo Simulation), Data management/analysis (Append / Merge, Calculated Field/ Functions, Cross Tabulate, Duplicates, Extract/Filter , Export ,Gap Analysis, Index / Sort, Join / Relate, sample, summarize),user forms design, and macros/Visual Basic Applications (VBA). The complexity of supply chains network data allows fraudsters to commit the fraud beyond the scope of internal controls but an effective approach of locating fraudulent on a data-set of supply chain network can be performed by using Benford distribution with help of excel sheet (Varma and Khan, 2012). Here are possibilities of different type of fraud risk in supply chain network as bid rigging, phantom bids, nepotism, substitution, false count, counterfeiting, creating fictitious accounting entities e.g., ghost employee, fake vendor, fake customer or vendor payments, falsified hours etc. We can easily detect and prevent fraudulent activities by help of excel functions (Varma and Khan, 2014).

Data mining

Data mining is a process that uses statistical, mathematical, artificial intelligence, and machine learning techniques to extract and identify useful information and subsequently gain knowledge from a large database (Turban et al., 2007) to uncover hidden patterns and subtle relationships in data and to infer rules that allow for the prediction of future results. Data mining helps the organisations in defining business rules (alerts based on intuition and general experience), anomaly detection (alerts are defined based on events that represent statistical deviation from normal or expected behavior), predictive models (statistical models which derived from event characteristics that are indicators of prior fraud incidents) and social network analysis (alerts are based on the level of association between the current event and individuals or accounts that are known or suspected of fraudulent behavior). Fraud detection has become one of the best established applications of data mining and it is useful to detect credit transaction fraud, telecoms subscription fraud, automobile insurance fraud and the like (Phua et al., 2005), application of data mining to extract and uncover the hidden truths behind very large quantities of data (Bose and Mahapatra, 2001), application of data mining technique in fraud detection such as neural networks (Cerullo and Cerullo,1999), logistic regression models (Owusu-Ansah et al., 2002; Yuan et al., 2008; Panik, 2009), regression analysis (Spathis et al., 2002), Bayes method (Viaene et al., 2004), decision trees and Bayesian belief network (Kirkos et al., 2007).

Computer assisted auditing tools and techniques (CAATTs)

There are a couple of reasons – Increase in use of electronic documents large firms developing computerized decision aids to assist themselves in decision making, customer relationship management and analytical procedures (Dowling and Leech, 2007) and impact of IT on the behavior and attitude of individuals (Janvrin et al., 2008). CAATTs are computer tools used by external or internal auditors as a part of the audit procedures to process significant data contained in organizations information systems. CAATTs can be classified to include the following groups: electronic documents, fraud prevention and detection, information retrieval and analysis, network security, continuous monitoring, audit reporting, database of audit history, computer based training, electronic commerce and internet security. Some of the techniques to detect fraud using CAATTs (KPMG. International, 2006) as calculation of statistical parameters – calculating average, standard deviation to find fraudsters outside the required calculation limit, Pattern classification – to find trends or patterns in data and detect an unusual pattern, Stratification – to identify unusual number of entries, Benford's Law – to identify unexpected occurrences of digits or combination of digits, Joining different diverse sources – to identify invalid columns which match in a dataset but should not be present there, Duplicate testing – to identify duplicate transactions., Gap testing – to identify missing values in sequential data, Validating entry dates or time – to identify transactions during suspicious date or time etc.

Intranet/extranet

The computer networks inside an organisation that are connected via internet based protocols (HTML: HTTP, FTP, Mail: SMTP, POP3) and are not accessible from outside. By using Web browsers and server software with their own internal systems, organizations can improve internal information systems and link otherwise incompatible groups of computers within supply chain networks for reducing manual intervention. Extranet provides secured access to its intranet and to additional information and services that may not be part of its intranet and it is secured via a firewall. Internal networks often start out as ways to link employees to company information, such as lists, product prices, or benefits. Because internal networks use the same language and seamlessly connect to the public Internet, they can easily be extended to include customers and suppliers, forming a supply chain "Extranet" at far less cost than a proprietary network.

Internet

Good supply-chain management is essential for a successful company. Supply chain management can reach beyond the boundaries of a single organisation to

share that information between suppliers, manufacturers, distributors, and retailers. This is where the Internet plays a central role.In terms of advancement in technology and communications capabilities, perhaps the most influential development over the past decade has been the adaptation of the Internet applications into the areas of commerce and mass communications and it provides instant and global access to an amazing number of organizations, individuals, and information sources. A key Internet concern is the issue of privacy regarding the sensitive information, the level of security for information because supply chains members are struggling the challenge of freely sharing the information. The internet is a source for cyber criminals. Internet security was ranked the first concern for customers and supply chain members.

World Wide Web

The World Wide Web (WWW) is the Internet system for hypertext linking of multimedia documents, allowing users to move from one Internet site to another and to inspect the information available without having to use complicated commands and protocols. The number of Web sites relevant to supply chain management is growing at a rapid pace. Enterprise Transportation management was recently launched by Metasys Inc. through the Oracle Web Applications Server; this system deploys a variety of critical information about transportation and distribution applications throughout the supply chain.

Wireless internet

Wireless Internet enables wireless connectivity to the Internet via radio waves rather than wires on a person's home computer, laptop, smartphone or similar mobile device. Wireless Internet can be accessed directly through service providers. Wi-Fi hotspots and wireless LANs are also options for wireless Internet connectivity. In these cases, Internet connectivity is typically delivered to a network hub via a wired connection like satellite, cable, DSL or fiber optics and then made available to wireless devices via a wireless access point.

Groupware (e.g., Outlook, Lotus Notes)

FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46
Lotus Notes has been one of the first complete groupware products to hit the market way in 1989, and ever since it has continued to dominate the Groupware market. Developers of Notes realized the importance of Security quite early, and therefore we see many Industry Standard Security Features built into Notes over and above Security Features unique to Notes. Together, they effectively cover many aspects of Security that are of significant importance today. Even after there is chance of e-mail bomb attack on Supply Chain Network in a form of net abuse consisting of sending huge volumes of e-mail (sending numerous duplicate mails to the same email address) to an address in an attempt to overflow the mailbox or overwhelm the server where the email address is hosted in a denial-of-service attack.

Mobile agent

A mobile agent is a software process, which can move autonomously from one physical network location to another. The agent performs its job wherever and whenever it is found appropriate and is not restricted to be co-located with its client. Thus, there is an inherent sense of autonomy in the mobility and execution of the agent. It is applied in SCM as the delegate of tasks, network load reducer, parallel processing facilitators, code shipper rather than data shipper etc. As distributed system, the mobile agent is subject to security threats such as eavesdropping, corruption, masquerading and denial of service, replaying, and repudiation. Issues such as encryption, authorization, authentication, and non-repudiation, therefore, must be addressed in a mobile agent. Moreover, a secure mobile agent must protect both the hosts and the agents from tampering by malicious activities.

M2M

Machine to machine technology (M2M) allows both wireless and wired systems to communicate with other devices of same ability. The modern M2M communication has expanded beyond a one to one connection and changed into system of network that transmits data to personnel appliances. M2M domains are system monitoring/telemetry, asset tracking, digital signature & advertising and telematics. There are many M2M application in supply chain has been implemented as tracking supply and demand and making informed decisions. Real time monitoring of the process is using sensor that makes operations to detect, predict and ensure smooth process. As the concept of Internet of Things, M2M will solidify in future, there will be requirement of optimised the high performance message handling component within the messaging network which is able to handle the connectivity between millions of devices and applications communicating with each other.

DISCUSSION

The use of information technology (IT) is considered a prerequisite for the effective control of today's complex supply chains. The exponential growth Information Technology in supply chain networks has significantly

changed the paper based communication to e-communication, which is a serious threat of cyber crime (e-risk) by unauthorized or illegal access by means of physical or / and virtual intrusion to a computer or computer system or computer network. Criminals may commit illegal access of confidential data, theft of data, manipulation in data, and denial of access of system of supply chain networks. They may also perform the fraudulent activities by help of IT in Supply chain networks and it can be curbed through help of IT. The application of data integrity verification, cryptography, intrusion detection and risk mitigation, authentication and authorization, auto-analysis of legitimate usage patterns and computer forensics are useful to reduce the e-risks in SCM. Barcodes are both cost effective and time saver which eliminate the human error, reduce the paper works to improve the customer service, the usage of this limited to supply chain partners. Improved data integrity allows decisions to be made with real time, accurate data, improving product and category management decisions. Bar code technology facilitates the use of automated replenishment or vendor managed inventory so the right product is always at the right store at the right time. Recently, organizations, from both government and corporate sectors had mandate to implement radio frequency identification (RFID) technology for their suppliers. The global standard for RFID such as the Electronic Product Code (EPC) and offer insight into the coexistence of barcodes and RFID increased their importance to curb the e-risks.Asymmetic cryptography with secure bit length still requires significantly larger chips in RFID than symmetric cryptography. The major risks to EDI messages are loss of integrity (that is, alteration, modification, or destruction), loss of confidentiality (that is, copied, seen, or heard by unauthorized persons) and non availability (that is, not accessible when needed). The claims made by ERP software vendors that their software solutions are complete and designed to be industry specific. In practice, these packages do not support many business processes and frequent up gradation required. Consequently, many organizations are forced to leave some processes un-automated and a few legacy systems in place. The organizations are worried that the implemented package will work in the future or not. However, ERP as SAP implemented integration of different business modules with business data ware and intelligences. Its new tool SAP HANA is very useful to stop fraudulent activities in even ultra-high-volume environments.The internet not only provides communication in virtual environment, but also enables the opportunity of online business with mutual benefits of customer and suppliers of supply chain networks globally. The online supply chain management creates the e-risks as hacking, spreading or dissemination of malicious software (Malware), theft of internet hours / identity theft, cyber squatting (an act of obtaining fraudulent registration with an intent to sell the domain name to the lawful owner of the name at a premium), Privacy violation, cyber terror, etc. Microsoft Excel has many powerful features and by using this for Supply Chain Management can easily detect and prevent fraudulent activity with some limitation of excel sheet that it can process only one million rows or records of data. Implementation of IT in SCM as discussed in the study appears to have modest role in decision making as well as reducing e-risks by supply chain management. The evolution of high performance and cloud computing systems have started appearing in the domain of SCM and helping to provide transparency and visibility in supply chains. This upcoming technology is predicted to revolutionary changes in field of performance and e-risks prevention of SCM. Similarly next generation Internet connects heterogeneous computing devices to create network traffic that is generated by automated objects from public sectors to day to day life of people rather than human intervention. The IT systems with service oriented architecture and web service standards, expected to come in future, may facilitate better supply chain management.

Conclusion

This paper discusses the role of IT as an enabler in Supply Chain Management with vast benefits to organisations with a comprehensive IT implementation as well as curbing e-risks. Technology is always a double-edged sword. Society that is dependent more and more on technology, cyber crimes are bound to increase because bytes are replacing bullets in the crime world. There will always be new and unexpected challenges to stay ahead of cyber criminals and cyber terrorists but we can win only through partnership and collaboration of both individuals and government. Cyber crime in India has gone by 60% in 2012 compared to 2011. History is the witness that no legislation and technology has succeeded in totally eliminating crime. Securing physical and virtual systems which is sabotage on computer systems and their access to information and databases by cyber criminal has always been one of the critical risks for the supply chain management. Criminal may involve deliberated deceit or misrepresentation of facts or significant information to obtain illegal gain from Supply Chain Networks. Information Technology be used as tool against bid rigging, phantom bids, nepotism, substitution, false count, counterfeiting, creating fictitious accounting entities e.g., ghost employee, fake vendor, fake customer or vendor payments, falsified hours etc. The alignments of IT technology in SCM, viz. implementation of Electronic Record Management (Bar Code, RFID,EDI), ERP system (SAP, Oracle, People Soft), Microsoft package, Data Ware House, software agents, decision support systems, web services, e-commerce, electronic

supply chains, etc will overcome the e-risks and increase the performance. To curb the e-risks in India, in July, 2013 Indian government releases the National Cyber Security Policy.

Conflict of Interests

The authors have not declared any conflict of interests.

REFERENCES

Attaran M (2007). 'RFID: An Enabler of Supply Chain Operations', Supply Chain Manag. 12(4): 249- 257.

Boone T, Ganeshan R (2007) 'The frontiers of e Business technology and supply chains', J. Oper. Manage. 25 (6): 1195-1198.

Bose I, Mahapatra RK (2001) 'Business data mining — a machine learning perspective', Inform. Manage. 39(3): 211–225.

Boyle RD (2004). 'Achieving your Supply Chain Goals: Conquering the 'First Mile' Hurdle of Data Capture'APICS-The Performance Advantage, July/August, Vol. 14, No.7.

Calia E (2010). 'The Internet of Things & Identity in the Future Internet', Istituto Superiore Mario Boella: Torino Italy.

Cerullo MJ, Cerullo V (1999). 'Using neural networks to predict financial reporting fraud, Computer Fraud & Security May/June 14–17.

Chandan AC, Shilpa SK (2009). 'RFID Adoption by Indian Retailers: An Exploratory Study', IUP J. Supply Chain Manage. 6(1): 66-77.

China', Int. J. Manage. 25(2):322–335.

Chou DC, Tan X, Yen DC (2004). 'Web technology and supply chain management', Inf. Manage Comp. Soc.12(4): pp.338–349.

Christopher M, Peck H (2007). 'Building the Resilient Supply Chain', http://www.martinchristopher.info/downloads/building%20the%20resilient%20supply%20chain.pdf (Accessed on 10.09.2014)

Coronado AE, Andrew CL, Zenon M, Dennis FK (2004). 'Automotive supply chain models and technologies: A review of some latest developments', www.emeraldinsight.com/1741-0398.htm (Accessed on 10.09.2014)

D'Avanzo R, Starr E, Von Lewinski H (2004). 'Supply chain and the bottom line: a critical link', Outlook: Accenture, 1: 39-45.

Davenport TH, Brooks FD (2004). 'Enterprise systems and the supply chain', J. Enterp. Inf. Manage. 17(1): 8–19.

Dowling C, Leech S (2007). 'Audit support systems and decision aids: Current practice and opportunities for future research', Int. J. Account. Inf. Syst. 8(2): 92-116.

Fosso WS (2012) 'Achieving Supply Chain Integration using RFID Technology: the Case of Emerging Intelligent B-to-B e-Commerce Processes in a Living Laboratory', Bus. Process Manage. J. 18(1):58-81.

Fosso WS, Lefebvre LA, Bendavid Y Lefebvre E (2008). 'Exploring the impact of RFID technology and the EPC network on mobile B2B eCommerce: A case study in the retail industry', Int. J. Prod. Econ. 112(2): 614-629.

Gao X, Wang H, Shen J, Huang J, Song B (2004). "An Approach to Security and Privacy of RFID System FOR Supply Chain," Proceedings of the IEEE International Conference on E-Commerce Technology for Dynamic E-Business (CEC-East'04), pp. 164-168.

Garcia-Dastugue SJ, Lambert D (2007). 'Inter organizational time-based postponement in the supply chain', J. Bus. Logistics, 28(1): 57–81

Gilaninia SHS, Danesh, SY, Amiri M, Mousavian SJ (2011). 'Effective Factors on Adoption of E-Commerce in SME Cooperative', Interdisciplinary J. Contemp. Res. Bus. 3(6): 13-21.

Gould LS (2000). 'What you need to know about RFID', Automotive Manufacturing & Production, 112(2): 46-49.

Hillman M, Keltz H (2007) 'Managing Risk in the Supply Chain – A Quantitative Study', http://www.amrresearch.com/Content/View.aspx?pmillid=19994 (Accessed on 10.09.2014)

Janvrin D, Bierstaker J, Love DJ (2008). 'An Examination of Audit Information Technology Use and Perceived Importance', Account. Horizons, 22(1): 1-21.

Jedermann R, Ruiz-Garcia L, Lang W (2009) 'Spatial temperature profiling by semi-passive RFID loggers for perishable food transportation', Comput. Electron. Agr. 65: 145–154.

Kirkos E, Spathis C, Manolopoulos Y (2007). 'Data mining techniques for the detection of fraudulent financial statement', Expert Syst. Appl. 32(2): 995–1003.

KPMG. International (2006). 'Developing a strategy for prevention, detection and response', Fraud Risk Management.

Kull TJ, Bojer K, Calantone R (2007). 'Last-Mile supply chain efficiency: an analysis of learning curves in online ordering', Int. J. Oper. Prod. Manage. 27(4): 409–434.

Laudon KC, Laudon JP (2000). Management Information Systems: Organization and Technology in the Networked Enterprises. 6th Edn., Prentice-Hall Inc., USA.

Lee HL, Padmanabhan P, Whang S (1997). 'Information Distortion in a Supply Chain: The Bullwhip Effect', Manage. Sci. 43: 546-558.

Little AG, Best PJ (2003). 'A framework for separation of duties in an SAP R/3 environment', Managerial Auditing J. 18(5): 419–430.

Mabert VM, Soni A, Venkataramanan MA (2001). 'Enterprise resource planning: Common myths versus evolving Reality', Bus. Horizons, 44(3): 69–76.

Mahamani A, Rao KP (2010). 'Development of a spreadsheet bases vendor managed inventory model for the single echelon supply chain: A case study', Serbian J. Manage. 5(2):199–211.

Mahinderjit-Singh M, Li X (2009). 'Trust Framework for RFID Tracking in Supply Chain Management', Proc of The 3rd International Workshop on RFID Technology – Concepts, Applications, Challenges (IWRT 2009), Milan, Italy, pp 17-26, 6-7 May.

Mahinderjit-Singh M, Li X (2010). 'Trust in RFID-Enabled Supply-Chain', Management', Int. J. Security Networks, 5(2/3): 96-105.

Moon YB (2007). 'Enterprise resource planning (ERP): A review of the literature', Int. J. Manage. Enterprise Dev. 4(3): 235-263.

Nair PR (2012). 'RFID for Supply Chain Management', CSI Communications, November. 36(8):14-18

Nair PR (2013). 'E-Supply Chain Management using Software Agents', CSI Communications, July 2013, 37(4): 13-16.

Ngai EWT, Gunasekaran A (2004). 'Information systems in supply chain integration and management', Eur. J. Oper. Res. 159(2): 269-295.

Owusu-Ansah S, Moyes GD, Oyelere PB, Hay P (2002). 'An empirical analysis of the likelihood of detecting fraud in New Zealand', Manage. Auditing J. 17(4): 192–204.

Panik M (2009). 'Regression Modeling Methods, Theory, and Computation with SAS', CRC Press.

Patel RB, Garg K (2004). 'Distributed Banking with Mobile Agents: An Approach for E-Commerce', WSEAS TRANSACTIONS ON COMPUTERS 3(1): 98-102.

Phua C, Lee V, Smith K, Gayler R (2005). 'A comprehensive survey of data mining-based fraud detection research', Artif. Intell. Rev. pp. 1–14.

Picco GP (2001) 'Mobile Agents: An Introduction', Microprocessors and Microsystems, 25(2): 65-74.

Prasad Ch.VVSNV, Govindan K, Kulkarni DM (2010). 'Role of IT in SCM environment', Int. J. Bus. Perfor. Supply Chain Modelling, 2(1): 81-94(14).

Ramya SG (2013) 'Role of Software Agents in E-Commerce', Int. J. Comp. Eng. Res. 3(3): 246-251.

Ronchi S, Brun A, Golini R, Fan X (2010). 'What is the value of an IT e-procurement system? J. Purchasing Supply Manage. 16(2): 131-140.

Sabbaghi A, Vaidyanathan G (2008) 'Effectiveness and Efficiency of RFID technology in Supply Chain Management: Strategic values and Challenges', J. Theor. Appl. Elect. Com. Res. ISSN 0718–1876 Electronic Version, 3(2): 71-81.

Sanchez A, Perez M (2003). 'The use of EDI for interorganisational co-operation and co-ordination in the supply chain', Integrated Manufacturing Systems, Vol. 14, No. 8, pp.642–651.

Sanders NR, Premus R (2002). 'IT applications in supply chain organizations: A link between competitive priorities and organizational benefits', J. Bus. Logistics, 23(1): 65–83.

SAP (2007), 'ABAP AS Authorization Concept-SAP NetWeaver', SAP

AG.
Sarac A, Absi N, Dauzère-Pérès S (2010), 'A literature review on the impact of RFID technologies on supply chain management', Int. J. Prod. Econ. 128(1): 77-95.
Silver EA, Pyke DF, Peterson R (1998). 'Inventory Management and Production Planning and Scheduling', third edition, John Wiley and Sons, New York
Simchi-Levi D, Kaminsky P, Simchi-Levi E (2003).' Designing and managing the supply chain. Concepts, strategies, and case studies' second edition, Boston.
Spathis C, Doumpos M, Zopounidis C (2002) 'Detecting falsified financial statements: a comparative study using multicriteria analysis and multivariate statistical techniques', Eur. Account.Rev.11(3): 509–535.
Srivastava, B (2004), 'Radio Frequency ID technology: the next revolution in SCM', Bus. Horizons, 47(6): 60-68.
Stroeken JHM (2000). 'Information technology, innovation and supply chain structure', Int J. Technol. Manage. 26(3): 7-13.
Talluri S., (2000). A benchmarking Method for Business-Process Reengineering and Improvement, Int. J. Flex. Manuf. Sys. 12(4): 291-304.
Turban E, Aronson JE, Liang TP, Sharda R (2007). 'Decision Support and Business Intelligence Systems', Eighth edition, Pearson Education.
Van Donk D, Van der Vaart T, Gimenez C (2008). 'Business Conditions, Integration and Performance in Supply Chains', 14th International Annual Euroma Conference, Supply Chain Management
Varma TN, Khan DA (2012). 'Fraud Detection in Supply Chain using Benford Distribution', Int. J. Res. Manage. 5(2): 90-96.
Varma TN, Khan DA (2014). 'MS excel functions as supply chain fraud detector', Afr. J. Bus. Manage. 8(24): 1109-1117.
Viaene S, Derrig RA, Dedene G (2004) 'A case study of applying boosting naive Bayes to claim fraud diagnosis', IEEE Transactions on Knowledge and Data Engineering, 16(5): 612–620.
Watson RT, Akelsen S, Pitt LF (1998). 'Building mountains in that flat landscape of the World Wide Web. California Manage. Rev. pp. 36–56
Wyld D (2006). 'RFID 101: The next big thing in management', Manage. Res. News, 29(4): 154-173.
Yuan J, Yuan C, Deng X, Yuan C (2008). 'The effects of manager compensation and market competition on financial fraud in public companies: an empirical study in China, Int. J. Manage. 25(2): 322–335.

Appendix I

Some terms related to cyber crime (e-risks)

Illegal Access (Hacking, Cracking)

Hacking means unauthorized or illegal access by means of physical or / and virtual intrusion to a computer or computer system.

Illegal data acquisition (Data Theft or Alteration)

If any person without permission of the owner or any other person, who is in charge of a Computer, its system or network - downloads, copies or extracts any data, computer data base or information from such computer, its system or network including information or data held or stored in any removable storage medium, then it is data theft.

Salami Attack

These attacks are used for the commission of financial crimes. The key here is to make the alternation so insignificant that in a single case it would go completely unnoticed. E.g. The Ziegler case wherein a logic bomb was introduced in the bank's system, which deducted 10 cents from every account and deposited it in a particular account.

Spreading or dissemination of malicious software (Malware)

The virus/malicious software means any computer instruction, information, data or program that destroys damages, degrades or adversely affects the performance of computer resource or attaches itself to other computer resources.

Data Diddling

Data diddling is the performing unauthorized modifications to data prior or during input into a computer or computer system. In data entry, a virus that changes data, the programmer of the database or application, exchanging valid disks and tapes with modified replacements.

Denial of Service Attack

The Internet Security Glossary (Shirley, 2000) defines Denial of Service (commonly named DOS attack) as "The prevention of authorised access to a system resource or the delaying of system operations and functions."

E-Mail Bombing

An e-mail bomb is a form of net abuse consisting of sending huge volumes of e-mail to an address in an attempt to overflow the mailbox or overwhelm the server where the email address is hosted in a denial-of-service attack. Mass mailing consists of sending numerous duplicate mails to the same email address.

Theft of Internet Hours / Identity Theft

The idea behind this is to prevent theft, misappropriation, fraud or forgery of access code/ user id / password etc; by the person to the account of another person by tempering with or manipulating any computer, computer system or network.

Cyber squatting

Cyber squatting refers “an act of obtaining fraudulent registration with an intent to sell the domain name to the lawful owner of the name at a premium”.

Sending offensive message

The offensive messages may be sent in the form of text viz. e-mail, SMS, blog, vblog, tweet; image, sound or voice through communication service, etc. Any information that is grossly offensive or has menacing character (obscenity in electronic form, morphing, defamation, text bullying, stalking , etc.) or any information which is false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will. It may be any electronic mail for the purpose of causing annoyance or inconvenience or to deceive addressee or recipient about the origin ie; spamming, unsolicited email/ telephone call, etc.

Cyber Stalking

Cyber Stalking can be defined as the repeated acts of harassment or threatening behavior of the cyber criminal towards the victim by using internet services. Stalking in general terms can be referred to as the repeated acts of harassment targeting the victim such as following the victim, making harassing phone calls, killing the victims pet, vandalizing victims property, leaving written messages or objects.

Spam

Spam is described as the emission of unsolicited bulk messages. Offenders send out millions of e-mails to users, often containing advertisements for products and services, but frequently also malicious software.

Vishing

Vishing is the practice of using social engineering over the system, most often using features facilitated by Voice over IP (VoIP), to gain access to private personal and financial information from the public for the purpose of financial reward. The term is a combination of “voice” and phishing.

Stolen Computer Resource or Communication

It is a theft with dishonestly receiving and retaining any stolen computer resource for wrong full gain.

Mail Spoofing or forgery

Email spoofing is a technique in which the sender address and other parts of the email header are altered to appear as though the email originated from a source other than its actual source.

Privacy violation

It is an offence, whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person. Nature of offence may include installation of spy cam/ hidden camera/ communication device inside private area or hotel rooms etc.

Cyber Terrorism

Cyber terror is a threat against the unity, integrity or sovereignty of any nation or to strike terror in people.