Computer and Information Science; Vol. 6, No. 3; 2013
ISSN 1913-8989 E-ISSN 1913-8997
Published by Canadian Center of Science and Education

Security of E-Procurement Transactions in Supply Chain Reengineering

Juliette Stephens[1] & Raul Valverde[2]

[1] School of Information Technology, University of Liverpool, Liverpool, UK

[2] John Molson School of Business, Concordia University, Montreal, Canada

Correspondence: Raul Valverde, John Molson School of Business, Concordia University, Montreal, QC., H3G 1M8, Canada. Tel: 44-514-848-2424 ext.2968. E-mail: rvalverde@jmsb.concordia.ca

Received: December 14, 2012 Accepted: April 15, 2013 Online Published: May 6, 2013

doi:10.5539/cis.v6n3p1 URL: http://dx.doi.org/10.5539/cis.v6n3p1

Abstract

With the rapid rise of Business to Business (B2B) transactions over the internet and the increasing use of e-procurement solutions by large organizations for purchasing, there is a need to reengineer current legacy supply chain management systems in order to integrate them with modern e-procurement systems. Although there is a great deal of research in the area of integration with e-procurement systems, there is little attention for security aspect of this integration that responds to the need for accurate and secure information exchange has become essential to doing business. Security is a consistent and growing problem for e-commerce and procurement solutions. As the number and frequency of security violations continues to rise, there is a corresponding dependence on information technology to drive business value, which in turn increases the importance and criticality of transaction data. The result is an increasing demand for secure e-procurement transactions to ensure the confidentiality, integrity and availability of data. Secure transactions are essential if organizations are to fully realize the benefits of e-procurement which include increased productivity, lower purchasing pricing, streamlined processes, reduced order fulfillment time and greater budgetary control; all of which can contribute to increasing an organization's competitive advantage. This research is a case study which evaluates the security of transactions for the integration of an e-procurement solution in a large organization. It addresses both business and technological issues by examining the current threat model, security policies, system architecture, and security controls that have been implemented to ensure data integrity and confidentiality. Finally, a new model will be proposed for reengineering projects that require the integration of e-procurement systems which includes recommendations for improvements that will be benchmarked against common security designed principles.

Keywords: legacy systems, e-procurement, reengineering, security and supply chain management systems

1. Introduction

E-Procurement, the electronic support of the professional buying process, which addresses the relationship of a business to its suppliers, is on the rise (Tanner et al., 2008). Broadly defined, e-procurement includes a company's requisitioning, purchasing, transportation, warehousing and in-bound receiving process. E-Procurement solutions often allow buyers or employees to order goods directly from the personal computers through the web in real time.

E-Procurement is on the rise and it is said to be one of the most efficient ways to conduct business. This evidenced by studies showing that organizations are spending as much as 50 to 60% of total revenue on e-procurement activities e-Procurement is generating great excitement because of its potential to reduce procurement costs and improve strategic sourcing (Subramaniam & Shaw, 2002).

However, with increasing use of reengineering projects including third party e-procurement solutions, concerns over the security and confidentiality of data exchanged in electronic environments has become a prominent issue (Angeles & Nath, 2007). As competition on the internet grows, companies seek to obtain as much information as possible from competitors (i.e. knowledge about competitors, prices, products, customers) by using various methods that threaten data security and help them gain an unfair advantage. Mohammadi et al. (2012) conducted a study that revealed that the improvement in supply chain capabilities through IT allows the firm to learn and

respond to market changes better and quicker than competitors. Therefore, concerns over the security of transaction data need to be addressed in order to allow organizations to continue to improve performance and maintain competitive advantage.

The research on this article evaluates the security of a third party e-procurement in a supply chain reengineering project for a large organizations, it proposes a new security model based on gaps identified in the current security practices and procedures.

2. Foundations

2.1 E-Procurement

E-Procurement is the electronic acquisition of goods and services for an organisation (Angeles, 2007). E-Procurement plays a central function in B2B e-commerce and can help an organisation achieve enormous cost saving and productivity improvements (Neef, 2001).

There are several varieties of E-Procurement systems:

- Buy-side procurement systems involve buyers who implement their own private exchanges, extranets, or networks in cooperation with selected technology partners.
- Supplier-side e-procurement systems are usually put up and managed by manufacturers with a major market presence i.e. Grainger.com. The benefits to buyers include easy access, content provided by multiple suppliers, free registration and site security usually guaranteed by the host supplier.
- Electronic marketplaces sponsored by neutral third parties. This involves an e-procurement environment where buyers are matched with sellers. The hosting party usually compiles product information from many supplier catalogs and makes it available to buyers in one venue. Buyers can easily compare product prices and other important attributes across a number of competing suppliers (Angeles, 2007).

There are two types of procurement activities: direct and indirect procurement.

- Direct procurement occurs which encompasses all items that make up the finished product such as raw materials, components and parts.
- Indirect procurement concerns all items and services that are not directly part of the finished product but support internal business activities, such as computers, office equipment, operating supplies, and office supplies. Procurement is often performed by non purchasing experts like a central purchasing unit or general members of staff and often includes items ranging from ‘simple’ office products to parts for maintenance, repair and operations (MRO) such as lubrication or spare parts to complex construction related items and various services. Purchases often occur on an infrequent basis and demand can be difficult to predict (Gebauer et al., 2003).

Organisations can either buy expensive e-procurement software packages which can be hosted and managed in house or rent e-procurement services from an Application Service Provider (ASP), thus saving costs and receiving high quality services (Klueber, 2002).

The security and privacy of procurement transactions is a major concern for most organizations especially where payment details and other pieces of sensitive information are sent over the internet. As a result, organizations have introducing a variety of security measures to ensure that confidentiality, integrity and availability of their data.

Computer Crime and Intellectual Property Section (CCIPS) at the US Department of Justice set a definition for the above terms and as defined by (Kouns & Minoli, 2011) as:

Confidentiality: A breach of confidentiality occurs when a person knowingly accesses a computer without authorization or exceeding authorized access;

Integrity: A breach of integrity occurs when a system or data has been accidentally or maliciously modified, altered, or destroyed without authorization;

Availability: A breach of availability occurs when an authorized user is prevented from timely, reliable access to data or a system;

Tai’s (2011) study revealed that internet based procurement systems enabled firms to improve their intra- and inter-organizational process integration capabilities which, in turn, yield sustained gains in organizational performance.

The following factors that create value have been identified as drivers for e-procurement (Tai, 2011):

(1) Reduced Transaction Costs: a reduction in some of the common issues including supplier over charge, poor invoice checks / matching, incompatible processes result in lower transaction costs.

(2) Higher Process Quality: the quality of a procurement process is a measure of how well a system meets the requirement needs of the organisation. A decrease in processing errors and a reduction in duplicate entry and non-value add activities due to streamlined process will result will result in better quality data and greater user satisfaction.

(3) Increased System Responsiveness: system responsiveness is the ability of an e-procurement system to respond to the needs of the user and the enterprise. It affects the time taken to get users what they need and ability to locate alternative sources if necessary. A reduction in the time taken and the number of people involved in the e-procurement process is a considerable driver for change.

(4) Increased Control: increased monitoring and control as a result of a centralized system and a consolidated supplier base consisting of a list of approved suppliers facilitates the negotiation of better prices. Further, the risk of non compliance is reduced by implementing strong financial authorities and controls and providing consistent and improved data for reporting (Subramaniam & Shaw, 2002).

The factors discussed above rely on secure transactions to ensure the confidentiality, integrity and availability of transaction data.

2.2 Information Security, Security Threats, Security Standards and Security Risks

Information Security is concerned with protecting the confidentiality, integrity, and availability of information and information systems (CIECA, 2010).

Information security protects information from a wide range of threats in order to ensure business continuity, minimize business damage and maximize return on investments and business opportunities. It is achieved by implementing a suitable set of controls, which could be policies, practices, procedures, organizational structures and software functions. These controls need to be established to ensure that the specific security objectives of the organization are met.

Security threats are things that can go wrong or attack a system i.e. fraud, fire, malicious code etc. Vulnerabilities make systems more prone to attack by a threat by increasing the probability, impact and success of an attack (The Security Risk Analysis Directory, 2005).

Web based applications are highly vulnerable to attacks and provide an entry points through which account details, social security numbers and other sensitive data can be accessed and stolen. This vulnerability is present because current security solutions–including network firewalls, intrusion detection systems, encryption, and manual measures such as aggressive quality assurance and audit procedures–are incapable of preventing attacks at the application layer and many times incapable also of stopping them at the operating system layer as well (Stankard & Gehling, 2005).

Security Standards are guidelines that help an organisation to initiate, implement, maintain and manage information and inherent vulnerability to information security issues.

ISO17799 is a code of practice for information security management. It addresses security in the widest sense, providing best practice, guidelines and general principle for implementing, maintaining and managing information security in any organisation, and producing and using information in any form. It recognizes that the level of security that can be achieved purely through technical means is limited and the required level of security should always be driven by appropriate management controls and procedures.

ISO/IEC 17799:2005 identifies the controls that form the starting point for information security. It covers the critical success factors, the organization of information security, asset management, human resources, physical and environmental security, communications and operations management, information systems acquisition, development and maintenance, incident management, business continuity management and compliance (ISO, 2006a). BS ISO/ IEC 17799 has been written to harmonize with other management system standards to assist in the integration and operation of an organization's management system.

Some of the principles for business to businesses interfaces are as follows:

- All interfaces should have some form of authentication, preferably strong authentication. Authentication is a basic element of securing any system.
- Internet and industry standards should be used whenever possible for networks, protocols, and algorithms, technologies, and data formats.

- Confidentiality and Integrity of data should be preserved at all times. Confidentiality and integrity should be protected both in transit, and while stored.
- Each transaction should have an audit trail. Each organization should keep audit trails for security related events to track the Who, What, When of each transaction (CIECA, 2010).

Risk is the likelihood of a threat agent taking advantage of vulnerability and the corresponding business impact. (Harris 2008). A security risk is the loss potential to an organisation's asset that will likely occur if a threat is able to exploit a vulnerability (Landoll, 2006). Security Risk management is the process of understanding, mitigating and controlling risk through risk assessment, risk mitigation and operational security and testing (Landoll, 2006).

It is not possible to provide total security against every single risk, but it is possible to provide effective security against most risks (Calder & Watkins, 2008). Security Risk Assessment can be defined as an objective analysis of the effectiveness of the current security controls that protect an organizations assets and a determination of the probability of losses to those assets (Landoll, 2006).

Security risk assessment is a process that focuses on:

- Prevention - stop security events before they occur.
- Detection - quickly and efficiently detect security violations.
- Response - quickly respond to any detected security violations.
- Improve- use the lessons learned to improve all of the steps in the process.

Security risk assessment provides a review of not just the current implementation of an application's protection strategy but provides an opportunity to measure the effectiveness of current threats in what is essentially a constantly changing environment (CIECA, 2010).

The evaluation of current security practices and controls are keys aspects of the risk assessment process. Security risk assessment can provide a measure of the effectiveness of current security practices and information necessary to adjust to the ever changing threat environment (Landoll, 2006).

While applying security improvements lowers the risk of security threats, over time these improvements become less effective due to the changing threats and environment over time. Therefore, periodic security risk assessment should be carried out to ensure that security practices don't become stagnant while threats, attacker skills, and indeed business mission changes (Landoll, 2006).

3. Research Methods

The case study used for this research was selected from a project for multinational company, one of the world's largest energy companies, providing its customers with fuel for transportation, energy for heat and light, retail services and petrochemicals products for everyday items.

The research methodology used in this study is based on OCTAVE-S, a variation of the OCTAVE approach developed to meet the needs of small less hierarchical organizations with limited means and unique constraints typically found in smaller organizations. OCTAVE-S emphasizes operation risk and security practices (Alberts et al., 2008). It is typically composed of a team of 3–5 people who have a broad insight into the organizational business and security processes and includes a limited exploration of the computer infrastructure during Phase 2 - Infrastructure Vulnerability and Identification.

OCTAVE-S is a self-directed information security risk evaluation. It involves the examination of security risks to an organization's critical assets in relation to its business objectives, ultimately yielding an organization-wide protection strategy and asset-based risk mitigation plans. While the case study used for the research is not a small organization–it currently has over 96,000 employees, a variation of the OCTAVE-S method has been chosen for this study for the following reasons because the e-Procurement solution is outsourced to a third party resulting in limited availability of computer infrastructure information.

The main phases of OCTAVE-S are as follows:

Phase 1 – Build an Asset Based Threat Profile: this is the evaluation of organizational aspects. The focus of this study is an e-procurement system within the case study selected.

Phase 2 – Identify Infrastructure Vulnerabilities: this involves a high level review of the organizations computer infrastructure – focusing on the extent to which security is considered by the maintainers of the system. This involves analyzing access to asset and examining technologically related processes.

Phase 3 – Develop Security Strategy and Plans: identify risks to the organization and decide what to do i.e. make a recommendation for a plan of action (Alberts et al., 2008).

Data for this research study was gathered using semi-structured interviews and a user survey in a two stage approach. The first stage involved initial interviews with staff in different parts of the organization i.e. Digital Security services, e-procurement helpdesk, project managers. Feedback from here resulted in questions being refined for subsequent interviews to capture all relevant information.

The second stage involved the use of survey questions sent to key e-procurement system users to gain an understanding about user perceptions of the importance of security for e-procurement transactions. The findings, which were drawn from very rich data, were constantly reflected back to the theory to test their validity.

Reliability was achieved by using the same interview format which involved a set of main questions for all employees with additional questions based on employee role. Data was also collected from historical technical documents and presentations as well as the company's intranet. Interviewees were sent an introductory email message and a series of standard main questions. This was followed up at the interview by further probing or secondary questions that are associated with each primary question based on area of expertise for the e-procurement solution.

Primary questions were asked first and the interviewee will be given sufficient time to respond before the next probing question. A tape recorder and hand written notes (for teleconferences and some face to face interviews) will be used to capture all the information discussed in the meeting.

Semi Structure interviews, Templates and a Survey Questionnaire were used to evaluate the security of e-procurement transactions. Semi structured interviews were carried out with open ended investigative questions using what, why, when, how, where, who. These were designed to gain a broad understanding of the e-procurement solution, security practices and policies, threats, requirements and control measures from the users' perspective. This highly adaptable semi-structured format allowed issues to be followed up, clarified and developed during the discussion. Templates from the OCTAVE-S process to determine both the risk and threat profile for the e-procurement solution.

Interviews were carried out with 6 key security and e-procurement staff who make up the project team as specified in the OCTAVE-S guidelines and consisted of by face to face and telephone interviews. The interviews were analyzed using content analysis, creating categories to classify the meanings expressed in the data.

A survey document was designed to understand and evaluate user perceptions of security issues during their day to day purchasing activities. It included various questions ranging from authentication and password management to security awareness & training. It was sent out to a small sample of Ketera staff (15 staff members) obtained from e-procurement Administrator.

The online Survey Questionnaires were sent selected sample with a covering letter stating its purpose. Participants were not specifically told the survey was about the security of e-procurement transactions (although it did contain security questions) to ensure that participants would not be influenced in this direction in their choice of responses. The sample was given 2 weeks to respond and a follow up email was sent after an initial slow response rate.

A set of pilot questions for both the interview and survey where textual data (notes, interview transcripts, responses to free form questions) was explored using content analysis to generate categories and explanations. The questions for both interview and survey were designed and pilot tested to cover the following areas:

1) General background information about e-Procurement system that will be integrated – the process, how it works etc
2) Security Practices – these include security policies and controls: Security Management, Security Policies and Regulations, Security Architecture and Design, Security Awareness and Training, Collaborative Security Management (see outsourcing policy); Monitoring and Auditing Physical Security, Authentication and Authorization, Encryption and Password Management.

The sample chosen for this research is theoretical sample, a non-random sample consisting of employees who work most closely with the system (Walliman, 2004) and have the knowledge and ability to provide information on the process and security consideration transaction data. These employees located primarily in the US and the UK and all use or work with Ketera network systems for indirect procurement. Ketera is a company that provides network services for procurement systems including e-procurement systems.

The different system roles played by users (manager, solutions architect, digital security solutions team etc.)

helped to define the security considerations and concerns for indirect procurement in the company used for this case study, particularly in IT&S (Information Technology Services).

The sample size was kept small in line with the OCTAVE-S method which recommends of team of 3–5 members. Similarly for the survey, the idea was to send out survey to a small number of people most closely associated with the system and who are most likely and motivated to respond.

The interviewees were represented at different levels of the organization from junior employees to senior management. The interview questionnaire, composed mostly of open questions with several sub-questions for clarification, was designed to take approximately 1 hour.

3.1 Case Study

The organisation's e-procurement model is a multi-supplier online catalog service. It has been specifically designed to enable end users to order supplies directly from a multi-vendor catalogue and, thus, supports self-service. Compliance with corporate purchasing rules is ensured as only approved suppliers who meet the quality and cost standard have their catalogues available online. Further, there is no Integration with any internal backend systems.

While purchasing operations are performed by end users, central purchasing is usually responsible for setting up and maintaining the systems, reviewing all approved purchase orders, for incorporating suppliers into the network, and for negotiating blanket order agreements and long-term contracts (Gebauer & Sergev, 2003).

The goal of the company is to reengineer its current system in order to incorporate SAP's Supplier Relationship Management (SRM) application that provides strategic value through sustainable cost savings, contract compliance and quick time to value. The organisation's initial focus for procurement is direct procurement, however, as part of the reengineering process, an interim solution that is called iBuy is currently used for indirect spend because SAP SRM functionality does not cover all indirect service requirements at this point and the reengineering team is evaluating possible options that will incorporate this functionality in the near future but a decision was made of using iBuy while this is completed. Figure 1 reproduced below shows the iBuy Brand and Vision and 3 main products:

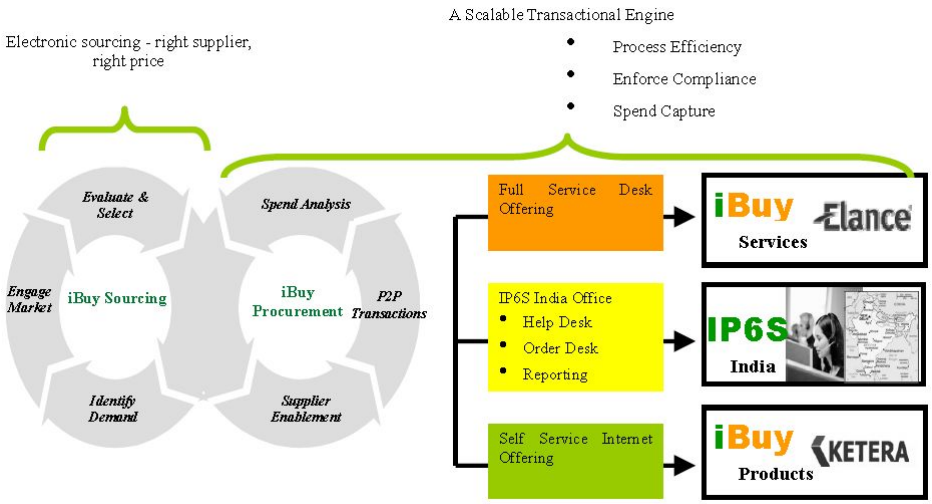


Figure 1. iBuy brand and vision

iBuy consists of 3 main procurement products: Elance, IP6S and Ketera. This research focuses on indirect procurement using Ketera – a self servicing internet offering developed by Ketera technologies. This includes the interfaces available to the organisation's users, limited information provided by the vendor and security policies, requirements and controls which relate to user access to the Ketera portal i.e. workstation security within the intranet.

Ketera, a Commercial of the Shelf (COTs) solution, is primary solution for indirect procurement for the system chosen for the study. Ketera is used mainly by head office staff in the US and UK and involves maintenance, repair and operating (MRO) purchases which include any materials or services not directly ascribed to primary production such as office supplies and other services. Under this model, users access Ketera over the intranet while Ketera provides all the storage, and network infrastructure needed to deliver the application, as well as the

staff to manage the entire platform.

The benefits of this outsourced e-procurement model as part of the reengineering project include a low capital outlay, application management and ongoing support (including upgrades), no IT staff maintenance burdens and a rapid ROI (Mulholland, 2012). Further, there is the convenience of scalable and demand driven usage which includes seamless, imperceptible upgrades and guaranteed service levels as agreed that is convenient in reengineering projects (Klueber, 2002).

Ketera incorporates an automated workflow process and the Delegation of Financial Authority (DoFA) model for the organization chosen for the study. The Delegation of Authority model describes who can approve requisition orders within the organization chosen for the study.

All purchase orders need to be approved by an authorized delegated authority with a budget approval limit. Different delegated authorities have different approval limits, and orders over the limit move up to the next approver in the DoFA chain i.e. all orders of $10,000 move up the DoFA chain. Once the goods have been delivered based on confirmation from the buyer, the supplier creates invoices in the system to match purchase order and delivered goods and invoices are sent to Accounts Payable. The system processes invoices to the value of $400,000 each night.

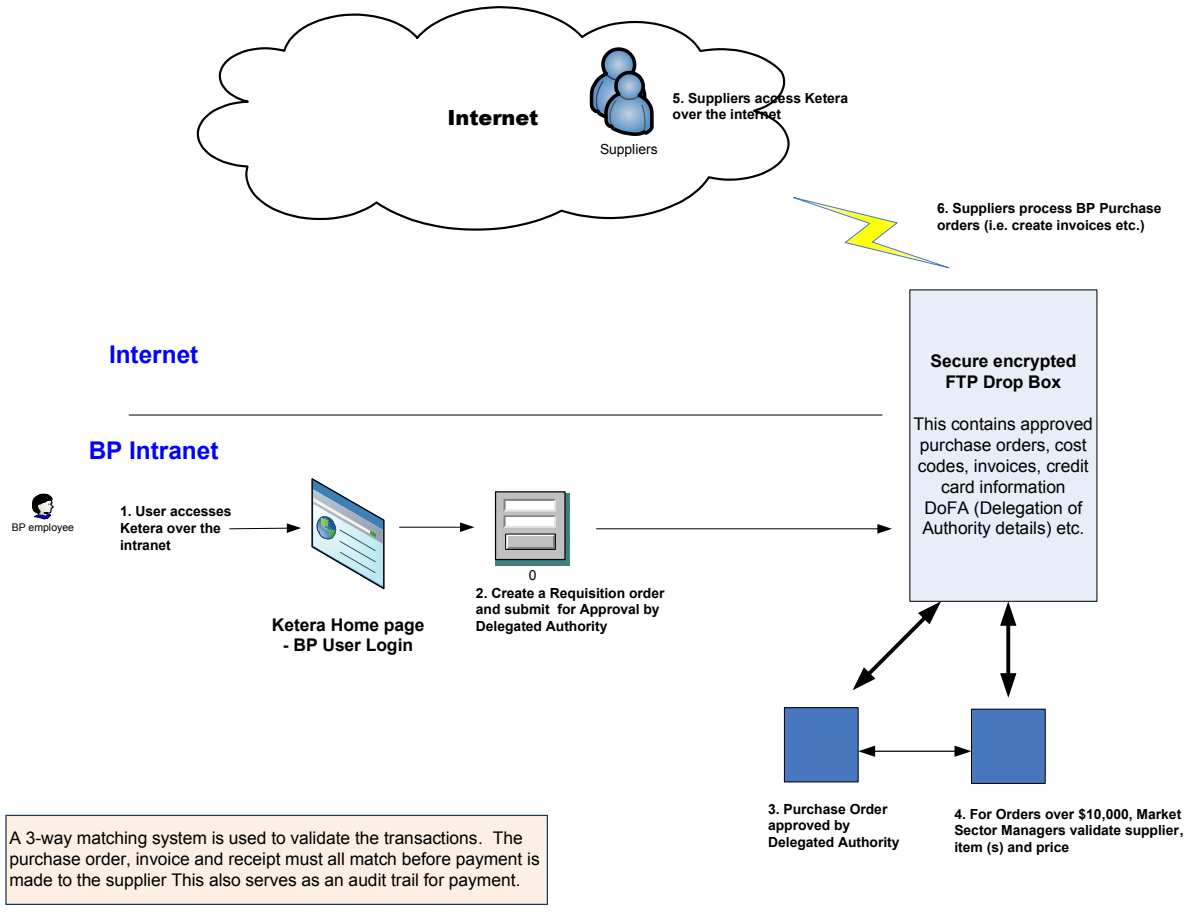


Figure 2. Ketera – High level business process model

Procurement employees access Ketera using their Windows NT network user names and password and when new users log on for the first time, they are asked to change their password. When a user creates a requisitions order, approvers received an email notification (sent to Microsoft Exchange Server email accounts) of requisition orders awaiting approval. Once the requisition has been approved, it is sent on to the procurement managers for validation and then on the suppliers as a completed purchase order for good.

Ketera e-Procurement has been designed and deployed to conform to n-tier architecture, with firewalls between each functional layer. It uses a shared database architecture and uses the same database to store data of different

corporate entities. Ketera contains data from the organisations's Global Address Book and up-to-date DoFA information obtained from the DoFA website. This information is sent overnight via a batch file to the secure FTP drop box. It also contains transaction data such as purchase orders, credit card information, supplier invoices. The Figure 2 shows the e-procurement process.

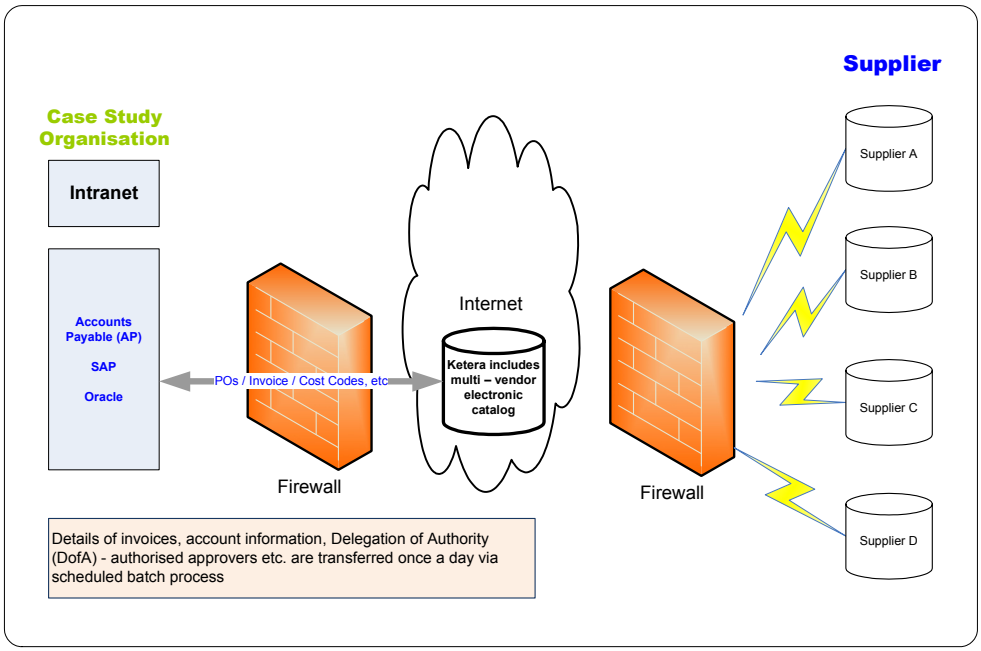


Figure 3. Ketera – Architecture

Figure 3 shows multiple suppliers accessing Ketera over the internet through a firewall to create invoices for goods ordered by employees. Procurement employees and other systems that transfer data via secure FTP must also go through a firewall that protects the system from unauthorized users.

There is no direct connection from the organizations' network to Ketera nor is there any integration with any case study's backend process.

4. Results

The analysis of the study was based on the 3 phases proposed by OCTAVE-S research methodology.

4.1 Phase 1- Build an Asset Based Threat Profiles

While the data in Ketera is confidential, it is not considered a critical application at a global level. The loss of service could have a medium to high impact at Business Unit level resulting in financial loss of $60 - $100 million. Further, this could result in non-achievement of performance expectation, embarrassment to the Group CEO, significant failure to improve in line with expectations. There would be no impact on the enterprise as it is an internet subscription service.

Classifying and describing the individuals involved in the production, maintenance and use of a web based e-procurement systems helps to identify typical attacks or security breaches. The following is a list of potential intruders who may attempt to attack the system:

- System vendor: who sell black-box components (e.g. an e-procurement vendors).
- System / Network Administrators who configure and run host machines in a corpo-rate environment; or who run the public network.
- Ketera support staff who provide application support.
- Users and suppliers who access the application over the intranet (Ambler, 2006).

A threat model becomes a plan for penetration tests which investigates threats by directly attacking the system in an informed or uninformed manner (Ambler, 2006). The threat model plays significant role in defining the security requirements and controls implemented to protect the integrity of information. User security awareness

can help to formulate a security model which supports the security policy and ensure the security of e-procurement transactions.

Identifying strategies to mitigate potential system threats helps to justify security features and practices implemented for a system to protect corporate assets.

Threats such as physical security of the application and natural disasters such as hurricane or other acts of God are not covered here because the risk has been transferred to the vendor.

Threat modeling is a structured approach for identifying, evaluating, and security mitigating risks to a system. It is the process of examining a system from an adversary perspective to anticipate attack goals and assessing and documenting a system's security risk to help an organization to understand system threats (Swiderski & Snyder, 2004).

A threat model includes a list of typical attacks or security breaches most likely to be carried out by intruders to a system. The data flow approach to threat modeling is a systematic approach that follows the adversary's data and commands through the system from entry points. It shows parts of the application susceptible to security failures. The data flow approach is based on two main principles:

- An application cannot be attacked unless the adversary has a way to interact with it- attackers must actively jeopardize application security by interacting with it
- An asset of interest to the adversary must exist i.e. the asset must contain something of value to the attacker (Swiderski & Snyder, 2004)

At the context level, the system as a whole is represented as a single process node with external entities and data stores interacting with the system as data flows.

In Figure 4 below, Ketera e-procurement is represented two processing nodes to illustrate that the application exists across of several machines or different layers. External entities and data interact with the system via data flows. Machine boundaries appear as privilege boundaries and are represented by the dotted blue lines.

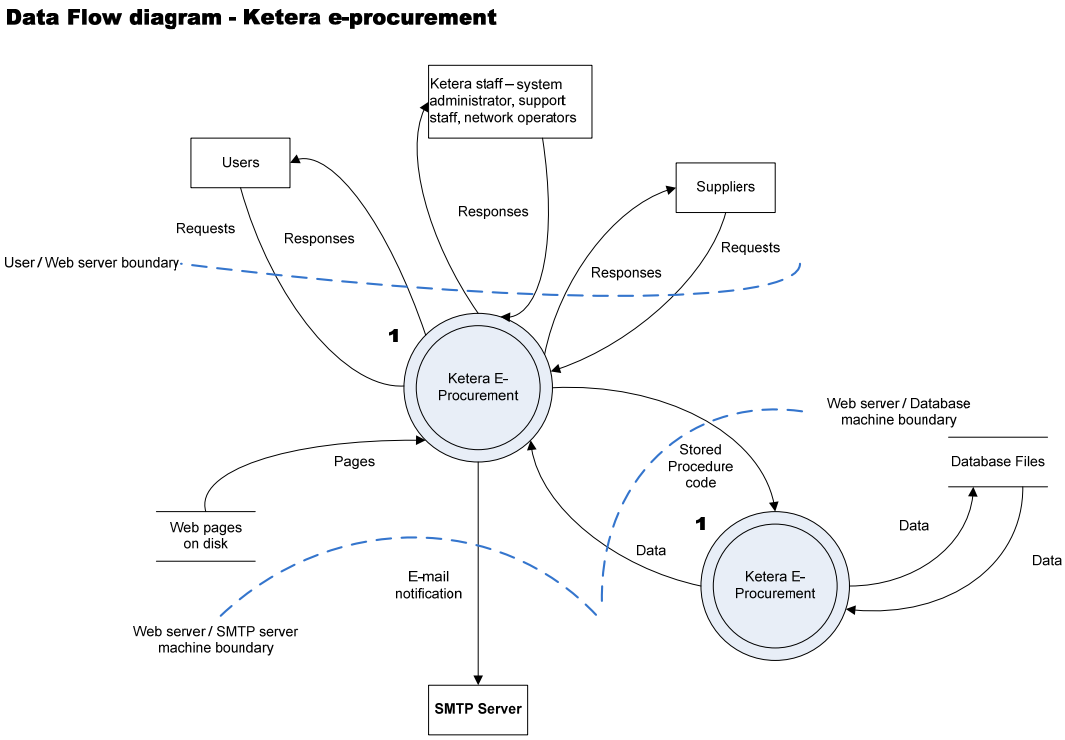


Figure 4. Level 1 data flow diagram

Table 1 shows the Risk Profile for Ketera. A risk profile denotes a range of risks or attacks to a specific asset. The organization receives e-procurement services from Ketera, therefore threats affecting the vendor could affect both access to the system by users and the ability of that service provider to provide critical services, skills, and

knowledge (Alberts et al., 2008).

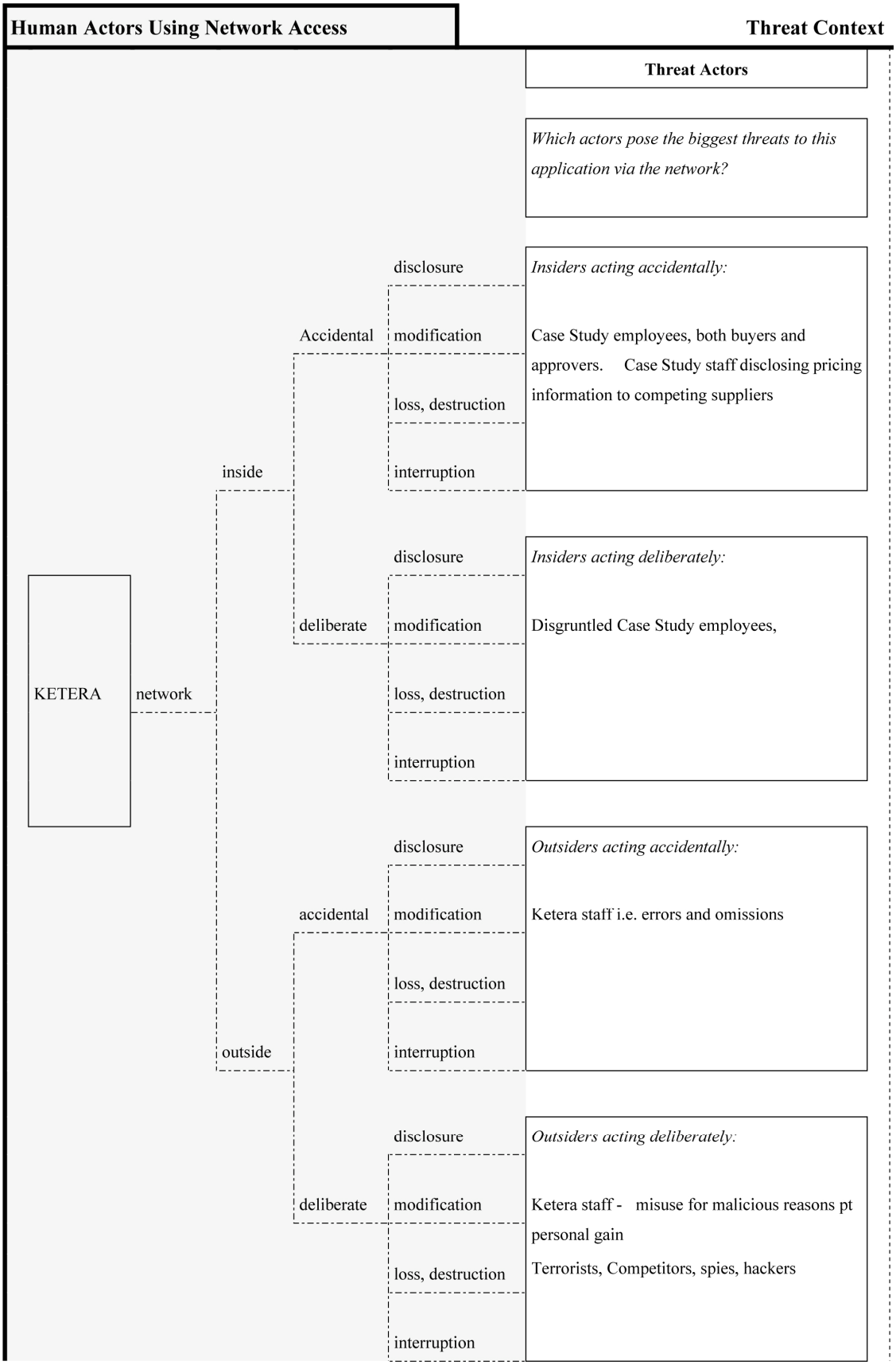
Table 2 above shows the Threat model for Human Actors using Ketera. Unauthorized insider attacks were ranked number 4 on the list of significant threats in 2001 (Whitman, 2004). Staff with legitimate system access can either deliberately or inadvertently dis-close supplier information in violation of the non-disclosure agreement. Further, disgruntled employees who are computer savvy can take over user login accounts and cause a considerable amount of destruction. There is no physical access to Ketera e-Procurement by case study employees because the application is hosted off site.

Ketera employees (administrators and support staff) with access the network can cause deliberate or accidental acts leading to significant disruption in service provision.

Table 1. Ketera risk profile key: L – Low; M – Medium; H - High

Application Problems			Basic Risk Profile						
	Threat *For which branches is there a non-negligible possibility of a threat to the asset? Mark these branches on the tree.* *For which of the remaining branches is there a negligible possibility or no possibility of a threat to the asset? Do not mark these branches.*		Impact Values *What is the potential impact on the organization in each applicable area?*						
Asset	**Actor**	**Outcome**	**Reputation**	**Financial**	**Productivity**	**Fines**	**Safety**	**Other**
KETERA	Case Study Employees	disclosure	H	M	L	-	-	-
		modification	M	M	L	-	-	-
		loss, destruction	M	M	H	-	-	-
		interruption	L	M	M	-	-	-
	Malicious Hackers (i.e. virus, worm Trojan, back door.)	disclosure	H	H	L	H	-	-
		modification	M	M	H	M	-	-
		loss, destruction	M	M	H	M	-	-
		interruption	M	M	H	M	-	
	Competitors / Spies	disclosure	H	M	M	M	-	
		modification	M	M	M	M	-	
		loss, destruction	M	M	H	M	-	-
		interruption	M	M	H	M	-	-
	Natural Disasters	disclosure						
		modification						
		loss, destruction	M	M	H	M	H	-
		interruption	M	M	H	M	M	-

Table 2. Threat model - Human factors



4.2 Phase 2-Identify Infrastructure Vulnerabilities

Ketera has ashared database architecture and security defense is primarily implemented at application level. Like many other COTS packages, the availability of Ketera is important for both users and customers and any disruptions have the potential to affect revenues, negatively impacting confidence of both the vendor and the buying organization and even damaging brand (De Vries, 2004).

There are 2 main types of application attacks: those that affect known vulnerabilities in commercial software (IIS, Apache, etc.), and those that target custom internally developed web application vulnerabilities that are specific to each enterprise.

1) Known attacks on commercial software require less sophistication on the part of the hacker, who mainly takes advantage hacking tools that are publicly available to exploit known vulnerabilities (the so-called script kiddies). Protection against these attacks can usually be achieved by ensuring regular application updates, and deployment of existing signature detection technology in the network firewall.
2) Attacks that target custom development vulnerabilities generally require insider knowledge (or a very determined attacker). Implementing password policies such locking unsuccessful accounts after 3 unsuccessful login attempts and detecting when an authentication attempt is a direct replay of a previous attempt using time-stamps should be incorporated into the authentication process (Stankard & Gehling, 2005).

Ketera is prone to application level attacks. Typically, these attacks exploit flaws in the bespoke application design and implementation to prevent legitimate access the service. Application level attacks will typically not be detectable or preventable by common security monitoring tools. Hacker's find them more efficient because they target bottlenecks and resource limitations within the application using small amounts of bandwidth.

Application level attacks tend to target the weakest link in the environment – i.e. for a web farm with many servers reliant on a single back-office host to authenticate users; an application attack may directly target it. Further, application level attacks are harder to trace (De Vries, 2004).

Security testing is performed to identify vulnerabilities to a system. The threat model drives security testing which is governed by these attacks. It is important to ensure that the most accessible areas of entry into the system are given priority during the testing process (Swiderski & Snider, 2004).

The results of security testing provide an organization with the information required to address these vulnerabilities (Landoll, 2006). There are 3 main types of testing:

Design/threat model reviews analyse a system's architecture for security flaws. The goal is to prevent system specific attacks the target the unique assets of the system.

Code reviews search for vulnerabilities that are countered by security coding practices. Code reviews typically follow the data and process flows from entry point and analyze the code for potential issues or flaws.

Penetration testing is a simulation of an adversary's attempt to achieve specific malicious goals to the system. Penetration testing shows how much an adversary with-out insider knowledge can discover about a system (Swiderski & Snyder, 2004).

Ketera is a vendor hosted solution and its security testing for the case study focuses on penetration testing involving both Network & Application level penetration testing.

Penetration testing helps to safeguard an organization against failure by preventing financial loss through fraud or lost revenue due to unreliable business systems and processes; provides due diligence and compliance for industry regulators, customer and shareholders; and protects organizational brand reputation by avoiding loss of confidence and reputation.

Network Penetration Testing is carried out to discover network services that are visible from the IP (Internet Protocol) address provided by case study. The tests involve searching for: The presence of known vulnerabilities, the degree of information that can be obtained from the service and whether available vendor fixes or patches have been applied to address vulnerabilities with the available services.

Application Penetration Test involves the following:

1) Anonymous User Review involves working without valid login credentials; the extent to which a malicious hacker can gain access or obtain unauthorized information was testing by exploiting vulnerabilities to gain unauthorized access.
2) Validated User Security Review: involves working with three valid sets of user authentication

credentials, attempting to subvert the application using one user credential to access or modify unauthorized data from the another company's (third party's) information space, or perform unauthorized actions by one of the accounts bypassing assigned permissions. Success is defined by a compromise in the integrity or confidentiality of the application or back-end data.

The Case Study has two main documented security policies which govern the transactional data in Ketera e-Procurement:

1) The Outsourcing Policy; and
2) the Digital Security Standards and Guide

While the organization doesn't have a security policy specifically for e-procurement systems, third party vendors must conform to standards set out in Case Study Outsourcing Policy below:

General: Security management will, at a minimum, meet all of the standards laid down in British Standard BS7799 / ISO 17799, including clearly defined security responsibilities, processes for risk management, authorization and administration, security design and configuration management, audit and assurance. BS7799 / ISO17799 certification will be attained/maintained or extended to cover the site, services and organization supporting the agreed services for the case study.

Ketera is required to make reasonable efforts to ensure that the following security standards are is in place throughout the life of the service to the case study, including the following points:

1) Any Data Protection (privacy) and other regulatory obligations are met.
2) Individuals and processes not authorized by the organization will not gain access to other systems and networks operated for and on behalf of the organization by using the Service Providers link to the organization.
3) Case Study systems and data will be shared or segregated from those of Ketera and other customers to the level agreed in each Project Engagement Definition.
4) The staff and contractors employed by Ketera will not inappropriately access, use or distribute personal and/or confidential information.
5) Following loss of data, system, network, key staff or physical environment, full service operation will be recovered within timescales agreed in the Project Engagement Definition. Tested plans will be in place to evidence that this target recovery can be reasonably achieved.
6) Unauthorized software, including viruses, will not be introduced into systems and networks operated for and on behalf of case study.
7) Intellectual property rights of organization, or licensed to organization by third parties, will not be violated.
8) The physical security of the perimeter of buildings used for the service will reasonably deter and detect unauthorized entry. Specific physical security requirements in terms of shared or segregated facilities will be agreed as part of each Project Engagement Definition.
9) Industry standards of fire, environment and water protection will be maintained for all systems supporting case study services.
10) In all cases, however, the organization expects the general principles for good security to be followed and reflected in actual management and operation of the services.
11) Risks relating to the security objectives will be assessed following any significant system change, as a result of new threat or vulnerability information and at least annually.

Ketera and the case study, working with other suppliers and service providers in the supply chain, will commit to a shared process of continuous improvement in security technology and operation to ensure security management objectives are met effectively and efficiently. The improvement process will recognize changes in business risks, operational requirements, technology, threat levels, and industry best practice. A security forum with members from relevant case study suppliers will be established to facilitate this and Ketera is required to participate in this.

Ketera will carry out an agreed level of reference and/or back-ground checking for all individuals (staff and contractors) involved in providing the service to gain assurance of integrity. Staff training, monitoring and segregation of duties will be sufficient to ensure management control is in place.

Ketera must have access to sufficient skills and knowledge in security and technology to provide both Ketera and case study assurance, through formal continual and periodic measurement processes that security objectives are actually being met.

Ketera will provide assurance that any encryption services specified in a particular service contract can be carried out in terms on government export, import or usage regulation. Expectations on government access to cryptographically protected messages and channels will be clearly defined in terms of who owns the government relationship and controls access to keys. The organization will always need to expressly authorize the release of keys or the use of key escrow for system securing our information.

The organization has a comprehensive set of well documented, current policies that are periodically reviewed and updated.

The following is a subset of the digital security standards and guide:

1) User Accounts & Passwords: Case study employees must take appropriate steps to manage their passwords in a secure manner, and to prevent their disclosure to unauthorized persons. The use of another person's account without permission or the impersonation of another user on case study systems or in any connection to third party systems is strictly forbidden.
2) Sensitive Information: The case study's Security of Information Standard sets requirements for classifying, disseminating, storing and destroying sensitive or valuable information. All employees must know and comply with the principles and duties for handling information set out there.
3) Viruses and Worm: All employees must act appropriately to prevent the spread of vi-ruses and worms within the case study's networks and Digital Systems. All personal computing devices that connect to or use case study information or case study Digital Systems must use up-to-date antivirus protection.
4) Software Patches & Updates: The use of up-to-date software and the application of software patches and updates are important to the organisations security. All personal computing devices that connect to or use case study information or case study IT Systems must be kept updated and patched.
5) Security Incidents: Awareness of any event or circumstance that leads to the belief or suspicion that the integrity or confidentiality of case study's IT Systems or of case study's digital information has been compromised or is being used in breach of case study's policies and standards or contrary to local law, must immediately be reported to the local Digital Security Controller or Group Security representative.

4.3 Phase 3-Develop Security Strategy and Plans

An independent risk assessment was carried out on Ketera by KMPG in October 2006. The tests were carried out in a live environment using a combination of black box testing and source code reviews appropriate tools and scripts. The risk classification is as follows:

Table 3. Risk classification in Ketera security assessment of eprocurement application (2006)

Classification	Severity	Likelihood
High	Ability to take full control of the system/environment, or ability to disable application.	Publicly released exploit or simple to exploit (by script kiddies, for example).
Medium	Ability to take restricted control of the system/environment, to reconfigure or cause localized malicious damage.	The vulnerability has been published, but an exploit may not necessarily have been published. A potential intruder with an average relative skill level may be able to exploit this vulnerability.
Low	Simple Information Gathering. With this relative danger level, it is unlikely that exploitation will lead to the potential intruder being able to gain further access or inflict malicious damage.	The vulnerability has not been publicly released or it may require a potential intruder with very advanced skills to be able to exploit the vulnerability.

The top threats identified for Ketera are listed in Table 4.

Table 4. Ketera – Top application level threats

No.	Issue	Risk
1	Database SQL Injection	High
2	Ability to list orders made by different corporate entities	High
3	Reflected unauthenticated cross-site scripting (XSS)	High
4	Reflected unauthenticated cross-site scripting (XSS)	High
5	Ability to edit approved requisitions	Medium
6	Auto-complete attribute is not disabled	Low
7	Apache Tomcat error pages leak information	Low

For more information on the threats and the impact on the system see Appendix A.

Issues 1 – 4 in Table 4 are all application level DoS (Denial of Service) attacks. They represent a subset of potential attacks on the application and are aimed specifically at disrupting operation rather than subverting the application controls i.e. Database SQL injection and Cross site Scripting (XSS) (De Vries, 2004).

Technical security controls can range from simple to complex and can be configured to guard against specific types of threats. The goal of security controls is to protect information systems, ensure data confidentiality, availability and support for critical business process.

Technical controls can be categorized according to their primary function.

- Supportive controls are universal and intrinsic to information technology systems. These include identification – the ability to uniquely identify resources; system protection which are built into systems during technical implementation; and security administration which includes subsystem security used to administer access and change to the environment (Vellani, 2007).
- Preventative controls aim to guard against threats exploiting vulnerabilities in the first place. These are superior to other types of controls and include: authorization, authentication, privacy, non-repudiation (verify sender and receiver information); and protected communications (encryption).
- Detective Controls detect or indicate that an error or possible error has occurred. These include auditing of events, virus detection and checksum (redundancy check to ensure that data is not being changed (Vellani, 2007).

Data gathering for technical controls involved a review of security controls supplied by the vendor, identifying existing vulnerabilities and documenting results.

Appendix B shows a list of technical controls of case study user categorized by primary function.

Appendix C shows a list of technical security controls identified for Ketera e-Procurement mapped against security threats.

5. Proposed Security Model

A security model can be defined as framework for managing security. It takes into account threats, attacks, vulnerabilities and control measures. The proposed security model is based on an evaluation of the security policies, procedures and practices for Ketera e-procurement, It focuses on risk mitigation activities which can be implemented to close the gaps identified in the current security model.

The following areas have been identified for improvement to increase the security of e-Procurement transactions in Ketera. These have been prioritized based on vulnerability and impact to the organization:

5.1 Application Level Security (Priority: High)

Ketera has implemented application level controls to protect confidentiality of data at application level. However, this must be considered an interim quick fix as it only fixes the effect of the design flaw and not the cause. The application should be reengineered to fix this design flaw by introducing database level controls in addition to application level controls to protect confidentiality of data (e.g. storing data of different clients in different

databases/tables, using different database credentials to access database for different corporate entities). This could effectively reduce the complexity of the application level ACL code, serve as an effective safeguard for the data stored in the back-end database and mitigate risk of programming errors in the application level controls. The recommendations are summarized in Table 5.

Table 5. Ketera – Recommendations for top application level threats

Threat No.	Recommendation	Risk / Priority
1	Input parameters such as form fields, which are used in SQL queries should never be passed from client side without proper validation and sanitization.	HIGH
2	The application should be reengineered to segregate data belonging to different clients into different databases and/or tables. Access control checks should also be built into the data retrieval modules to prevent unauthorised access to data.	HIGH
3 & 4	The application should not rely on client-side input even if there is client side validation. Sanitize potentially dangerous characters on the server side at all times. In addition (or if these characters are needed), HTML encode meta-characters in the response.	HIGH
5	Application checks should be carried out to prevent unauthorised modification to "read-only" requisitions.	HIGH
6	Turn off AUTOCOMPLETE attribute in form or individual input elements containing username or password by using AUTOCOMPLETE='OFF'	LOW
7	Generic error message should be displayed to the user and all exceptions should be logged for further examination by developers and/or administrators.	LOW

5.2 Security Awareness Training (Priority: Medium)

Security Awareness training is not actively promoted throughout the organization. The following improvements should be implemented.

1) Case Study Management needs to back a strategy for increased and comprehensive security awareness training for all staff. For example, security awareness training should be incorporated into the yearly pass renewal programme for all employees.
2) The frequency of security awareness communication and training should be increased and not left to the discretion of line managers

Security awareness that brings about behavioral change, reduces employees' vulnerability, and protects against threats can have a positive impact overall on risks related to in-formation assets (Okenyi & Owens, 2007)

5.3 Authentication (Priority: Low)

Ketera requires one form of identification when users log on to the system – namely user name and password. New users who log on to Ketera for the first time are requested to change password. While this represents a measure of security, two factor authentication – the practice of requiring at least two forms of identification for a user prior to confirming their identity (something you know, something you have or something you are) represents strong authentication (Landoll, 2006) would provide additional security controls. However, this option may not be considered appropriate because the information asset is considered confidential not secret. Further, the cost of implementing two factor authentication when measured against the potential benefits may not be justifiable.

5.4 Vulnerability Assessment (Priority: Low)

Penetration tests are carried out once a year as a planned exercise. This gives Ketera an opportunity to correct any outstanding identify risk areas. Further, while cost is a factor in determining the frequency and scope of penetration tests, it may be prudent to carry out more than once a year to ensure that Ketera meets the security challenges of a constantly changing environment.

6. Conclusions

The security policies, procedures and results of interview and surveys were assessed to understand the current security practices and make recommendations for a new security model that could be part of the reengineering process of the supply chain management system of the case study.

While both the Outsourcing Policy and Digital Security Standards and Guide for case study employees appear to meet most of these requirements, these policies are not effectively communicated to employees evidenced by the results of the survey which showed that most users were unsure of the escalation procedures for security breaches and the importance of keeping passwords secure. Some thought it acceptable to give IT staff and colleague their passwords as they are 'trusted' employees. Indeed, only members of the Digital Security Solutions team seem to know about these polices and policies and procedure for escalating security breaches.

Passwords are often the foundation on which much of information security is built and represent one of the biggest practical areas of vulnerability for a system (Anderson, 2001). Ketera relies on users keeping their password secret and poor security awareness training makes users vulnerable to social engineering were attackers extract passwords directly by telling some plausible untruth (Anderson, 2001).

Authentication and Vulnerability Assessment have been given a low priority rating be-cause the e-procurement transaction data is confidential not secret, and therefore, while important, is not critical to the organization.

The shared database architecture has been identified as an area of high risk for Ketera. At present, Ketera appear to be unwilling to reengineer their application to segregate data belonging to different clients into different databases and / or tables and build access control checks into the data retrieval modules to prevent unauthorized access to data. They are however, committed to looking for ways to add additional access controls beyond the application layer access controls.

A proactive approach to mitigating this area of high risk is to ensure that vendors are not just compliant with a security architecture which supports secure operation between Case Study's desktop and internal applications in a manner transparent to the end user but have an systems design and architecture which conforms to the organisation's internal standards for development where access control mechanisms for applications are applied at both the network and application level – a features that does not apply to Ketera e-procurement. The organisation's management needs to make a decision about whether or not this continues to be acceptable risk and act accordingly.

This case study examines and evaluates the organization's security practices for transaction data for the integration with the Ketera e-Procurement. The risks identified were based on solid empirical findings and the recommendations for mitigating these risks can protect the organization against threats that can have a significant negative impact on the organization's reputation and directly affect the bottom line. The research highlights areas of risk and new security model can help the organisation to better focus its security efforts, thus increasing the probability of protecting information and reducing the vulnerability of e-procurement transaction data to attack.

The proposed research methodology for the assessment of security of integrated e-procurement systems can be used for supply chain reengineering projects that require integration of similar outsources e-procurement solutions and most share similar concerns. The security model proposed for e-Procurement integration for this research can be applied to many reengineering projects of similar sizes that rely on an external system like Ketera. While the proposed model is valid today, a security assessment performed in the future may lead to different results due to emerging new threats or those not previously identified due to the limitations of this study.

References

Alberts, C., Dorofee, A., Stevens, J., & Woody, C. (2008). *OCTAVE-S Implementation Guide*. Retrieved October 20, 2012, from http://www.cert.org/octave/osig.html

American Psychological Association. (1972). *Ethical standards of psychologists*. Washington, DC: American Psychological Association.

Anderson. R. (2001). *Security Engineering: a Guide to Building Dependable Distributed Systems*. USA: John Wiley & Sons.

Angeles, R., & Nath, R. (2007). Business-to-business e-procurement: success factors and challenges to implementation. *Supply Chain Management: An International Journal, 12*(2), 104-115. http://dx.doi.org/10.1108/13598540710737299

Calder, A., & Watkins, S. (2012). *IT Governance: An International Guide to Data Security and ISO27001/ISO27002*. Kogan Page.

CIECA. (2010). *Security for Electronic B2B Transactions*. Retrieved April 15, 2013, from http://www.cieca.com/Resources/Documents/SecurityforElectronicB2BTransactions-2010-06-23.pdf

De Vries, S. (2004). *Application level – Denial of Service Attacks*. Retrieved July 17, 2012, from http://www.net-security.org/dl/articles/Application_Level_DoS_Attacks.pdf

Gebauer, J., Shaw, M. J., & Zhao, K. (2003). The efficacy of mobile e-procurement: A pilot study. In *System Sciences, 2003. Proceedings of the 36th Annual Hawaii International Conference on* (pp. 1-10). IEEE.

Gehling, B., & Stankard, D. (2005). eCommerce Security. *Proceedings of the 2nd annual conference on Information security curriculum development*. InfoSecCD 2005 2nd Annual Information Security Curriculum Development Conference, ACM, NY. http://dx.doi.org/10.1145/1107622.1107631

Ketera Technologies. (2012). *Procurement*. Retrieved April 14, 2012, from http://www.ketera.com/solutions/procurement.html

Klueber, R. (2002). ASP Strategies and Solutions for eProcurement Processes Offered by an eMarket. In *System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on* (pp. 2820-2829). IEEE.

Kouns, J., & Minoli, D. (2011). *Information Technology Risk Management in Enterprise Environments: A Review of Industry Practices and a Practical Guide to Risk Management Teams*. Wiley-Interscience.

Landoll, D. J. (2006). *The Security Risk Assessment Handbook: a Complete Guide to Performing Security Risk Assessment*. New York: Auerbach Publications.

Mohammadi, A., Sahrakar, M., & Yazdani, H. R. (2012). Investigating the effects of information technology on the capabilities and performance of the supply chain of dairy companies in Fars province: A multiple case study. *African Journal of Business Management*, *6*(3), 933-945.

Mulholland, S. (2012). *Procurement, the Internet & You*. Retrieved April 29, 2012, from http://www.e-hub.com/pages/procurement.doc

Neef, D. (2001). *E-procurement: from strategy to implementation*. FT press.

Okenyi, P. O., & Owens, T. J. (2007). On the Anatomy of Human Hacking. *Information Systems Security. 16*(6), 302-314. http://dx.doi.org/10.1080/10658980701747237

Price Waterhouse Coopers. (2012). *Sarbanes- Oxley and Strategies for Compliance*. Retrieved July 18, 2012, from http://www.pwc.com/sg/en/audit/sarbanes-oxley-compliance.jhtml

Subramaniam, C., & Shaw, M. J. (2002). A study of the value and impact of B2B e-commerce: the case of web-based procurement. *International Journal of Electronic Commerce, 6*, 19-40.

Swiderski, F., & Snyder, W. (2004). *Threat Modeling*. Washington: Microsoft Press.

Tai, Y. M. (2011). Exploring the performance impact of web-based direct procurement systems: from the perspective of process integration. *WSEAS Transactions on Information Science and Applications, 8*(9), 380-390.

Tanner, C., Wölfle, R., Schubert, P., & Quade, M. (2008). Current Trends and Challenges in Electronic Procurement: An Empirical Study. *Electronic Markets, 18*(1), 6-18. http://dx.doi.org/10.1080/10196780701797599

The Security Risk Analysis Directory. (2005). Introduction to Risk Analysis. Retrieved April 15, 2013, from http://www.security-risk-analysis.com/introduction.htm

Vellani, K. H. (2007). *Strategic Security Management*. Oxford: Elsevier.

Whitman, M. E. (2003). Enemy at the Gate: Threats to Information Security. *Communications of the ACM, 46*(8), 91-96. http://dx.doi.org/10.1145/859670.859675

Appendices

Appendix A. Ketera: Top threats & impact

Ref.	Threat / Issue	Impact	Likelihood	Severity	Risk
1	Database SQL Inject	Depending on back-end database, it may be possible to retrieve arbitrary data from the database.	High	Medium	High
2	Ability to list orders made by different corporate entities	Privacy and confidentiality of customer data can be compromised	High	High	High
3	Stored Cross Site Scripting (XSS) vulnerability	Ability to execute arbitrary Javascript may potential intruder to force an approver's browser to approve / request approver knowledge, one the approver clicks on the attachment. Cross Site Scripting (XSS) allows potential intruders to steal session cookies, thus exposing the user's session to hijacking / replay attacks.	Medium	High	High
4	Reflected unauthenticated cross site (XSS) vulnerability	If potential intruder manages to trick users into clicking on specially crafted URL, users' session can be hijacked as the intruder would be able to obtain the users' session cookies. Further, the above vulnerability can be used to perform phishing attacks, which may damage business reputation.	High	High	High
5	Ability to edit approved requisition	Vulnerability may allow potential intruder to commit fraud by bypassing the approval process control to change the quantity, billing/shipping addresses.	High	High	High
6	Reflected authenticated cross site (XSS) vulnerability	If potential intruder manages to trick authenticated user into clicking on specially crafted URL, user's session can be hijacked if the intruder obtains the session cookies. Additionally the above vulnerability can be used to perform phishing attacks, which may damage business reputation. Intruder could also perform actions by using the privileges of the affected user.	Low	Medium	Medium
7	Auto-complete attribute was not disabled.	Usernames and passwords stored in the browsers may be retrieved by potential intruders. Thus compromising the user accounts.	High	Low	Low
8	Apache Tomcat exception error pages leaked information	Information leakage which allows potential intruders to understand the internal logic and codes of the application.	Medium	Low	High

Appendix B. Technical controls for case study users

Control Measure	Function
• The use of a secure RSA key to access the Ketera via the Intranet	Preventative - authentication
• Password policies – passwords are of medium strength and consist of a combination of upper and lower case letters and numbers	Supporting – administer and manage changes to the environment
• E-mail monitoring • Anti-virus Software • Anti-spam filters • Spy-ware removal software on all Case Study workstations	Detective – virus detection
• Screen savers - all workstations have active screen savers with passwords	Supporting – system protection
• Personal Firewalls on all Case Study workstations	Detective – auditing events

Appendix C. Security threats and technical controls

No.	Threat	Motivation	Actions	Outcome	Controls
1	**Insiders** (Case Study employee – poorly trained, disgruntled, malicious or terminated employees)	Curiosity; Ego; Intelligence; Monetary gain; Revenge; Unintentional errors and omissions	Blackmail; browsing proprietary information; computer abuse; fraud and theft; input of falsified or corrupted data; malicious code; sale of personal information; system sabotage; un-authorised system access.	Disclosure Modification Loss, disruption Interruption	Network Monitoring, Audit Logs; Discretionary access control, Encryption, Antivirus system, Anti-spyware system
2	**Outsider**s – Ketera staff	Curiosity; Ego; Intelligence; Monetary gain; Revenge; Unintentional errors and omissions	Blackmail; browsing proprietary information; computer abuse; fraud and theft; input of falsified or corrupted data; malicious code; sale of personal information; system sabotage; un-authorised system access.	Disclosure Modification Loss, disruption Interruption	Network Monitoring, Audit Logs; Discretionary access control, Encryption, Antivirus system, Anti-virus system
3	**Hackers**	Challenge; Ego	Social Engineering, System Intrusion, break-ins, unauthorized system access	Disclosure Modification Loss, disruption Interruption	Logical Access Control, Vulnerability scanning tools; Path management. Anti-virus, Anti-spyware; data encryption - SSL, Secure FTP (sFTP); for data transfer; digital signatures used for workflow processes; Security Policies, Security Awareness training for employees, Password controls.
4	**Industrial Espionage** - Competitors	Ego; Intelligence; Monetary gain; Revenge;	Competitive advantage, Economic Espionage Economic exploitation, information theft; social engineering, unauthorized system access (to classified or proprietary information	Disclosure Modification Loss, disruption Interruption	Antivirus Software; Intrusion detection systems i.e. Firewall; Security Audit logs; Backup Management; Security Awareness Training for Ketera Staff