Secured Information Access based on Bell LaPadula Model A Case of Novel Publishing Company

Rathnakar Acharya
Alliance Business Academy
Bangalore. India

Dr. V. Vityanathan
Dept. of CSE. SASTRA University
India

Dr. Pethur Raj Chellaih
Robert Bosch Bangalore,
India

ABSTRACT
Information is one of the important assets of an organization. Protection of information assets is necessary to establish and maintain trust between the organizations and its customers. Information security is the process by which an organization protects and secures its resources and maintains information vital to its operation. When our resources go online are available to multiple users it is vulnerable to all kinds of security threats. Proper access control mechanisms will prevent the unauthorized users to make an attempt to access the corporate database or other user's information'. This paper presents an approach to the formed analysis of security required and access based on Bell LaPadula model followed with a case study conducted on a leading publishing company.

Keywords
Information security, Bell LaPadula model, IDS, Access mode, Access control.

1. INTRODUCTION
Information is today's most vulnerable resource in any organization. The American Arbitration Association with reference to the case of dispute between IBM and Fujitsu Ltd in 1987 issued a resolution of the dispute that included continued access to the information of each party by the order, in secured facilities and following precise rules, and monitoring of compliance with the rules by a technically expert independent supervisor. The extent, cost, and complexity of arbitration demonstrate the value of the matter in dispute, namely information on software constructions. Today in any business, information has become a valuable and necessary resource. An excellent manager may take better decision with poor quality information but an average manager would be in a position to take better decision with high quality information. In today's competitive business environment, a company without quality information would suffer a serious competitive advantage.

Security to 'resources' of the organization is considered as an essential function in an organization and also as one of the strategic issues considered in planning and development process. In the electronic era security to data and information becomes a critical factor. While we talk of good governance and transparency, with an intention to provide access to information, securing the strategic resource becomes very crucial. It has special attention in publishing industry especially that also provides allied services where third party information is in the process. Securing the data and at the same time extending accessibility to the same data to both internal and external customers is a challenging task. Since the technology being made available to the users with out any discrimination, and the information that is made available over the Internet, it is virtually the intelligence of the organization to see how best it makes use of the information and stands different and meets the requirements of the customers. Managing, preserving and making the data and information accessible on demand at various levels in the working environment can be made possible when the organization has a well planned information security system. Following paragraph illustrates the importance of data and information security.

Protegrity Corporation, during Nov04, the leading technology innovator for enterprise-wide database and storage security, has signed a contract with a company in the top 50 of the Fortune 500 to implement Secure.Data, the company's software solution for centralized management and auditing of data security policies and for data encryption. 'Secure.Data' will be immediately installed to protect sensitive and private customer, employee, and financial data on 15 to 20 different servers operating Oracle- and MS SQL Server-based applications. This was basically to focus on data encryption to application and hardware-based security solutions", automatic key management, the ability to separately manage and audit security responsibilities, and to effectively secure data with minimal impact on application performance." With minimal staff resources to avoid risk and face the challenges of customizing mission-critical applications and gain legal compliance.

The primary driver behind the decision was California SB 1386, a law that encourages businesses to encrypt non-public personal data in order to avoid penalties. The law affects all organizations that maintain information about California residents. Corporate customers implement Protegrity's solutions to centrally define and manage enterprise data security policies and to comply with current and emerging regulations such as HIPAA, Sarbanes-Oxley, and Visa's Cardholder Information Security Program (Visa CISP), as well as California SB 1386. Data and information security is a critical factor and the most challenging task. In US despite the considerable amount of research is made to tighten up IT security and amount of money and effort already spent on protecting sensitive U.S. government data, the threats keep getting more sophisticated and also the stakes. The U.S. Department of Defense (DOD) is leveraging PC blades to address a long-time concern that electromagnetic waves containing key characteristics of classified data could be intercepted by enemies of the United States and then used to compromise national security.

At the same time, in India too many companies are extending the data and information security application service to other countries. In the beginning of 2004 India invited higher participation from France in clinical research and assured French companies that they would be provided "data security and patents' under the new law from January 2004. India would adhere to the January 1 deadline set by the World Trade Organization for introducing the products patent regime in the country. By introducing legislation in this regard, India could prove to be a stepping stone for global entry. This snapshot provides us the potential India has in providing this service across the globe. Probably this could be another reason why India has been chosen as a destination for BPO activities apart from the reason like cheap labour.

We organize rest of this paper as follows; section II provides overview about what is information security. In section III we explain the controlling access of information flow. Section IV gives details about the commonly used security tools. In section V we have taken up the case study of a publishing company having global presence and with diversified services to clients apart from its core publishing activity and followed with conclusion.

2. WHAT IS INFORMATION SECURITY

Over the last five decades, distinct ways of doing business have emerged - in the 1950s, anyone who had access to capital was making money; in the 1970s and 1980s, it became information driven, so companies like Juniper and Cisco did well because they were leading in information. But today information is in abundance, so doing business is about intelligence. When a Pfizer competes with a Ranbaxy, they aren't competing on information. They are competing on one innovative formula. Unilever (HLL) is competing on a brand strategy, so it is competition on intelligence and innovation. And it is not just important to generate that innovation. It is more important to protect that innovation. They realized that to do business, things like competitive strategy and competitive intelligence are critical.

About 10 years ago, when security started becoming a concern, people thought of security as information technology (IT) security. So passwords, firewalls and elaborate software came up. The trigger at those times was online transactions - banks started going online and suddenly everyone wanted to figure out a way to transact money online. That was when the security actually surfaced, and so information security became synonymous with IT security. But very quickly people realized that there was more to security than that. The need for security is directly influenced by business dependence on IT and also the budgets allotted for it and hence the security solutions are specific to different verticals. This has a great momentum for BPO industry because information is the life blood of this industry.

Information security isn't limited to businesses alone. It also transcends borders. Today, information warfare isn't between businesses only but also between countries. Information security is the process of ensuring that all types of information (that is information (ie. Paper, microforms, electronic and mental) created during company business operations including engineering, structuring and delivering the services) is appropriately protected. Appropriately refers to a process of management risk acceptance and the assignment of relative information value through classification. Management risk acceptance refers to senior management guidance, from decisions based on risk analysis and other data, concerning the investments considered appropriate to information protection, generally or in specific cases of information sets or applications. Assignment of relative values refers to decisions made by the originator or owner in the case of a system application of an information item or set, concerning the appropriate digital classification, and hence the protection effort to be expanded for that item or set. Information security policy [10] and standards specify the definitions and protection for each classification that include network security, computer security, application security and document security.

2.1 Evolution of information security

Reflecting on the evolution of security, we see four waves or phases. In the first phase (before the mid 90s) enterprise had not yet connected to internet. In fact inter office or inter branch connectivity were rare or not constant. The prime objective was confidentiality and integrity of information. Organizations put in access control to lock up information, making selective information available to select individuals or groups.

In the second wave (mid to late 1990s), companies began connecting to the Internet. This was also the time when the major security threat was internet worms and viruses which is still today a major issue, and hence antivirus products and firewalls were prime security solutions. People then resorted to more sophisticated means of attack. Malicious codes on the web pages or embedded in e-mail overwhelmed corporate web servers. Hacking tools like were made available on web sites, and anyone could download these and use it to launch attacks on internet servers. This led to firewalls and its implementation to filter out malicious codes and safeguard themselves from script kiddies.

In the third phase (present day) worms spread within minutes and disrupt corporate networks. Hackers no longer attack just to brag about it. They now seek financial gain and steal credit card numbers or competitive information from corporate servers. Enterprises have opened up their networks to global customers, mobile workers, and suppliers. More sophisticated defenses are necessary to keep out the 'bad guys' and let in business associates. Sensitive information in transit needs to be secured. New tools like encryption, digital signatures [12], intrusion detection systems, virtual private networks, Access control mechanisms etc are being used. The fourth wave is around the corner. It is about security audit and certification. This not only cover just technology, but also people and processes. Enterprises will approach security from the attacker's end and safeguard new risks like social engineering and dumpster diving.

Information security is thus not just about technology issue- is also about people and process also. The answer to this is awareness and education. It has to be understood as a business issue apart from a technology issue alone. Data and information security is now considered as a business enabler and this is very much true with BPO industry. Here any

industry must involve employees at all levels, customers and all entities that deal with the organization. Hence information security is characterized as the preservation of: Confidentiality: ensuring that information is accessible only to those authorized to have access; Integrity: Safeguarding the accuracy and completeness of information and processing methods; Availability: Ensuring that authorized users have access to information and associated assets when required.

Information security management is a mechanism to achieve information security by implementing a suitable set of controls, which could be policies, practices, procedures, organizational structures and software functions. The three major sources that enable to identify the risk sources lies in the process of assessing the risk to the organization, legal and statutory, regulatory and contractual requirements that an organization, its trading partners, contractors and service providers, and the set of principles, objectives and requirements for information processing that an organization has developed to support its operations. In this context, the Primary goal of an information manager is to allow uninterrupted, secured access to information and keep the intruder at bay. When we think about the security of the information in an organization number of questions arise like; 'is the information system vulnerable to external attacks'? How to identify the risk to business and how to protect company's vital information recourse from hackers, competitors and unauthorized internal users? Does the organization have the right internal controls in place? While most of the companies understand the importance of IS security, but are seldom aware of what it takes to succeed in their security mission. However the security tools and applications are readily available but face big hurdles in choosing the right tool and implementing the right security initiative.

2.2 Security system structure

Security system may be proposed to all the layers like host link layer, application layer, and database layer of an IT based business system as in fig.1

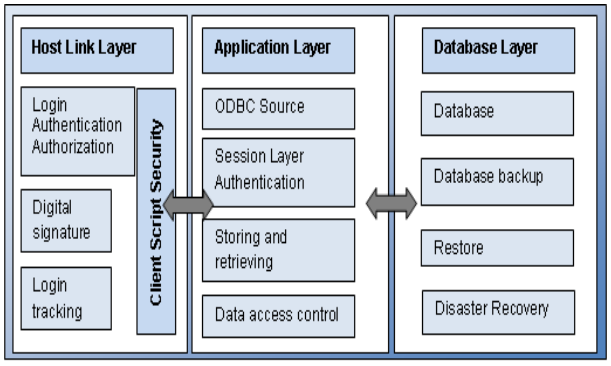

Fig. I Security system structure

Host link layer

It is an access layer for the users. Here users log's on to the system to enter, process or to do certain tasks on the data which is stored in the database. The security system incorporated in this section uses password it may be encrypted and store the password field of the database. This encrypted information cannot be accessed and used by unauthorized users without having proper decryption key.

User blocks: This module blocks the unauthorized users when they fails to login to the system.

Log Tracing: A log view is maintained by the system used by the user to access the information. It provides the information's about the users they tried to access the information like the different resources or files.

Digital signature: Digital signature [12] can realize the deification of the integrity of the original message also for non-repudiations.

Application layer security

Application layer is the main layer of any system. It is responsible for the management and control of different services requested by the users.

ODBC Data store: ODBC data store including oracle, SQL server, Sybase, MySQL, DB2, LUW, Teradata, Ingres, Informix, Progress and others. The ODBC extension can be used for distributed systems to mask and subset ODBC data help on windows, UNIX and Linux.

Session login authentication: This security mechanism avoids illegal users making attempts to access the information. i.e, it checks whether the user has the right to access the information.

Stored procedures: In web database system it is often to establish parametric storage procedures to access database. If the web layer is destroyed, attackers cannot insert any queries in order to search, change or delete the data stored in the database. Using stored procedures, web applications communicate with databases only through several specific strict parameters so as to separate user's identity from data processing, increasing the safety of data access.

Data access control: An access control has to limit and check data objects user can access and the access style of the same data objects is different for different users. Access control can be divided into three categories; Independent access control, forcible access control, and role based access control.

Database layer security

The function of data layer is to provide data storage service and data access interface for application layer, so security mechanism for database layer is the key concerns in every organization. Because of database exposure to the network any user with password in the network can access the database causing illegal users stealing or modifying or damaging data by direct access to database through illegal means.

Database: The database system contains customer's data, company data and all types of transaction data.

Database backup: The database has to create a backup at periodic intervals. Most of the database systems incorporated backup and recovery mechanisms. With the growing dependency in the workplace on information and general, and the information on our database requires safe backups and reliable recovery.

Restore: In a database is to bring back or rebuild the effected database.

Data recovery: It provides the management, monitoring and automation of software to create and maintain one or more standby database to protect the corporate data from failures, disasters, human error, and data corruptions. Manual or automatic failures to a disaster recovery stand by database to maintain high available for mission critical applications.

Security architecture life cycle

The security architecture is not a onetime solution for any organization [10]. It is an iterative process. That unifies the evolving business, technical and security domains. The four main phases of generalized security system architecture are;

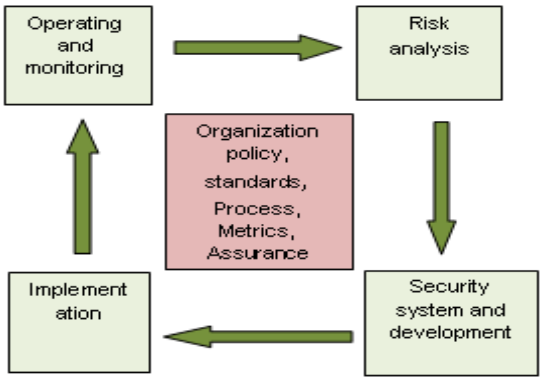

Fig. II Security architecture lifecycle

1. Risk analysis and assessment
2. Security system design and development
3. Implementation
4. Operating and monitoring

All these phases are related the organization policy [3], standard process, metrics assurance and IT strategies of the organization.

3. CONTROLLING ACCESS OF INFORMATION FLOW

A security policy [10] describes requirements for a system. Security models are a way of formalizing a policy. There are two basic paradigms.

1. *Access Control:* A system controls whether a physical (the subject) [2] is allowed to a resource (the object).

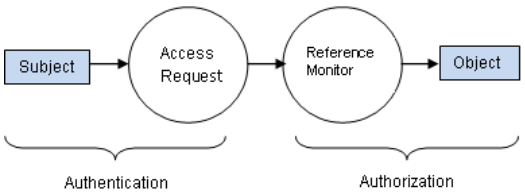

Fig. III Access Control

2. *Information flow control:* Dual notion some times used when confidentiality is the primary concert. The system control whether information may flow from a resource to a principal.

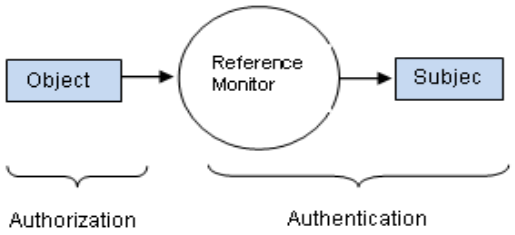

Fig. IV information flow control

Access operations: Access rights are models levels of granularity for defining security policy [10]. Each real operation requires partial access rights.

The basic access modes are:

Observe object ⟺ Examine contents of an

Alter ⟺ Change content of an object

With the above two models the access rights and their profiles are as below:

	exec	Read	append	write
Observe		**X**		**X**
Alter			**X**	**X**

Fig. V The access mode

The access control rights are modeled and defined as below;

Let, a set S of subjects and a set O of objects

A set A of operations (modeled by access rights)

We will consider $A = [exec, read, write]$ 'Eq. (1)'

An access control matrix $M = (M_{so})_{s \in S, o \in O}$ 'Eq.(2)'

	circular.doc	edit.exe	fun.com
User 1	**{ }**	**{exec}**	**{exec, Read}**
User 2	**{read, Write}**	**{exec}**	**{exec, read write}**

Fig.VI. Access rights allotted to different users

Where each entry $M_{so} \subseteq A$ defines rights for s to access o

Ex:

The matrix for $S = \{User1, User2]$ and three objects are;

3.1BELL-LAPADULA (BLP) Model

Bell-La Padula[1] (1973) stated a machine model for confidentiality. According to BLP permissions use an access control matrix and security levels. The security policy [10] prevents information following from a higher level to a lower level.

Consider the parameters;

Subject S, Object O, Accesses A as above.

A set L, of security level with a partial ordering, the state set $B \times M \times F$ captures the current permissions and subjects accessing objects.
The three parts are;

B= Possible current accesses
M= Permission matrices
F= Security assignment

The BLP state is triple (b, M, F),

$B = P(S \times O \times A)$ is the set of all possible current access. An element $b \in B$ is a set of triples (s, o, a). It means that s is performing operations a on an object o.

M is the set of permission matrices.

$M = (M_{so})_{s \in S, o \in O}$ 'Eq. (3)'

$F \subset = [L^s \times L^s \times L^o]$ is the set o security level assignment . 'Eq. (4)'

An element $f \in F$ is a triple (f_s, f_c, f_o)

Where,

$f_c : S \to L$ gives the maximum security level each subject can have $f_c : S \to L$ gives the current security level each subject $(st \quad f_c \le f_s)$ and $f_o : O \to L$ gives classification of all objects.

BLP Mandatory Access Control Policy (MAC):

Consider a state (b, M, f) where b is the set of current accesses.

Simple Security Property:

The ss-Property states for each access $(s, o, a) \in b.$ where $a \in \{read, write\}, then f(o) \le f_s(S)$ - no read-up

Star Property:

The *-Property states for each access $(s, o, a) \in b.$

Where,

$a \in \{append, write\} then \; f_s(S) \le f_o(O)$ and moreover, we must have $f_o(O) \le f_o(O)$ for all o' $with (s, o, a) \in b.$

$a' \in \{read, write\}$ (O must dominate any other object s can read).

These are the mandatory access control policy for BLP.

BLP allows the discretionary access control (DAC). The discretionary security property ds-property for each access $(s, o, a) \in b, we \; have that \; a \in M_{so}$ - discretionary access control is obeyed.

4. COMMON SECURITY TOOLS

Some common tools that are available today are:

Firewall: A firewall is a combination of software and hardware used to isolate a private system or network from the

public network. It is commonly used as a barrier between the secured corporate intranet, or other internal networks, and the internet which is assumed to be unsecured. Firewalls produce an easy to manage entry point to multiple systems behind it by controlling the type of information that is allowed to pass from the public network to the private network and vice versa. Firewall can also perform log activity to provide an audit trial in case of network being penetrated. It is a necessary tool when individuals trying to connect to the internet using their personal computers and dial–up–Line to safe guard against intrusion.

Intrusion detection system: Intrusion detection is the ability to analyze real time data to detect log and stop unauthorized network access. Business can install intrusion detection systems to monitor the network for real time intrusion and respond to intrusion in a variety of user determined ways and defend a web site against Denial of Service (DOS) attacks by adding more servers to increase the network traffic handled by the website by using filters and routers and by having a backup plan to route legitimate traffic during an attack. Cisco's secure intrusion detection system and network ICE's ICEpac security suite are the two examples of intrusion detection systems.

Virus scanning software: Virus scanning software including e-mail virus scanning called Antivirus software must be always kept updated. Two top rated antivirus software products are MCAfee's VirusScan and Symantec's Norton AntiVirus. The different types of Antivirus solutions are Gateway Antivirus Solutions, Desktop/Server Antivirus, Layered Protection, and Real-time Protection.

Secure Socket Layer Protocol: Using the secure socket Layer (SSL) Protocol [4] to protect data transmitted over the Internet provides encryption of data between the browser on the customer's computer and the software on the Web Server, allowing data such as credit card information to be transmitted securely. SSL uses digital certificates [12] so that a web browser can authenticate the server it is connected to making sure that credit card data is going to the appropriate server.

Security audit and penetration testing: Security audit can provide an overall assessment of a company web site and security issues by checking for vulnerabilities in those systems and providing recommendations for fixing those vulnerabilities. Security consultants such as DefendNet Solutions Inc., Internet Security system and Pinkerton Systems Integration offer security audit services. Accounting firms such as Arthur Andersen L.L.P and Ernst & Young also offer security auditing services.

Content vectoring and antivirus solution: The Content Vectoring is an asynchronous interface to server applications that perform file content validation. An important feature of this is scanning files for viruses or harmful applets as they pass through firewalls. The Content Vector Protocol defines a client/server relationship that enables different firewall systems to share a common content validation server. In essence, the one content validation server collects from multiple firewalls the incoming files that have been flagged for inspection. Content Vectoring Protocol (CVP) enables third-party Content Vectoring Servers to extend their content validation coverage to data streams controlled by VPN-1/FireWall-1 (which is developed by check point) gateways. Connections that match VPN-1/FireWall-1 Security Policy Resource rules will be passed or dropped based on the CVP Server's "opinion" of the safety of the data stream. The Resource rule may also be configured to give the CVP Server complete data stream editing control to replace or modify the data as needed. VPN-1/FireWall-1 and OPSEC auditing tools will log the CVP inspection results and issue alerts if configured to do so base on the information provided by the CVP Server.

Two factor authentication: Two-factor authentication is a security process that confirms user identities using two distinctive factors – something they have and something they know. By requiring two different forms of electronic identification, corporations reduce the risk of fraud and create greater assurance that the Internet is a safe place to do business. In a simplistic example, an automated teller machine (ATM) card and a personal identification number (PIN) represent a form of two-factor authentication. The ATM card and the PIN by themselves are useless to a prospective identity thief. Only when a person has and knows both factors can an identity be confirmed and access granted. This paper will explore the benefits of a variety of two-factor authentication methods and address possible applications for each method.

Public key infrastructure: Public key technology and a PKI depend upon complicated mathematical concepts, but its effects are simple and understandable. These keys are generated by using a local cryptographic module or provided through trustworthy mechanisms, subject to certain mathematical requirements. One of these keys is secret (*private*) and the other is published (*public*).The essence of public key technology is that messages or transactions authenticated or encrypted using one of the keys can only be verified or decrypted using his other key. The PKI uses special digitally signed messages (called "certificates") to bind identity to the public keys. A digital certificate [12] is issued by a trusted "Certification Authority" (CA) and signed using that CA's private signature key.

5. NOVELL AND NOVELL INDIA

Novell was established in 1843, in Great Britain, by Alexander and Daniel Novell. Over the years, the group has grown into one of the leading publishing houses of the world with presence in over seventy countries. Today, the Novell group is owned by Verlagsgruppe George von Holtzbrinck GmbH, a large Germany-based media company with interests in publishing, information technology and Internet service providing. **Novell India Ltd** was established in 1893 and became a corporate entity on January 19, 1970 and today it has extended its activities in the areas of Publishing, Information Processing and e-business. twenty-two showrooms and branches across major cities in India and sales offices in London and New York with its Corporate office in Bangalore and the National Editorial situated in New Delhi.

Activities: Novell India's Information Processing Division is world-renowned for its typesetting and originating services. The company has two main units, one each in Bangalore and in Chennai. The main unit in Bangalore is one of the largest scientific and mathematical typesetting units in the world, employing the most advanced software and hardware. The present output of pages is around 400,000 pages a year and that of scanning is around a thousand lines and halftone illustrations per day. **Novell India** has always assimilated the best of both traditional ideals and time-tested values with the latest technical knowledge and state-of-the-art developments. The e-business division, ***eNovell,*** was established as the company's foray into the world of the Internet - the impact and reach of which is unparalleled. ***eNovell*** is yet another step towards furthering the company's commitment towards excellence in the field of education. ***eNovell*** has undertaken ambitious educational ventures on the Internet, including online transactions, besides being a software-sourcing center.

Services:

Novell India develops and provides services in the domain of software and specialized services in varied vertical domains in publishing and also in the other domain areas like Health Care, Banking and Finance. E-Novell Software Services has a comprehensive knowledgeable base thus provides the necessary process orientation and competitive advantage for managing operations of leading international organizations. Some of its **Outsourced Application Services** include Custom Solution Development, System Maintenance, System Re-engineering, and Testing and Validation. Its **Enterprise Services** include Business Intelligence and Data Warehousing, Enterprise Content Management, Infrastructure Management, Business Continuity, and Vista Services. Brief not in these services is illustrated below.

Its Custom solutions enable enterprises gain competitive advantage by better aligning their IT /application portfolio with their unique business processes. Custom solutions help to address the gaps in existing functionality being provided by packaged solutions (COTS) and in tackling business processes for which no solutions are currently available. While eNovell's Global Delivery Model, combined with technology and domain expertise and its value proposition, is distinctly placed to help enterprises attain maximum value from custom development engagements. It also offer experts who can help you elicit and outline system requirements from different user groups to ensure an effective solution while minimizing TCO. The key features of its approach in providing solutions are due its: Proven methodologies, Systematic requirements management, Custom tools to enhance development effectiveness, Process and software frameworks, and Rigorous project and account management. Maintenance of any system is another area where the company extends it expert service. With enterprises spending upwards of 60% of their IT budgets on application and system maintenance, it is critical for organizational success that IT becomes more efficient and effective while continuing to provide the competitive edge. This service is provided at three levels viz: Corrective, Adaptive, and Preventive.

Other services include Business Intelligence and Data Warehousing that addresses to create optimally designed DW to provide comprehensive and qualitative information and focus providing business results oriented solutions by optimally mapping our deep understanding of the business domain with technology. Our teams fully exploit best practices prevalent in the industry and reduce TCO by delivering the service through our Global Delivery Model. It includes Designing Enterprise Data Warehouses / Data Marts, Data migration – ETL and Database integration, Data Cleansing, Business Intelligence and Data Mining, Decision Support and Reporting. The **Enterprise Content Management is another area that addresses the management of** enormous amounts of content in rich and varied forms generated in the organization by focusing on Create/Capture, Manage, Deliver / Disseminate and Archive /Dispose Content.

The **Infrastructure Management service ensure** maximize ROI on infrastructure by 24x7 availability, Employing existing infrastructure for delivering optimum ROI while minimizing TCO, meeting reliability and security requirements, and Tool-based infrastructure monitoring thereby reducing human error and oversight. eNovell's Business Continuity services ensure that IT systems are disaster-proof, and provide enterprise with a high degree of business continuity in the form of High Availability, fail over analysis of systems (backup and recovery of applications, servers, and network infrastructure),Recovery strategy development and implementation, Disaster Recovery, Disaster Recovery Planning and Disaster Recovery Operation. Lastly the Vista Services address the need to implement a homogeneous and consistent end-to-end solution without compromising quality and security. VCG's offerings includes Program and Application maintenance services for various Vista systems such as: Order Processing, Backorder System, Discount Matrix , Financial System, Invoicing, ,Inventory Management, Shipping, Mass compilations, DayEnd, X3-X5, and ISBN 13.

Offshore Activities: An offshore development centre with eNovell Software Services offers the following advantages like Infrastructure, Project Management Techniques, Skill Sets, Quality Processes, Value Proposition, Cost Effectiveness, 24 Hours Facility And Robust Process, Interactive Multimedia (Animation Development , Interactive Games Development, Interactive e-Learning Content , Video Conversion Services, Storyboard Development, and Website Development etc., Apart from this also provides Hosting and Technical Support through FALCON.

New venture: Novell India, a leader in education for over a hundred years, offers online courses on business management and design in collaboration with some of the leading professional learning institutes of India. Its online training programs provide certification from the professional institutes like Indian Institute of Management, Calcutta, and Novell India Ltd have collaborated to provide learning opportunities on the Internet to professionals. The courses are designed considering the challenges faced by professionals in the changing modern economic environment. Online Executive Development Programmes that are easily accessible and offer

the flexibility of time and ease of learning have been a long-felt need of working executives. Indian Institute of Technology, Delhi and Novell India Ltd have collaborated to provide online courses to executives on the Internet. Management Development Institute, Gurgaon and Novell India Ltd have collaborated to provide learning opportunities to executives, on the Internet. The objective of these courses is to widen the horizon of knowledge and skills of the participants to enable them to understand business processes in a holistic way and to prepare them for larger responsibilities.

Security system at novel: In order to secure the NOVEL's information generated and used both internally and externally for various purposes, it has signed up for three security measures and that include firewall, antivirus, and Intrusion Detection Service. The concept of security today is evolving into many folds because of its complexity and also due to the involvement of people both internal and external. In this context the security issue also needs to be considered with external and internal perspective both physical and digital form. This must begin with identifying the responsibilities and build accountability among the employees and stakeholders at all levels. An analysis of business process and the kind of people involved in performing that process enables to identify the check points required in developing, designing and implementing the security system for the organization. Alignment of business process and security requirement defines the security model and one must understand that no model can be simulated in another organization as the process differs in the way they are performed. The security analysis process would involve Vulnerability assessment, Threat identification, and Impact assessment.

While we know the benefits and constraints of the present security tools implemented at Novell India Ltd, one would feel that there is gap in the security system which is visible with the kind of business Novell is into and it's also due to its global presence. The present system for example IDS would help them to have a log view on all the web site visited which is only internal to the company and content filtering, Antivirus to block bandwidth chocking or full maximum utilization of bandwidth, and firewall to prevent the external intrusion into the server and protect the customer data. However, may not provide a framework to the security management process to handle in terns of vulnerability assessment, threat identification and its impact assessment in the light of its activities, services and new venture.

What needs to be done: In order to facilitate full fledged security system for NOVELL we feel that unless it develops a comprehensive security policy [10] would not be able to develop security system that would address all possible vulnerabilities and threats. Security policy [10] needs to be developed based on the business policy, strategy and services that Novell extends to its clients. We would suggest the following additional security tools/systems to Novell.

1. **Biometrics device:** for desktop systems and also it would be better solution for the new venture where it provides online education programs. Here it may help to authenticate a user in case the registered user may give his ID and Password to some one known.
2. **RSA Token/Secure ID:** To have security where the system extends multiple login and enables the system to identify the authorized user and establish accountability for authorized user. It mitigates the two major risks of e-learning such as identity fraud by outsiders and hard to detect misdeeds by insiders. It will also enable its clients to feel and ensure reliability in its services.
3. **VPN:** Since E business needs validation of user identity and to achieve this, the enterprise must routinely expose its high value applications and data to diverse users both internal and external. Unless reliable authentication, it may not be possible to make the source available to its clients with out any vulnerability to fraud, theft and malicious activities. Here VPN comes as an alternative. It also ensures the safety in the process when an user uses mobile devices such as laptop, PDA etc.,
4. In future Novell as well can think of venturing into the implementation of retina scanning and go for security certification.

6. CONCLUSION

We have proposed a single model and process for combined analysis and understanding the information security [14]. The focus is on designing a security system structure in tackling security challenges in an organization. In the case study analyzed here it was clear that unless there is a comprehensive security policy would not be able to develop and implement a security system in an organization to address all possible security threats. Based on the organization culture, strategy, business policy, types of the customers the security system can be devised and implemented.

7. REFERENCES

[1]. D. Bell and L. LaPadula. Secure computer system: Unified exposition and multics interpretation. Technical Report MTR-2997, MITRE Corp., Bedford, MA, July 1976. Available from World Wide Web: http://csrc.nist.gov/publications/history/bell76.pdf.

[2] M. Blaze. "Cryptology and Physical Security: Rights Amplification in Master-Keyed Mechanical Locks." March 2003. *IEEE Security and Privacy*. March/April 2003

[3] M. Blaze, J. Ioannidis, A. Keromytis. "DSA and RSA Key and Signature Encoding for the KeyNote Trust Management System." *RFC-2792*. IETF, March 2000

[4] M. Blaze. "Toward a broader view of security protocols." *12th Cambridge International Workshop on Security Protocols*. Cambridge, UK. April 2004

[5]. Briney, A & Prince, F (2002), Does sixe Matter? Information security, September, 36-39.

[6]. Brown, C, V., & Bostrom, R.P (1994) Organization designs for the management of end-user computing: Reexamining the contingences Journal of Management Information Systems, 10(4), 183.

[7].CAMERO, KIM what is a digital Identity? 2005.http://www.identityblog.com/2005/03/07.html#a152.

[8] E. Cronin, M. Sherr, and M. Blaze. "The Eavedsdropper's Dilemma." Technical Report MS-CIS-05-24. University of Pennsylvania. 2005

[9]. Cullery A, (2003), Computer forensics: past present and future, Information security Technical report, vol 8 nr 2, p32-35, Elsevier.

[10]. ELOFF JHP. (2002a). what does an international standard say on information security policies? IT security workshop.

[11] M. Sherr, E. Cronin, S. Clark and M. Blaze. "Signaling Vulnerabilities in Wiretapping Systems." *IEEE Security and Privacy*. November/December 2005

[12]. SINANGIN D, (2002), Computer forensics investigation in a corporate environment, Computer Fraud and Security Bulletin, 8, p.11-14, June 2002.

[13]. VON SOLMS SH. (2001a). Information security A multidimensional discipline, Computers and security, volume 19, number 7, Elsevier.

[14]. WHITMAN, MATFORD H, (2003), Principles of Information Security. Thompson Publishing

AUTHORS PROFILE

Dr. V. Vaithiynathan is a Professor in the Department of Computer Science and Engineering at SASTRA University Tanjavur India.

Prof. Rathnakar Acharya Graduate in Electrical an Electronic Engg, from Mysore University and Post Graduate in Technology and Management. Having 18 years, of experience in teaching/ research. Presently perusing research (PhD) in QoS issues in WLAN.

Dr. Pethur Raj Chelliah, PhD from Anna University, India, worked as a research associate at the Dept. of Computer Science and Automation at IISc. Bangalore and then Postdoctoral research at Japan (Nagaya Institute of Technology Kyoto University and University of Tsukuba) currently working as Lead Architect at Robert Bosch Bangalore.