Chapter 2
Other computerised applications in Indian Railways

2.1 IT Security on Western Railway

2.1.1 Highlights

Even 20 years after implementation of computerised applications in Western Railway, IT security policy was not laid down. Both the physical and logical access controls were inadequate exposing the systems to unauthorised access and malicious software. Western Railway Administration did not conduct any threat based risk assessment for systems and data. An independent vulnerability assessment by Audit using the tool NS Auditor revealed as many as 274 vulnerabilities, out of which 197 were of high risk.

(Para Nos. 2.1.6.1 and 2.1.6.3)

Network security was inadequate as open ports were found in personal computers in Western Railway rendering the systems vulnerable to viruses and worms and intrusion by hackers. There was no mechanism to monitor and control internet usage of users.

(Para No.2.1.6.2)

Physical and information assets in Western Railway were not classified and there was no mechanism to designate ownership of critical information raising questions on safeguarding of assets and classified information. Training in IT security was inadequate and internal audit of IT assets, application and its security were not conducted.

(Para Nos.2.1.6.4, 2.1.6.6 and 2.1.6.7)

2.1.2 Recommendations

- Western Railway Administration should develop a proper IT security policy and assess the risks and vulnerabilities on priority basis.
- Western Railway Administration should continuously monitor the network traffic and system usage and institute adequate security controls- both physical and logical to safeguard IT assets, systems and data from external and internal threats.
- Internal audit of IT systems should be conducted. IS security training should be adequately imparted. Physical and information assets should be classified based on their sensitivity.

2.1.3 Introduction

IT Security encompasses understanding and management of risks involved, managing the network traffic and security, safeguarding IT assets, data, applications, infrastructure and personnel, selecting and implementing effective controls to ensure confidentiality, integrity and availability of the information and communication systems that store, process and transmit data. Dramatic increase in reported computer security incidents, ease of obtaining

and using hacking tools, steady advance in sophistication and effectiveness of attack technology and the dire warnings of new and more destructive cyber attacks etc., could affect the Railway's computer system.

2.1.4 Audit objective

The audit of IT security of the computerised applications in Western Railway was carried out with a view to assessing whether adequate and effective information security controls were implemented to protect confidentiality, integrity and availability of the systems and data.

2.1.5 Audit scope, criteria and methodology

IT Security audit was confined to assessing the security program management, which provides a framework for understanding the associated risks and instituting effective controls for mitigating the risks, network security management, access and change management controls.

Standard Information Security practices were used as audit criteria to evaluate the IT Security in Western Railway.

Relevant records, reports and documents relating to IT assets were analysed. Network security was analysed using network security scanner. A questionnaire was used to obtain information with regard to IS Security policy and other aspects apart from discussion with the users.

2.1.6 Audit findings

The IT Security audit of computerised applications in Western Railway disclosed inadequacies in IT Security, network security and traffic management, lack of risk assessment, non-classification of IT assets and information, inadequate change management and training, absence of internal audit of IT systems and inadequate management of business continuity process as brought out below:

2.1.6.1 Inadequate IT Security

A proper policy framework for IT security embodies adherence to strict norms and procedures in the system for ensuring confidentiality, integrity and availability of reliable and authentic information. Moreover, critical or sensitive business information processing facilities should be housed in secured areas, protected by defined perimeter security with appropriate security barriers and entry controls. Precautions are also required to prevent and detect malicious software since both the software and information processing facilities are vulnerable to introduction of malicious software, such as computer viruses, network worms, Trojan horses and logic bombs. Audit observed that:

- Even after 20 years of implementation of computerised applications in Western Railway, IT security policy was not laid down by the Railway Administration. Absence of laid down security policy result in ineffective segregation of responsibility, absence of established performance centres and demarcated areas of operation.

- Physical security control weaknesses such as inadequate physical barriers and ineffective screening of visitors contributed to weakening the perimeter security at several facilities of the department exposing sensitive computer resources and data to unauthorised access.
- There was no mechanism to guard against internal threats (an action or event initiated by an employee or staff having valid access to information as part of performing his or her duties) to information security. In response to an audit questionnaire one (EDP centre) out of the seven departments stated that there was no loss caused by insider threats. A test check, however, disclosed that a temporary employee had misused the Passenger Reservation System (PRS) facility by issuing reserved tickets to passengers against seats already allotted to other passengers, which was discovered in the train when there were ten passengers for five seats.
- Inadequate logical access controls reduced the reliability of department's computerised data and increased the risk of unauthorised disclosure and modification. It was seen that IP addresses were misused by staff to access the internet network. A test check further disclosed that five out of twelve PC's connected to Railnet could be opened using the administrator's account without a password.
- Personal computers installed in various departments did not have the latest antivirus definition files nor were the staff aware of antivirus definition files to be downloaded through the internet. Railway Administration accepted that personal computers connected to Railnet were affected by virus.
- There was no filtering mechanism to restrict users from downloading malicious content on computers. This coupled with poor physical controls exposed the system to malicious software and rendered the system vulnerable to frequent break downs.

2.1.6.2 Inadequate network management

Network management includes management of network security and traffic. Network security management encompasses deployment, maintenance and monitoring of the effectiveness of network security controls to safeguard information and information systems and protect supporting network infrastructure. Effective network security management practices also require established and documented procedures that provide instructions for the system to restart and recover in the event of system failure in a short time. Further, to manage network traffic effectively network devices have to be configured correctly. Audit observed inadequacies in the network security and traffic management as brought out below:

- In a test check conducted on 12 January 2007 using GFI LANGUARD Network security scanner and on 08 June 2007 using Network Security Auditor (NS Auditor), it was noticed that ten ports were open in the personal computers connected to Railnet, exposing the users of the system to risks as mentioned below apart from penetration of viruses and worms in servers and personal computers and other intrusion by hackers.

Type of risk	Impact
Denial of Service on Port 135	The usage of Central Processing Unit (CPU) could be raised up to 100% by telneting to port 135 and irrelevant data/characters could be input.
OOB denial of Service	An attacker can send a custom packet causing the system to stop responding.
Teardrop denial of service	An attacker can send a custom UDP packet causing the system to stop responding.
Land denial of service	An attacker can send a custom packet causing the system to stop responding. The source code written in 'C' language is also available on the internet.

- Railway administration did not have a mechanism (either by installation of hardware or software) to monitor and control internet usage of users. On scrutiny of files, Audit noticed that some users of Railnet in Western Railway had downloaded and uploaded voluminous data (of 5.3 GB and 3.3 GB respectively) resulting in wastage of time besides denial of Internet service to other genuine users.

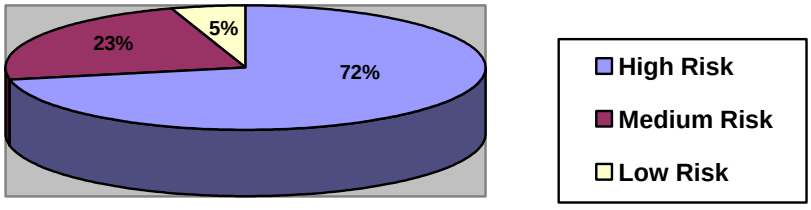
Railway Administration stated that there was no system to monitor the pattern of usage by individual users and as a result cyber slacking[1] could go uncontrolled.

2.1.6.3 Lack of risk assessment

Risk assessment is essential for risk management and overall security programme. This assists in identification of security risks and institution of effective controls. Audit observed that:

- Railway Administration has not performed any threat based risk assessment for systems and data. An independent vulnerability assessment by Audit in 3com switch (Host IP 10.3.3.103) using the tool NS Auditor revealed as many as 274 vulnerabilities, out of which 197 were of high risk (for e.g. Cross-site scripting, Avenger's News system command Execution, Directory transversal vulnerability, Remote command execution, Web_store and cgi etc) 63 were of medium risk and 14 were of low risk. Railway Administration accepted that automated tools were not identified to scan and monitor the network and host devices.

[1] practice of emloyees using the Internet or other employer-provided resources for leisure during work hours, contributing to inefficiency



2.1.6.4 Absence of classification of IT assets and information

Physical and information assets should be classified to indicate the need, priorities and to provide proper degree of protection. Information and physical assets have varying degrees of sensitivity and criticality. As per the IT Security standards, the information may be classified as unclassified, operational use only, private, restricted and confidential. Audit observed that:

- There is no centralised inventory of critical information and systems maintained by the Railway administration. Test check of the Stores & Signal &Telecommunication department revealed that inventory database was also not maintained department wise. In these circumstances, the Railway administration may not be in a position to do proper asset classification of the system based on the importance and sensitivity of the system/data in use, indicating lack of effective control.
- In spite of incurring expenditure of the order of Rs.32.06 crore during the last three years on acquisition of IT assets, the assets were neither classified nor was there a mechanism to designate ownership of critical information raising questions on safeguarding of assets and classified information.

2.1.6.5 Inadequate change management

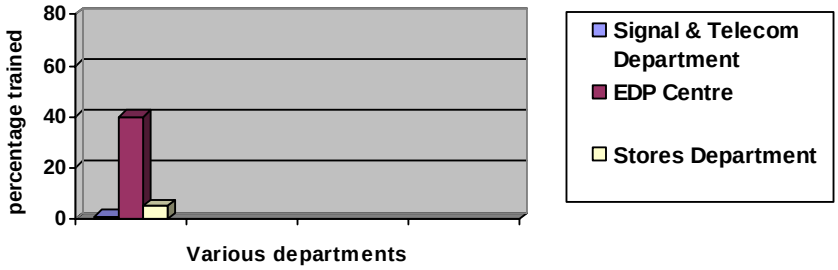
Established change management practices/ procedures are required to ensure that unauthorised changes are not carried out to the system. This should ensure only approved changes are incorporated in the programme and in time. Audit observed that:

- Changes in the system necessitated due to change in introduction of rules were not carried out in a timely fashion resulting in inconvenience to the traveling public as well as increasing the risk of loss of revenue to the Railways. For instance pursuant to Government of India notification of March 2006 regarding introduction of service tax on catering services on board the trains of Indian Railways, service tax for catering service on Rajdhani/ Shatabdi trains was not updated immediately in the fare structure resulting in short recovery of Rs.0.42 crore for the period from 1 April 2006 to 31 May 2006. Railway Administration stated that this has since (June 2006) been introduced after obtaining necessary instructions from Railway Board.
- No records were maintained to indicate the requests for change and the changes carried out in the system.

2.1.6.6 Inadequate training

An effective security awareness program is the means through which the organisation communicates the importance of security policies, procedures and responsibilities to its employees. Audit observed that:

- Out of three departments (Signal &Telecommunication, EDP centre and Stores), training in IT security awareness was imparted only in the EDP centre. Even in the EDP Centre, only 10 out of 25 employees were trained in security awareness. In the other two departments only basic training (use of Login & password) was imparted, which was inadequate.



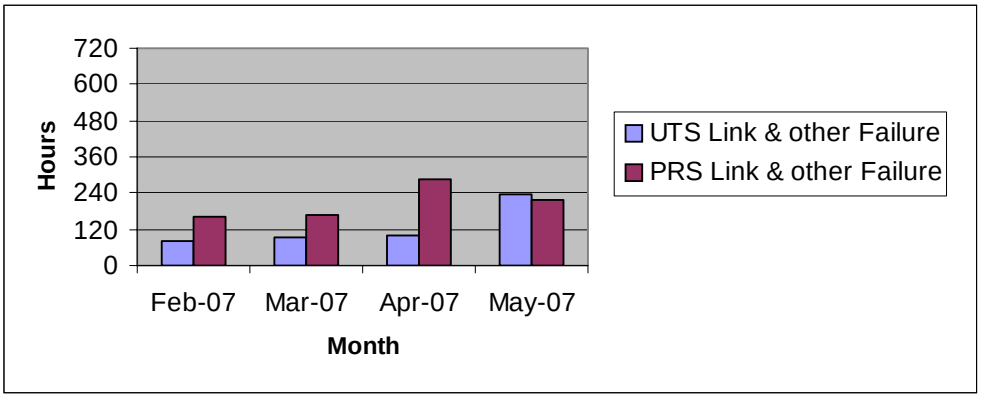
2.1.6.7 Absence of internal audit of IT systems

Internal audit assists in providing an assurance that safeguards are adequate and in alerting the administration to potential problems and threats. Audit noticed that Railway Administration has not covered internal audit of IT assets, application and its security in the annual inspection programme and hence internal audit of IT assets, application and its security has not been done so far.

2.1.6.8 Inadequate management of business continuity process

A business continuity management process should be implemented to reduce the disruption caused by disasters and security failures to an acceptable level through a combination of preventive and recovery controls. The business continuity plan should be tested regularly to ensure that they are updated and periodically reviewed for their continuing effectiveness. Audit observed that:

- There was no managed process for developing and maintaining business continuity throughout the organization, regular testing and updating of the plan, formulating and documenting a business continuity strategy etc.
- Link failures in UTS and PRS were not addressed on time resulting in disruption of service. A test check in audit of link failure for a period of four months at major locations revealed that link failures ranged from 10 minutes to 54 hours (minimum at Vapi station and maximum at Vasai station) in UTS and from 10 minutes to 20 hours and 30 minutes (minimum at Malad station and maximum at Okha station) in PRS respectively. The link showed an increasing trend, reflecting that there was no appropriate contingency plan to minimise the impact of this failure.



2.1.7 Conclusion

The IT security of the computerised applications in Western Railway was grossly inadequate. Neither a comprehensive IT security policy was developed nor were the risks and vulnerabilities assessed. The network security and network traffic was not effectively monitored, information security and access controls were inadequate to protect the confidentiality, integrity and availability of the systems and data thereby exposing the IT systems to both external and internal threats.

~~2.2 Provident Fund Accounting System in Izatnagar Division of North Eastern Railway~~

~~2.2.1 Highlights~~

~~Business rules relating to accounting of Provident Fund transactions were not fully incorporated in the Provident Fund Accounting System in Izatnagar Division of North Eastern Railway leading to incorrect processing of transactions.~~

~~(Para No.2.2.6.1)~~

~~The Provident Fund Accounting System was not functioning concurrently with the Pay Roll System and therefore up to date balances of subscribers' PF accounts were not available.~~

~~(Para No.2.2.6.2)~~

~~Validation controls were deficient, which adversely affected the reliability of data. IT Security policy was not framed and weak access control mechanisms coupled with absence of audit trail rendered the Provident Fund Accounting System vulnerable to manipulation.~~

~~(Para Nos.2.2.6.3 and 2.2.6.4)~~