Framework Based Approach for the Mitigation of Insider Threats in E-governance IT Infrastructure

M Hari Haran

Scientist-SB, National Informatics Centre,
Ministry of Communications & IT, Government of India, Gujarat State Centre, India

Abstract: ***E-governance has made massive inroads in the way the government delivers services to its citizens. To enhance and empower this electronic service delivery mechanism, the government of India established a strong IT Infrastructure at the state level to deliver the e-governance services. This e-governance IT Infrastructure comprises the following 3 core components: State Data Centre (SDC), State Wide Area Network (SWAN) and the Common Service Centre's (CSC). The state governments have taken forward the mandate of delivering the e-governance services to the stakeholders through these cores IT Infrastructure components. Any IT Infrastructure environment is exposed to a certain degree of threats and vulnerabilities propagating from different sources in different forms. This paper focuses on one particular threat to the e-governance IT Infrastructure i.e., The Insider Threat. This paper identifies key stakeholders who are the probable Insiders from an e-governance IT Infrastructure perspective and outlines the various threats and vulnerabilities that might arise out due to the activities of the Insider and finally, proposes a robust framework mechanism for early detection and mitigation of such Insider threats.***

Keywords: e-governance, IT Infrastructure, Cyber Security, Insider Threats.

1. Introduction

The e-governance IT Infrastructure has grown in leaps and bounds in the past decade. With the massive impetus from DeitY (Department of Electronics and Information Technology) under the NeGP (National e-Governance Plan) , the states were provided with adequate funding from the central government for establishing the e-governance IT Infrastructure. With the IT Infrastructure in place, the drive for converting all manual processes to electronic form was undertaken and over 31 key projects were identified as a Mission Mode Projects (MMP) [1]. At the state level the IT Infrastructure comprises the following 3 core components [2]:

a) State Data Centre (SDC)
b) State Wide Area Network (SWAN)
c) Common Service Centre (CSC)

Figure 1: E-governance Core IT Infrastructure

These 3 Core IT Infrastructure components together makes the backbone of nearly 60% of the total e-governance IT Infrastructure of the nation. The remaining 40% constitutes the National Knowledge Network (NKN), National Data Centers (NDC) and National Informatics Centre Network (NICNET), which are maintained and operated at the central level by central government agencies like National Informatics Centre [3].

The data centers (i.e., both State Data Centre and National Data Centre) are the central repository for storing the data & hosting Networks (i.e., SWAN & NKN), are the medium or connectivity which connects the Data Centers and the end-users (both within government and outside i.e., Internet). The CSCs are the centers which are established at the district level and taluka level for providing the e-governance services to the citizens. So to sum it up, the e-governance services hosted in the data centers are delivered to the end-users through CSCs, whereas, the SWAN/NKN, is the medium of connectivity between the data centre and the CSC/other government offices.

With almost every government department having some sort of online presence, their digital data stored in SDCs and delivered through SWAN/NKN, the cyber security threats pertaining to these data and services are manifold and are posing a daunting challenge to the government to safeguard its data and assets from these cyber security threats. The cyber security threats can be generally classified into:

a) Internal Threats
b) External Threats

External threats are those threats which originate from outside the government sector and are generally caused due to hackers operating from outside the government networks. Whereas, Internal Threats are those threats which originate from within the governments caused by its own employees/contractors/third parties, who are working for the government. The external cyber security threats can be detected and mitigated to a certain extent. But the threats caused by the Insiders, are the most complex and cumbersome to detect and mitigate. Moreover, the insider

threats can completely devastate the entire government machinery, due to the sheer knowledge and resources available at the disposition of these Insiders. A recent case in point would be the revealing of NSA (National Security Agency) Secret files by a former contract employee Mr. Edward Snowden [4]. The massive troves of classified documents released by Mr.Snowden into the public domain have caused a huge damage and embarrassment for NSA and the US Government as a whole. The damage caused was not so huge that, the NSA was still not able to ascertain the actual amount of confidential data that Mr. Snowden might have compromised, nor were they able to ascertain the financial loss incurred due to the damage. The case of Mr. Edward Snowden was an eye opener, for Governments and other organizations world-wide, to give a serious consideration for Insider Threats.

2. The Key Stakeholders and Insiders

From an e-governance IT Infrastructure perspective at the state level, the various stakeholders or Insiders, who are privy to confidential information, related to the IT Infrastructure and services can be classified as follows:

1. Government Employees / Management Team
2. Data Centre Operator (DCO)
3. SWAN Operator (SWO)
4. CSC Operator (CSCO)
5. Third Party Auditors (TPA)
6. Consultants
7. Vendors / OEMs
8. Third Party Contractors

The above mentioned list of Insiders covers most of the key personnel who are privy to different levels of confidential information related to e-governance IT Infrastructure. The Governments both at the centre and the states have given adequate attention for IT Infrastructure & data protection against the external cyber security threats, through the Firewalls, Intrusion Prevention Systems, Anti-Virus…etc. But only, little or no attention has been given to the Cyber Security threats caused by Insider. In most cases due to their proximity and nature of job functions, Government usually tends to overlook the threats pertaining from Insiders.

3. Insider Threat Mitigation Framework

This proposed framework provides a mechanism for detecting and mitigating the Insider threats at an early stage. Thereby, providing the government an opportunity to prevent such threats and build a safe and secure e-governance ecosystem.

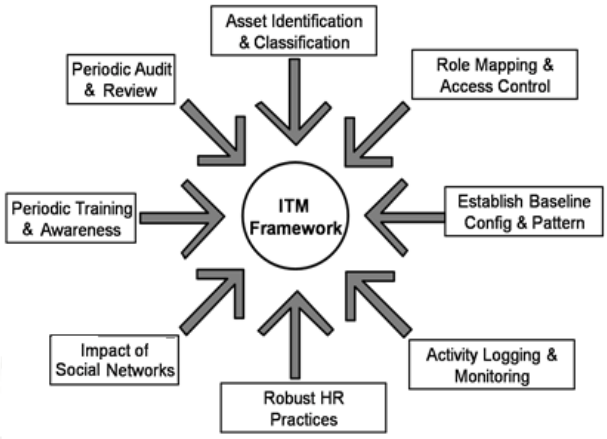

Figure 2: Insider Threat Mitigation Framework

3.1 Asset Identification and Classification

The first step of this framework is to identify and categorize the list of assets (IT assets, documents, Information, Human resources, facilities & other sensitive physical assets). The identification & categorization of the assets is such a humongous task that requires a lot of effort & time from the state governments. Each of the identified assets should carry a asset confidentiality & risk ratings. The Assets list should include State Data centers, State Wide Area Networks, IT Equipments & Personal Computers/Laptops at the individual Department level. Initially, the state governments can start with IT Assets and in due course of time the scope can be expanded to Human Resource Assets & Document assets. Since the asset list is bound to run into several thousands of asset names, it would be better if automated asset management software is used, else it would be practically difficult to list & track thousands of asset in a single spreadsheet. A sample Asset list is given below for the reference, however the state governments can customize it further to suit their requirements.

Table 1: Asset ID & Classification Matrix

S. No	*Asset Name*	*Asset ID*	*Owner (with contact details)*	*Current Status*	*Asset Location*	*C*	*I*	*A*	*Asset Operator (with contact detals)*	*Asset Usage Purpose*	*Asset Installation Date*	*Warranty Exiration Date*	*Maintenance & Support Contact*	*Risk for the Asset*
1	Web servers	State-SDC-WBSR-01	State Govern-ment	Active	Rack K1, bay2-SDC Gandhi Nagar	3	3	3	IT Dept Employee Name Phone No. & E-Mail	For hosting Govt. websites	1/12/2013	31-11-2017	Vendor Name, e-mail & Ph. No.	High Risk

Legend:
C- Confidentiality Rating; I- Integrity Rating; A-Availability Rating; CIA ratings are on a scale of 3 (with 1=low, 2 =medium & 3=High).
The Asset ID Naming convention can be with State Name-location-equipment type-number. For ex: GJ-SDC-WBSR-01 for an asset belonging to Govt. of Gujarat, located in Gujarat SDC & The type of asset is Webserver

3.2 Role Mapping and Access Control

Once the list of assets is identified and classified, next the State Governments can start with the role mapping & access

control. This process will ensure on, who will have, what kind of access to which resources. Role mapping should consider the list of Government personnel & vendors and other third parties. Based on their job functions and business requirements of the Government, the access levels for each individual should be mapped to particular devices, as per their roles & responsibilities. The following Role based Access Matrix can be used for mapping the access levels for each individuals & assets. This role based access matrix should be reviewed at least 2 twice a year to ensure that the access granted is properly used by each individual and in case of any misuse of access, the privileges shall be revoked and appropriate disciplinary action can be initiated depending on the nature & kind of misuse.

Table 2: Role based Access Control Matrix

S. No	*Individual Name*	*Department & Designation*	*Job Function*	*Access Allowed*			*Type of Access*	*Purpose of Access*	*Access Authorized by*	*Access Granted on*	*Access Valid till*	*Remarks*
				Asset Name	Asset ID	Asset Location						
1	Hari Harann	IT Department Scientist	Data Centre Management	Web Server	GJ-SDC-WBSR-001	SDC, Gandhi Nagar	Read & Write Access	Website Updation	IT Dept. Head	1/12/2013	30-11-2014	
				Application Server	GJ-SDC-APLN-	SDC, Gandhi Nagar	Read only Access	Application Monitoring				

3.3 Establish Baseline Configuration and Pattern

Establishing the baseline configuration & pattern for the IT environment and individual behavior, is one of the most crucial aspects of the Insider Threats Mitigation process. As this baseline, would provide a reference threshold parameter which would be used for identifying any possible threats arising due to the Insider activities. To establish a baseline configuration, first a "Standard Operating Procedure" (SOP) manual has to be designed for operating all IT equipments owned by the government. The SOPs should cover everything right from servers, applications, databases, network equipments, up to the individual Desktop PCs and Laptops, which are used by various individuals to access the government IT Infrastructure and Services. The SOPs should take into account the industry standard hardening practices and also incorporate the policies of the government.

It would be better, if the states use an access control tool or active directory or an LDAP (Light Weight Directory Access Protocol) tool, to restrict access and enforce policies from a single server to all clients connected in the network. This will eliminate the need of individual end-users to change the configuration of their systems, every time, whenever there's a policy change. Once an SOP is defined and implemented in the IT environment with all the access controls in place. The next step is to observe and develop the usage pattern.

The Usage pattern involves, observing the normal daily bandwidth consumption of all users & IT equipments in the IT Infrastructure environment. Also, the event log analysis can also be done to identify the most common occurrences of events in each server or applications or databases or PCs…etc, this pattern can be observed over a period of six months to a year, at least. Then based on the observed data an approximation is done to arrive at an average threshold value. While arriving at a threshold value, many environmental factors have to be considered to eliminate any factual error. For example, the normal working hours of a government office will be morning 9:00 AM to evening 6:00 PM, so the IT Utilization and bandwidth consumption will be at higher levels during this time, whereas, during the remaining time period, i.e., from evening 6:00 PM to 9:00AM the next day, the total IT utilization will be very less, maybe in single digits. So these kind of anomalies have to be factored into while arriving at an approximation. These approximated threshold parameters should be revised periodically in tandem with the changes in the IT environment. Once the threshold parameters are finalized these can be configured in an enterprise management tool to raise alarms, as and when the threshold limit is violated. Also daily, monthly quarterly, half-yearly & yearly reports may be generated to measure the compliance levels and violations, with respect to the threshold parameters.

Table 3: Baseline Configuration Threshold Matrix

S. No	*Asset Name*	*Asset ID*	*Asset Location*	*Avg Daily Band Width Usage (A)*	*Avg CPU Utilization per day (B)*	*Avg Memory Utilization pr day (c)*	*Average no. of hints per day (D)*	*Avg No. of admin login per day (E)*	*Most No. of unique hits from a single IP per day (F)*	*Avg No of Event log errors & warnings per day (G)*
1	Webservers	GJ-SDC-WBSR-001	SDC, Gandhi Nagar	18 GB	54%	79%	3 Lakh	8	684	394

3.4 Activity Logging and Monitoring

Activity Monitoring & Logging is another crucial component of this Insider Threats Mitigation framework. All the IT devices & Software's (i.e., Servers, Network devices, Security Devices, Desktops, laptops, Applications, Websites, Databases, Operating System…etc) should be configured to record all logs and the logs can be stored in a centralized "Log Server", the analysis of these logs can be done through professional Log Analyzer Tools. Correlation of the

collected logs will provide more insights into the overall picture of the various activities happening in the IT Environment. This correlation or data analytics will also help us to pre-empt many potential security breaches, by proactively detecting and alerting us on various suspicious patterns of traffic/log events. All the state government's SDCs & SWANs will be equipped with Firewalls, Intrusion Prevention Systems, Antivirus…etc., and all these devices may generate Gigabytes of logs every day. But, the absence of a proper log analysis poses a huge security threat to the entire Government IT Infrastructure. It may be possible, that several security breaches are happening on a daily basis in the Government IT Infrastructure and the same is recorded / reflected through the logs, but due to the absence of the log analysis, these security breaches may go un-noticed. Hence, Log Analysis should be accorded prime importance by all state governments.

Let's consider an example of a hacking incident where, a hacker hacks into a server and transfers Gigabytes of data from the Government servers to his personal computer/laptop…etc. So how do we detect this incident through Log Analysis?

1) First when the hacker enters into your network his Source IP Address will be logged in the Firewall & his request packet will be scanned by the Intrusion Prevention System, both at the perimeter security level of the data centre. A hacker usually does a recce or reconnaissance of the IT Infrastructure, to identify basic information of the existing IT Setup and find out possible weak points. *Port Scanning* is one of the most popular methods deployed by hackers to probe the network and check for open ports and then they decide on the type of attack/exploit, which needs to be deployed depending on the list of open ports.
2) Then after identifying the list of open ports and entering your network, the hacker tries to gain access to the server for taking out confidential data. For this the hacker may use any zero-day exploits, or un-patched vulnerability or a simple brute force attack for gaining the entry into the server. All these access logs will be reflected in the Operating System's Event Log and the same will be recorded in the Applications logs also (if the hacker tries to gain un-authorized access through application).
3) Once the hacker gains access to the server, then he browses the directory & file-system for confidential data and then starts transferring those confidential data to his PC/Laptop. This data transfer will be recorded in the server, firewall, IPS & other monitoring tools (if any).

In the above scenario, if one does not carry out a log analysis, then there is no way of knowing about the hacking incident, until and unless something is not in order. Usually, professional hackers leave their target system untouched, after their work is completed and they would also leave a backdoor to gain future access un-detected. If any destruction is caused by the hacker to the IT environment, like website defacement or deletion/creation of files, Denial of Service Attacks…etc., then it will be noticed by the administrator and appropriate quarantine action will be taken. But in this case, where the hacker does his job silently and leaves without a trace, it is difficult for an administrator to detect the hacking event. This is where log analysis will come in handy. When the hacker starts a port scan on the network in the step one, at that time itself, the log analysis will red flag the event and will highlight it to the administrator that someone is carrying out a port scan on the network. And further when the hacker tries to gain access to the server, all the login attempts will be logged and the log analysis will point out that someone is trying to gain unauthorized entry in to the servers. And one step further, when the hacker transfers the data from the Government server to his machine, this will again be red-flagged by the log analysis and will be highlighted as some high bandwidth activity is detected from a single external IP and also the huge chunk of data being transferred will also be found to be deviate from the existing daily pattern of bandwidth usage.

3.5 Robust HR Practices

The robustness of the HR (Human Resource) Practices should reflect in the recruitment, retainment, development and exit management of every human resource, who are involved or have privileged access to confidential data or information in the e-governance projects. Appropriate back ground verification checks have to be carried out for all personnel (both Government and non-Government) involved in e-governance projects. The work-life cycle of the individual from the time of joining the e-government project till his/her exit, from the project should be tracked and recorded appropriately. The roles and responsibilities assigned to the individual should be in line with his/her skills. Appropriate competence mapping should be carried out for the entire work-force involved in the e-governance projects and where gaps are found, the same should be addressed through training.

The individual's job satisfaction has to be measured periodically at least once in every quarter. A Threshold value of 80% can be set. If the job satisfaction levels of the individual decreases below the threshold, then Government should take appropriate measures to address the concerns of the individual and ensure that he is always on high-spirits and loyal to the Government. If an employee is not satisfied with his job, then it may lead him to resort to commit malicious/unauthorized activities, thereby leading to the compromise/damage of the confidential information & systems of the Government. The recent case of Whistleblower, Edward Snowden who revealed troves of confidential documents of US Government, is a classic example of the kind of damage which could be done by a dissatisfied employee or Insider.

3.6 Impact of Social Networks

In the rapidly expanding digital foot-print of Internet, the social networks have brought a new paradigm shift in the way through which information is shared or exchanged. The Facebook, Twitter & You Tube, are quite synonymous with the digital revolution and has a huge user base across all ages. The personnel involved in the e-governance projects should be sensitized on the diligent use of social media, and they should refrain from disclosing any sensitive information through the social media.

In recent years, the concept of "social engineering" has gained more prominence and it has proved to be quite effective in finding gullible targets in the organization. In social media, individuals are prone to disclose many personal information like name, photograph, date of birth, home town, details of family members, job details, address , current location, contact number, e-mail address….etc. The availability of all these information in public view at a centralized portal, makes it a treasure trove for Foreign Intelligence agencies and other individuals with a malicious intent to compromise the e-governance IT Infrastructure. Moreover, these malicious persons can also get a live update of the happenings in the life of the government personnel through their status updates on the social media. With all these metadata available publicly in the social media, an overall picture of the individual can be constructed, based on which they can be tricked into defecting to foreign govt/ revealing confidential government data.

Hence, the persons involved in the e-governance projects, should be discrete about their job and responsibilities in the Government sector. They should refrain from discussing anything related to their job through the social media. They should also make judicious use of the privacy features of the social media, by restricting the amount of their personal information which is accessible to the public. Government should also keep tabs of the social media activities of the personnel involved in the e-governance projects and correlate the same with their online & personal behavior and their corresponding IT System footprint in the e-governance IT Infrastructure.

3.7 Periodic Training & Awareness

Periodic Training and Awareness to all the personnel involved in the e-governance projects, plays a very vital role in the success of the Insider Threat Mitigation. Employees should be taken into confidence and they should be given a clear perspective of the objective of the Insider Threats Mitigation and what is expected from them. Employees should not feel alienated or get a big brother feeling of the Government, which will then be counter-productive.

A properly charted out training & awareness programme should educate the Government employees on the criticality and confidentiality of the Government information and the role which each employee has to play in safeguarding this information. The training content should be periodically revised, so as to keep the employees abreast of the latest technological advances and threats pertaining to the e-governance IT Infrastructure. Employees should also be encouraged to report to the concerned authorities regarding any unusual /suspicious, activities, so that appropriate pro-active action can be initiated.

3.8 Periodic Audit and Review

The effectiveness of this Insider Threats Mitigation framework can be measured through periodic Audit & Review. An Independent Audit team comprising individuals from cross-functional domains should be constituted and this team can carry out periodic / surprise audits, and review the implementation-cum-adherence levels of the personnel involved in the e-governance projects. The members of the audit team should not be a part of the operational team and the most important factor is that the audit team members should possess a very high level of integrity and should not be biased towards anyone.

A comprehensive audit framework should be worked out with at least 2 audits in a year. Once audit can be a planned audit, where the audit date & schedule are pre-decided and communicated to all stakeholders. The other audit can be a surprise audit, which can be conducted at any time, without any pre-intimation. The Audit Team should be comprised of highly capable individuals and they should be thoroughly trained on the Audit methodology and other aspects of the Insider Threats pertaining to the Government IT Infrastructure. The audit reports of each year should be compared with the previous historical reports to gauge the effectiveness and the cyber security readiness of the Government.

4. Conclusion

The Insider Threat Mitigation Framework proposed in this paper, may not be a one medicine cure all ailments for addressing the Cyber Security Threats. But, rather it is a step in the direction of establishing a self-sustaining cyber-secure & safe, government IT Infrastructure. This paper highlights the lack of adequate attention by the Governments both at the State and Centre in India, towards Insider Threats. The following are some of the cases of Insider Compromising confidential information, in the Indian Government Sector:

- The Data Entry Operator breaching into RTO (Regional Transport Office) Databases and misappropriating Government funds to the tune of 11.69 lakhs [5].
- The Data Entry Operators of the Aadhar Project of the Unique Identity Authority of India (UIDAI), offering to print Aadhar Cards for illegal immigrants (from Bangladesh, Nepal…etc) for a sum of Rs.500 to Rs.2500, per card [6].
- The Compromise of BSNL Servers by Pakistani Hackers (masquerading as Indian Army Officials) through a BSNL Employee [7].
- The navy War Room Leaks case, where retired navy Lieutenant Ravi Shankaran, compromised confidential navy secrets to M/s. Thales, for clinching the Sub-Marine Deal with Indian Navy [8].
- Confidential Documents & Future Strategy Plans of the Indian Air force leaked by Arms Dealer Abhishek Verma & his partner Edmonds Allen [9]
- Eastern Naval Command Head Quarters of the Indian Navy compromised by a Virus carried in a pen drive by an Insider. The virus, collected confidential naval information and sent it to China based IP Addresses [10].

The above list is just indicative, but not exhaustive, there are still many cases of Insider Compromising confidential Government data, but most of the cases go un-reported. It's high time that the Government at the centre and the state take cognizance of these humongous threats, posed by Insider Activity and take appropriate measures to mitigate it.

For the consequences of the data compromise of an Insider will be devastating.

References

[1] National e-Governance Plan, Mission Mode Projects, Department of Electronics & IT, 2010
[2] Subhash Chander, Sharmila, "E-Governance: Interoperability Issues," in International Journal of Research in Economics and Social Sciences, Volume 2, Issue 7, July 2012.
[3] Services offered by National Informatics Centre, Retrieved from www.nic.in/services on 24th March 2014.
[4] Michelle Van Cleave, "Myth, Paradox & the Obligations of Leadership : Edward Snowden, Bradley Manning & the next leak," in Centre for Security Policy, October 2013.
[5] "Data Entry Operators Hack NIC Security System". [Online]. Available: http://www.dailypioneer.com/state-editions/bhubaneswar/data-entry-operators-hack-nic-security-system.html. [Accessed: 24th March 2014].
[6] "Exposing the Underbelly of Aadhaar". [Online]. Available: http://cobrapost.com/index.php/news-detail?nid= 5773&cid=23. [Accessed : 24th March 2014]
[7] "Did Pakistan's ISI penetrate BSNL's Systems". [Online]. Available: http://www.livemint.com/Industry/ZoQivrvfFjfOJV74NGaW8K/Did-Pakistans-ISI-penetrate-BSNLs-systems.html. [Accessed: 24th March 2014].
[8] Rajesh Ramachandran, "Tinker, Sailor, Spy?" in Outlook Magazine, 26th December 2005.
[9] Mannu Pubby, "Express Exclusive " Airforce Projects, Plans leaked," in Indian Express, issued on 21st July 2012.
[10] "Chinese Hackers steal Indian Navy secrets with thumb drive virus". [Online]. Available: http://arstechnica.com/security/2012/07/chinese-hackers-steal-indian-navy-secrets-with-thumbdrive-virus/. [Accessed: 24th March 2014].

Author Profile

M Hari Haran received the B.E. degree in Computer Science from Anna University and MBA degree from IGNOU. He holds a certification in Cyber Laws from Indian Law Institute. He is also a certified ISO Auditor for ISO 20000 and ISO 27001. He is currently pursuing Research in Cyber Security and Cloud Computing. He is now working in National Informatics Centre, Gujarat State Centre. For over 4 years he has been involved in the Gujarat State Data Centre and has played a vital role in the commissioning and management of the Data Centre. He is also instrumental in drafting dozens of Policies related to Cyber Security and IT Infrastructure Management for Government of Gujarat. Apart from Policies, He has also published key strategy documents for Cloud Computing, IPv6 Migration, e-Governance Transformation, Cyber Law…etc, for Government of Gujarat and has provided key Technical Advisory-Consultancy to Government of Gujarat on e-governance. His areas of Interest include Cloud Computing, Cyber Security, e-Governance & Cyber Laws.

Note: All The views expressed by the Author in this paper are the author's own and does not reflect those of National Informatics Centre or Government of India, whatsoever.