eGov@Gujarat

Application Secutiry Audit

e-Governance Bulletin from Gujarat Informatics Ltd.

Vol. 6 | No. 7
March 2009

Appication Security Audit

Courtesy By

Dr. Neeta Shah
Director (eGovernance)
Gujarat Informatics Ltd.

Recently, Government of Gujarat has done Security Audit of its IWDMS & VATIS applications as per the guidelines laid down by Department of Information Technology, Government of India. Based on these experiences, Government of Gujarat has taken the conscious decision to get all its Websites Security Audited in the first phase. Government of Gujarat has consulted CERT-In empanelled Security Auditing organizations working on the guidelines formulated in consultation of DIT, GoI. At present, the IT Security Audit of all Government of Gujarat Websites is being carried out and Web Assessment reports submitted by appointed consultants are being forwarded to their respective website owners (Government Departments) for rectification of the same. Readers may be well interested to know about the "IT Security Audit"

Security Audit is an evaluation of how secure a company's information system is by measuring how well it conforms to a set of established criteria.

Security audit is a big component of the IT auditing exercise. As a stand-alone exercise it can be big enough to encompass the whole organization or be simple enough as a technical audit of critical servers. However, IT security audit is one of the most integral components of the IT auditing process and has to be taken up in a holistic perspective and its standalone exercise may not justify the audit. "Whatever the size of the exercise, IT security auditing remains a critical management aid in controlling IT risks and ensuring compliance to legislations," opines Banerjee.

Since IT is an integral part of the enterprise, IT security audit too is critical. Security audit focuses on protection of data and a whole lot of controls built around it. Data being the mainstay of the business, its security is imperative.

Security audit covers the organization's risk appetite, what controls are defined and how they are practiced in accordance to the policy. The primary goal of a security audit is to assess the effectiveness of the organization's ability to protect its information assets. This audit covers the various measures a client organization has taken to secure its systems from internal and external intrusions. The recommendations arising out of the review lead to an updated security policy.

Security auditing is the formal examination and review of actions taken by system users. This process is necessary to determine the effectiveness of existing security controls, watch for system misuse or abuse by users, verify compliance with current security policies, capture evidence of the commission of a crime (computer or non-computer related), validate that documented procedures are followed, and the detection of anomalies or intrusions. Effective auditing requires that the correct data to be recorded and that is undergoes periodic review.

A security audit is a systematic, measurable technical assessment of how the organization's security policy is employed at a specific site. Computer security auditors work with the full knowledge of the organization, at times with considerable inside information, in order to understand the resources to be audited.

Security audits do not take place in a vacuum; they are part of the on-going process of defining and maintaining effective security policies. This is not just a conference room activity. It involves everyone who uses any computer resources throughout the organization. Given the dynamic nature of computer configurations and information storage, some managers may wonder if there is truly any way to check the security ledgers. Security audits provide such a tool, a fair and measurable way to examine how secure a site really is.

Security Policy Defined

As stated, a security audit is essentially an assessment of how effectively the organization's security policy is being implemented. Of course, this assumes that the organization has a security policy in place which, unfortunately, is not always the case. Even today, it is possible to find a number of organizations where a written security policy does not exist. Security policies are a means of standardizing security practices by having them codified (in writing) and agreed to by employees who read them and sign off on them. When security practices are unwritten or informal, they may not be generally understood and practiced by all employees in the organization. Furthermore, until all employees have read and signed off on the security policy, compliance of the policy cannot

be enforced. Written security policies are not about questioning the integrity and competency of employees; rather, they ensure that everyone at every level understands how to protect company data and agrees to fulfill their obligations in order to do so.

Natural tensions frequently exist between workplace culture and security policy. Even with the best of intentions, employees often choose convenience over security. For example, users may know that they should choose difficult-to-guess passwords, but they may also want those passwords to be close at hand. So every fledgling auditor knows to check for sticky notes on the monitor and to pick up the keyboard and look under it for passwords. IT staff may know that every local administrator account should have a password; yet, in the haste to build a system, they may just bypass that step, intending to set the password later, and therefore place an insecure system on the network.
The security audit should seek to measure security policy compliance and recommend solutions to deficiencies in compliance. The policy should also be subject to scrutiny. Is it a living document, accurately reflecting how the organization protects IT assets on a daily basis? Does the policy reflect industry standards for the type of IT resources in use throughout the organization?

Security Policy Issues

Internet and Security Concepts

- **The Internet and Its Vulnerabilities**
  - When it started as a project of the Advanced Research Project of the US Defense Department in 1969, the system was designed for openness and flexibility, not security.
  - The first publicized international security incident was identified in 1986. An attempt was made to use the network to access computers in the US to copy information from them.
  - In 1988, the network had its first automated network security incident courtesy of a worm program.

- **Important Security Concepts**
  - Confidentiality of Information
    - Confidentiality is lost when someone without authority is able to read or copy information
  - Integrity of Information
    - Modifying information in unexpected ways makes it lose its integrity
  - Availability of Information
    - The erasure of information makes it unavailable when needed. Often, this is the most important attribute in service oriented businesses

At the Audit Site

When the auditors arrive at the site, their aim is to not to adversely affect business transactions during the audit. They should conduct an entry briefing where they again outline the scope of the audit and what they are going to accomplish. Any questions that site management may have should be addressed and last minute requests considered within the framework of the original audit proposal.

The auditors should be thorough and fair, applying consistent standards and procedures throughout the audit. During the audit, they will collect data about the physical security of computer assets and perform interviews of site staff. They may perform network vulnerability assessments, operating system and application security assessments, access controls assessment, and other evaluations. Throughout this process, the auditors should follow their Checklists, but also keep eyes open for unexpected problems. Here they get their noses off the checklist and start to sniff the air. They should look beyond any preconceived notions or expectations of what they should find and see what is actually there.

Conduct Outgoing Briefing

After the audit is complete, the auditors will conduct an outgoing briefing, ensuring that management is aware of any problems that need immediate correction. Questions from management are answered in a general manner so as not to create a false impression of the audit's outcome. It should be stressed that the auditors may not be in a position to provide definitive answers at this point in time. Any final answers will be provided following the final analysis of the audit results.

Back in the Office

Once back in the home office, the auditors will begin to comb their checklists and analyze data discovered through vulnerability assessment tools. There should be an initial meeting to help focus the outcome of the audit results. During this meeting, the auditors can identify problem areas and possible solutions. The audit report can be prepared in a number of formats, but auditors should keep the report simple and direct, containing concrete findings with measurable ways to correct the discovered deficiencies.
The audit report can follow a general format of executive summary, detailed findings and supporting data, such as scan reports as report appendices. When you write the report, develop executive summary first, as you may have to brief management soon after return. It's important to realize that strengths as well as deficiencies can be addressed in the executive summary to help give an overall balance to the audit report. Next, the auditors can provide detailed report based on audit checklists. The audit findings should be

organized in a simple and logical manner on one-page worksheets for each discovered problem.

Don't Keep Them Waiting

Finally, the audit staff should prepare the report as speedily as accuracy allows so that the site staff can correct the problems discovered during the audit. Depending on company policy, auditors should be ready to guide the audited site staff in correcting deficiencies and help them measure the success of these efforts. Management should continually supervise deficiencies that are turned up by the audit until they are completely corrected. The motto for higher management armed with the audit report should be, "follow up, follow up, and follow up."

The Audit - Not an Event but a Process

It must be kept in mind that as organizations evolve, their security structures will change as well. With this in mind, the security audit is not a one-time task, but a continual effort to improve data protection. The audit measures the organization's security policy and provides an analysis of the effectiveness of that policy within the context of the organization's structure, objectives and activities. The audit should build on previous audit efforts to help refine the policy and correct deficiencies that are discovered through the audit process. Whereas tools are an important part of the audit process, the audit is less about the use of the latest and greatest vulnerability assessment tool, and more about the use of organized, consistent, accurate, data collection and analysis to produce findings that can be measurably corrected.

Why security audit is required?

Security audit is required for the following reason.
Here, many attacks which are affect on Application Security and Computer Security.

1. Business Attacks.
2. Financial Attacks.
3. Terrorist Attacks.
4. Fun Attacks.
5. Browser Attacks.
6. Networks and OSes Attacks.
7. Cross Site Scripting Attacks.
8. Directory Traversal Attacks.
9. Authentication Hacking Attacks.

Most Common Computer Crimes.

- Fraud by computer manipulation.
- Computer forgery.
- Damage to or modifications of computer data or programs.
- Unauthorized access to computer systems and service.
- Unauthorized reproduction of legally protected computer programs.

Kinds of Incidents

- Probe.
  - Attempts to gain access into a system.
- Scan.
  - Large number of probes.
- Account Compromise.
  - Unauthorized use of an account by someone other than the owner.
- Root Compromise.
  - An account compromise where the account has special privileges on the system.
- Packet Sniffer.
  - A program that captures data as packets travel through the network.
- Denial of Service.
  - Preventing authorized users from using the system.
- Exploitation of Trust.
  - Forging of identity in order to gain unauthorized access.
- Malicious Code.
  - Programs that, when executed, cause undesired results such as loss of data, downtime, denial of service.
- Internet Infrastructure Attacks.
  - Rare but serious attacks on key components of the Internet structure such as network name servers and large archive sites.

Virus Trends

1. URL-BASED VIRUSES.

URL-based viruses increased from 3 in 2005 to 13 in 2006. URL-based viruses are extremely potent because they propagate via email. The email contains only a URL and a subject line that entices a user to click.

It is very difficult for a traditional email security system to detect these messages because they look so legitimate. They do not contain an attachment that traditional email antivirus systems can scan. Instead, they use social engineering to entice end users to click the link, thereby delivering the virus payload via the Web. Since more and more companies are deploying sophisticated defenses on Port 25 of their network, virus writers are increasingly turning to port 80—the HTTP (Web) port—as an easy way into the corporate network.

2. MACRO-BASED VIRUSES.

Macro-based viruses increased from zero outbreaks in 2005 to 15 outbreaks in 2006. Macro-based viruses are viruses that reside inside Microsoft files such as Word and Excel files. These viruses can be very potent, since many email administrators rely on attachment file type filtering to limit exposure to new outbreaks. Furthermore, Word and Excel files are much more familiar to end users, resulting in higher open and infection rates than more esoteric attachment file types.

3. EMAIL-BORNE SPYWARE.

Email-borne Spyware continues to flourish. As another example of blended threats, email has become a preferred distribution vector for Spyware. Six of the ten largest virus outbreaks contained some form of Spyware. Most of this Spyware involved Trojans that open a back door on an infected PC and download very harmful code, such as Rootkits. From 2005 through 2006, email-borne Spyware increased by more than 200 percent, a pace consistent with Spyware growth from 2004 to 2005. Clearly, the widespread prevalence of Spyware in viruses supports one of the macro trends highlighted by this report—that these threats are coming from the same sources and that the current state of the art for attackers is to blend this email and Web techniques.

4. MULTIPLE VARIANTS.

Virus writers are using multiple variants of the same virus to evade signature vendors. A great example of this was the Stration virus of 2006. Between September and November 2006, virus writers released waves of variants of the Stration virus, designed to induce customers to open messages by claiming to be security alerts or updates. Many of these variants contained spam engines that were used to propagate the virus by spamming out new copies.

Fraud Prevention

There are many more scams that target online retailers, and fraudsters think up new ones every day. Online retailers will sometimes be victimized, but they can take steps to combat the fraud.

A. By building an in-house solution.
B. By outsourcing the software creation to a service bureau.
C. By purchasing a software package and installing it in-house.

In other words, technology is the solution. E-commerce sites must take advantage of every fraud-fighting tool available in order to triumph over the scammers. Small merchants can scrutinize every transaction for inconsistence a software program might miss.

If something doesn't look right, smaller online retailers should take the same precautions they would with a telephone order, such as calling the bank or the customer to verify card and order information.

Why are security audits of software critical for addressing IT risk?

One of the greatest - but least understood - sources of IT security risks lies within software applications. As the engines that power today's global enterprises, they process, calculate, transmit, and store the data that are an organization's primary asset. Gartner states that 70% of attacks come at the application layer, yet security audits are never performed on most critical software applications to identify vulnerabilities that may expose critical data and operations to hackers. Increasing consequences caused by regulations, targeted attacks and consumer awareness mandate IT security audits and an enterprise-wide approach for measuring and addressing risk to operations from vulnerable software.

What are the key components of a software security audit?

Ongoing security auditing and monitoring provide the means for ongoing effective software security assurance practices. Audit review provides an independent assessment and attestation to management's assurance of an effective system of security vulnerability management, while internal auditing is an important element of the overall system of internal controls.

Compliance audits and other information security audits should specifically address management of security vulnerabilities in the source code, and need to include the following elements:

- Measurement of vulnerabilities against prescribed standards for security and risk management.
- Testing of software applications for the existence of security vulnerabilities using security auditing software.
- Management of software security vulnerabilities in the IT system design, development, maintenance, and change management processes.
- Management of software security in all outsourced IT systems and programming processes.

What is the Executive's role in assuring application security in the organization and IT security audits?

While many positions within an organization have responsibilities for ensuring the security of online applications - starting with the programmer writing the source code, software security assurance is a broad management responsibility. Because software

vulnerabilities represent significant control deficiencies in terms of secure and reliable information, processes, and reporting, they fall within the direct purview of the CEO, CFO, and audit committee of the board. Security vulnerabilities may also result in the disclosure of personal and other sensitive information, and therefore also impact the roles and responsibilities of management positions throughout the enterprise. For a detailed discussion of roles and responsibilities within a software security auditing program, please refer to the Ounce Labs' Software Security Audit Framework.

How can an organization determine the most appropriate method and resources to implement security audit in their development lifecycle?

The three models explained in Ounce Labs' whitepaper titled "Implementing Source Code Vulnerability Testing in the Software Development Lifecycle" represent common scenarios currently being used to successfully implement security audit processes in the development lifecycle and reduce security vulnerabilities. These audit models help establish criteria for assessing goals, resources, obstacles, and ultimately, the most favorable approach for individual organizations.

Although it is clear that development organizations and processes each have their own distinct characteristics, the models outlined in this paper address the common elements that should be leveraged to achieve effective security auditing.

The primary functions that must be served by existing IT staff or security audit experts brought in during implementation are:

Set security requirements: A manager or central source of IT security expertise defines what should be considered vulnerabilities and how to judge criticality based on business needs.

Configure security analysis: Internal definitions are used to customize the source code analysis tool to match policies.

Analyze source code: The source code analysis tool is run against the target application or parts of the application to pinpoint vulnerabilities.

Triage results: Staff members with knowledge of IT security issues and of the application study results to prioritize remediation workflow.

Remediate flaws: Security vulnerabilities are eliminated by rewriting code, removing flawed components, or adding security-related functions.

Verify fixes: The code is rescanned and analyzed to assure the code changes have eliminated the security vulnerability while maintaining application functionality.

Security as a Concern in Governance

For this audit report, we define "governance" as setting clear expectations for the conduct (behaviors and actions) of the entity being governed, and directing, controlling, and strongly influencing the entity to achieve these expectations. It includes specifying a framework for decision making, with assigned decision rights and accountabilities, intended to consistently produce desired behaviors and actions. Governance relies on well-informed decision making and the assurance that such decisions are routinely enacted as intended. Governance is most effective when it is systemic, woven into the culture and fabric of organizational behaviors and actions. Governance actions create and sustain the connections among principles, policies, processes, products, people, and performance.

Enterprise security is important to almost all organizations. But with so many other topics vying for leadership attention, what priority should be assigned to enterprise security? What constitutes adequate security and what constitutes adequate oversight of it? How can leaders use governance to sustain adequate security in a constantly changing business, customer, risk, and technology environment?

Adequate security is about managing risk. Governance and risk management are inextricably linked—governance is an expression of responsible risk management, and effective risk management requires efficient governance. Inserting security into ongoing governance and Risk management conversations are an effective and sustainable approach for addressing security.

Art Coviello, president and CEO at RSA Security and co-chair of the Corporate Governance Task Force, 3 states that "It is the fiduciary responsibility of senior management in organizations to take reasonable steps to secure their information systems. Information Security is not just a technology issue; it is also a corporate governance issue" [Braun 04].

As a result, director and officer oversight of corporate digital security is embedded within the fiduciary duty of care owed to company shareholders. In the absence of some type of meaningful governance structure and way of measuring enterprise security, the following questions naturally arise:

- How can an organization know what its greatest security risk exposures are?
- How can an organization know if it is secure enough?

- To detect and prevent security events that requires business-continuity, crisis management, and disaster-recovery actions?
- To protect stakeholder interests and meet stakeholder expectations?
- To ensure enterprise viability?

Governing for enterprise security means viewing adequate security as a non-negotiable requirement of being in business. To achieve a sustainable capability, enterprise security must be addressed at a governance level by organizational leaders and not be relegated to a technical specialty within the IT department.

The role of boards of directors, senior executives, and indeed all managers includes establishing and reinforcing the business need for effective enterprise security. Otherwise, the organization's desired state of security will not be articulated, achieved, or sustained. If the responsibility for enterprise security is relegated to a role in the organization that lacks the authority, accountability, and resources to act and enforce, enterprise security will not be optimal.

e-Gov News

12th National eGovernance Conference 2008-09

The 12th National Conference on e-Governance organized by Department of Administrative Reforms & Public Grievance, Department of Information Technology, Government of India in collaboration with State Government of Goa on 12th -13th February, 2009 at Goa.

The theme for this year's conference was "e-Governance: Breaking Barriers, Building Bridges". Special focus shall be given to eGovernance initiatives in the area of Local Governance and National flagship programmes such as National Rural Employment Guarantee Scheme (NREGS) & Jawaharlal Nehru National Urban Renewal Mission (JNNURM) that provide services in the underserved section of society. The conference would also deliberate on issues pertaining to building capacities for meeting these challenges.

Senior Officers from the Government, industry, academicians, technical experts and NGOs will participate in the event. Goa Governor Dr. Shivinder Singh Sidhu will inaugurate the conference. Other dignitaries present on the occasion include, Goa Chief Minister Digambar Kamat, and Jainder Singh, Secretary, Department of Information Technology, Government of Goa.

During the Conference, national awards for e-Governance will be presented. The objectives of these awards are to recognize and promote excellence in implementation of e-Governance initiatives. These awards are given in seven different categories concerning various aspects of e-Governance.
The national awards on e-Governance distinguish some of the best Government to Government (G2G), Government of Citizen (G2C), Government of Business (G2B) initiatives by various government departments and public sector units.

Gujarat State had won following 5 awards:

Name of Project nominated for Award	Category
eCity- Ahmedabad Municipal Corporation	Exemplary Horizontal Transfer of ICT-based Best Practice**(Gold Award)**
Drug Logistics Information & Management System -Central Medical Stores Organization	Specific Sectoral Award: Focus Sector for the current year: **Health (Silver Award)**
Hospital Management Information System- Health & Family Welfare Department	Specific Sectoral Award: Focus Sector for the current year: Health**(Bronze Award)**
eProcurement-Industries & Mines Department	Exemplary Horizontal Transfer of ICT-based Best Practice**(Bronze Award)**
e-Krishi Kiran –Anand Agriculture University	Outstanding Performance in Citizen-Centric Service Delivery**(Bronze Award)**

12th National eGovernance Conference-Inauguration

eCity- Ahmedabad Municipal Corporation – Gold Award

Drug Logistics Information & Management System – Silver Award

Hospital Management Information System- Bronze Award

eProcurement - Bronze Award

e-Krishi Kiran - Bronze Award

For electronic subscription to the bulletin, please email us with your email address at:

webmaster@gujaratinformatics.com

or visit us at:

www.gujaratinformatics.com

Contact Address:
Gujarat Informatics Ltd.
Block No. 1, 8th Floor,
Udyog Bhavan,
Gandhinagar – 382017
Phone: 079 – 23256022
Fax: 079 – 23238925