State Auditor's Office
Lawrence F. Alwin, CPA
State Auditor

A Legislative Summary Document Regarding Information System Vulnerability Assessment

Contents

Prepared for the 78th Legislature
by the State Auditor's Office

January 2003

SAO No. 03-396

This is not an audit report and the material in this document has not been subjected to all of the tests and confirmations performed in an audit.

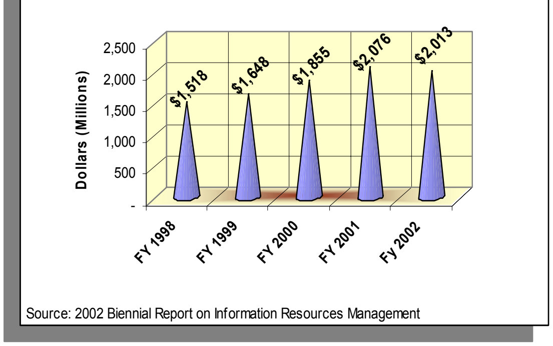
Information System Vulnerability Assessment

SAO Contact: Pat Keith, Chief Information Officer
(512) 936-9500

Background – How Big Is The Risk?

The State is increasing its dependence on information systems, as its growing level of technology spending demonstrates. From fiscal year 1998 through fiscal year 2002, the State spent more than $9 billion (an average of $1.8 billion each fiscal year) on technology. The four major categories of information technology spending (contract services, hardware, software, and telecommunications) reflect increases in spending and project scope across this same time period. Expenditures in the contract services category in particular have increased significantly. The growing reliance on information systems to perform daily tasks and achieve state objectives requires greater attention to security and control over the State's technology assets.

Technology Expenditures: FY1998-2000



Source: 2002 Biennial Report on Information Resources Management

In response to increasing risks and to satisfy audit standards, the State Auditor's Office (SAO) has developed capabilities to assess information system vulnerabilities, including wireless technology. Additionally, the Department of Information Resources (DIR) established a Security Office to set policies and standards and to provide security services and information system penetration testing.

In September 2001, the SAO and DIR agreed to collaborate on security assessments and share information regarding system vulnerabilities. This cooperative arrangement maximizes the effectiveness of current resources without duplicating costs.

The significance of performing vulnerability assessments is twofold. First, when systems and information that are confidential and protected are compromised, the State is at risk of legal action. Second, system intrusions have an impact on the State's day-to-day operations and increase inefficiencies. The dollars and person-hours required to detect, contain, and rectify these intrusions could be better used elsewhere. As of November 25, 2002, DIR's Security Office estimated that security incidents occurring from June 2002 through September 2002 cost the State 5,058 person-hours and $161,490 (see text box). If state efforts in the area of security parallel the American private sector, many state entities are unprepared for even minor virus-oriented attacks.[1]

Security Incident Summary Results June 2002 – September 2002	
Number of agency/university incident reports	264
Estimated total person-hours	5,058
Estimated total costs	$161,490
Source: DIR Security Office – www.dir.state.tx.us	

Vulnerability Assessment Results

During fiscal years 2000 and 2001, DIR performed 38 vulnerability assessments. Since DIR and the SAO began working collaboratively in September 2001, the SAO performed 9 vulnerability assessments and DIR performed 16. The total number of vulnerability assessments performed since the beginning of fiscal year 2000 is 63. Results from those vulnerability assessments were as follows:

[1] Source: State of Texas, Office of the Attorney General, State Infrastructure Protection Advisory Committee, *The Texas Infrastructure Protection: A State Model for Information Assurance and Information Sharing to Protect Critical Infrastructures* (SIPAC Report, March 25, 2002)

- Twenty-five vulnerability assessments (40 percent) resulted in ratings of *poor*, indicating that significant vulnerabilities were found (see text box).
- Twenty-one vulnerability assessments (33 percent) found enough security weaknesses to result in ratings of *fair*.
- Seventeen vulnerability assessments (27 percent) resulted in ratings of *adequate*, indicating that major vulnerabilities were not found.

Rating Scheme

Poor - Either (1) DIR gained proprietary information from and control of target systems, or (2) the SAO identified vulnerabilities or combinations of vulnerabilities that place the system at severe risk.

Fair - Either (1) DIR gained proprietary information from or control of target systems, or (2) the SAO identified vulnerabilities that could allow system penetration given more time.

Adequate - Either (1) DIR was unable to gain proprietary information from or control of target systems, or (2) the SAO did not identify major vulnerabilities that put systems at risk.

Testing results alone, however, do not fully depict the risks the State faces with respect to its information systems. A vulnerability assessment does not usually encompass an entire system's infrastructure, nor can it provide assurances over time. Vulnerability assessments represent a snapshot of the security profile of selected system components at the time the assessment was conducted.

The scope of vulnerability assessment testing is driven by the size of the state entity; the importance of the system tested; and, in the case of the SAO, the scope of the audit. Additionally, if information system issues are known or suspected, testing may be changed to accommodate those issues. Some systems are known to be vulnerable yet are also critical to the operation of a state entity. Because testing could interfere with critical operations, direct testing of these systems may be avoided.

Confidentiality

Vulnerability assessment results constitute sensitive information because they could be used by others to gain unauthorized access to an information system. The sensitivity of this information is recognized in Texas Government Code, Section 2054.077(c), which states that a vulnerability report and any information or communication prepared or maintained for use in the preparation of a vulnerability report is confidential and is not subject to disclosure under Texas Government Code, Chapter 552. Appropriately, information that could be used to harm information systems and/or the information itself should not be made available for public use. The SAO has developed both public and detailed/confidential reports for vulnerability assessments, thereby providing high level information for the public and still maintaining the confidentiality of sensitive information. State entities at which vulnerability assessments have been conducted receive both reports so that they can manage public inquiry and remedy system weaknesses.

The SAO is prepared to brief the Legislature on vulnerability assessments and other technology-related issues. For further information, contact Pat Keith, Chief Information Officer, at (512) 936-9500.