TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Computer Security Controls Should Be Strengthened in the Former Brooklyn District

DRAFT

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

Phone Number | 202-622-6500
Email Address | TIGTACommunications@tigta.treas.gov
Web Site | http://www.tigta.gov

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C, 20220

INSPECTOR GENERAL
FOR TAX
ADMINISTRATION

October 25, 2000

Response Date
November 24, 2000

MEMORANDUM FOR CHIEF INFORMATION OFFICER

FROM: Scott E. Wilson /s/ Scott E. Wilson
Associate Inspector General for Audit (Information Systems Programs)

SUBJECT: Draft Audit Report -Computer Security Controls Should Be Strengthened ill the Former Brooklyn District

Attached for your review and comments are two copies of the subject draft audit report. In summary, steps should be taken to strengthen the former Brooklyn District's controls to guard against and detect inappropriate accesses. Specifically, the Internal Revenue Service (IRS) can improve security controls over information systems in the following three areas: user account management, security surveillance, and physical security.

We would appreciate receiving your written response to the findings and recommendations in the draft report within 30 calendar days, from the date of this memorandum. We are also providing copies of the report to the IF~S managers who are affected by the report recommendations.

The Treasury Inspector General for Tax Administration (TIGTA) has designated this report as Limited Official Use (LOU) pursuant to Treasury Directive TO P-71-10, Chapter III, Section 2, "Limited Official Use Information and Other Legends" of the Department of Treasury Security Manual. Because this document has been designated LOU, it may only be made available to those officials; who have a need to know the information contained within this report in the performance or their official duties. This report must be safeguarded and protected from unauthorized disclosure; therefore, all requests for disclosure of this report must be referred to the Disclosure Unit within the TIGTA's Office of Chief Counsel.

Please contact me at (202) 622-8510 if you have questions, or your staff may contact Steve Mullins at (925) 210-7024.

Attachments (2)

Table of Contents

Executive Summary

Advances in information technology have caused the daily activities of the Internal Revenue Service (IRS) to become increasingly automated and inter-linked. These advances, while improving efficiency, have .also increased the risk that hackers or dishonest employee; could misuse taxpayer data. Malicious acts by employees present an even greater risk since they already have access to data via networks. The former Brooklyn District had over 1,000 employees connected to its local area network (LAN). On October I, 2000, the Brooklyn District was realigned as part of the IRS' organizational modernization.

The overall objective of this review was to determine whether the former Brooklyn District had effective security controls over its computer systems to safeguard information against unauthorized access or use, disclosure, damage, modification, and loss. We reviewed controls over the former District's LAN with emphasis on the Taxpayer Advocate Management Information System (TAMIS)[1] to demonstrate the impact of security weaknesses. This review was part of a series of reviews initiated to assess the overall effectiveness of security controls over the IR S' information systems.

Results

The former District had various computer security controls in place which reduce the risk, to some degree, of unauthorized access; and destruction of data. For example, logical access controls, such as user identification and passwords, were properly set up at the minicomputer and LAN level. Also, logical access to data on sensitive systems, such as the TAMIS, was correctly limited, and physical security was generally sufficient. However, additional steps in the following areas can further strengthen the computer security program:

User Account Management

LAN and TAMIS user accounts were not always cancelled when employees transferred or left the IRS. In addition, current employees were given unneeded access to the TAMIS, thus increasing the risk of unauthorized access to taxpayer information on the system. However, we did not identify any inappropriate activity by any of these users.

In addition, special capabilities to research the TAMIS had been granted to all TAMIS users, most of whom had no need for it. Those employees had the capability to browse data for over one million taxpayers without detection. We were unable to determine if such browsing occurred because controls were insufficient to detect this activity.

[1] The TAMIS is an automated system for processing and controlling Taxpayer Advocate Service cases.

Security Surveillance

There was no documented monitoring of the TAMIS system or the LAN to identify who was logging on or what they did. While audit trails[2] were run on minicomputers, the TAMIS database application, and the LAN to detect improper system activity, there was no indication they had been reviewed. Essentially, the former District did not use audit trails to detect improper activity on its computer systems.

Physical Security

In general, physical security was sufficient to protect computer systems from damage or unauthorized access, and environmental controls were adequate in protecting 1axpayer data. However, one concern was that the Information Systems (IS) Division is housed on a floor that is regularly accessed by taxpayers visiting a Collection Division interview unit, and we noted that keypads used to access this area were not shielded to prevent observation of the security code. A similar finding was reported by the National Headquarters Security, Evaluation & Oversight function during a district security review in 1998. We suggest using shields to increase access protection to the area.

Summary of Recommendations

The Chief Information Officer and the appropriate IRS operations executives need to take steps to address the specific weaknesses identified in this report. Actions management should take include: allowing only appropriate system permissions and annually reviewing employee access privileges; ensuring system access is promptly removed for departing employees; and training responsible employees on performing audit trail reviews.

[2] Audit trails are a control for detecting improper activity on computer systems. Generally, they should show who took the action, what they did, where they did it, and when.

Our objective was to determine whether the former Brooklyn District had effective security controls over its computer systems to safeguard information against unauthorized access or use, disclosure, damage, modification, and loss.

Objective and Scope

The overall objective of this review was to determine whether the Internal Revenue Service's (IRS) former Brooklyn District had effective security controls over its computer systems to safeguard information against unauthorized access or use, disclosure, damage, modification, and loss.

We visited the District from April to June 2008. Over 1,000 employees have access to the former District's local area network (LAN), approximately 30 of whom have access to taxpayer information through the Taxpayer Advocate Management Information System (TAMIS)[3]. We selected and reviewed TAMIS controls to demonstrate the impact of security weaknesses.

During our visit, we reviewed user account management, security surveillance, physical security, and logical access controls for the LAN, minicomputers, and the TAMIS. We performed this review in accordance with *Government Auditing Standards.*

Details of our audit objective, scope, and methodology are presented in Appendix I, Major Contributors to This Report are listed in Appendix II.

Background

The purpose of computer security is to protect an organization's valuable resources, such as information, hardware, and software, through the selection and application of appropriate safeguards, security helps the organization meet its mission by protecting its physical and financial resources, reputation, legal position, employees, and other tangible and intangible assets.

[3] The TAMIS is an automated system for processing and controlling Taxpayer Advocate Service cases.

Physical and logical access controls, restricting users' privileges, and monitoring system activity are all tools to help ensure adequate security.

The IRS, along with other high-profile government agencies and corporations, is at risk of outsiders' efforts to break into its computer systems. Advances in information technology have caused the daily activities of the IRS to become increasingly automated and interlinked. These advances, while improving efficiency, have also increased the risk that hackers or dishonest employees could misuse taxpayer data. Malicious acts by employees present an even greater risk since they already have access to networks, in addition to being physically located where the computers are housed.

Achieving adequate security depends on properly applying several types of controls. These can be categorized into the following four groups:

- User Account Management-Manual processes to grant computer access privileges. Access should be granted to only those employees who need it to perform their official duties;
- System Security Surveillance -Processes to log and monitor computer system activities for indications of security violations as well as to timely respond to such incidents.
- Physical Security --Controls to limit physical access to computer system components (workstations, servers, and networks) to only those who are authorized and to provide a suitable physical environment which protects computer system components from man-made and natural hazards.
- System Logical Access -Computer system controls, such as password verification, to restrict access to computing resources.

The Congress recognized the significance of maintaining adequate information system security in the IRS Restructuring and Reform Act of 1998[4] This law directs the Treasury Inspector General for Tax Administration (TIGTA) to report to the Congress an assessment of the adequacy and security of the IRS' information technology. This report is part of TIGTA's effort to provide that assessment.

Results

The former Brooklyn District has various computer security controls in place which reduce the risk, to some degree, of unauthorized access and destruction of data. For example, logical access controls, such as user identification and passwords, were properly set up at the minicomputer and LAN level Logical access to data on sensitive systems, such as the TAMIS, was correctly limited, and physical security was generally sufficient.

[4] Pub. L No. 105-206, 112 Stat. 685.

However, additional steps can strengthen the computer security program. User accounts were assigned to employees who did not need access to the LAN and the TAMIS. In addition, security surveillance was not sufficient to detect improper computer activity. While physical security was sufficient, we noted one weakness that should be corrected. These conditions increase the risk that sensitive data could be improperly disclosed or misused, possibly to commit fraud or other crimes.

Although various controls in place reduced risks to some degree, additional steps can strengthen the computer security program.

User Account Management

Users were given unneeded access to the LAN and the TAMIS.

Managers should restrict access to computer data to only those users who need it to carry out their duties. Because employees' responsibilities often change, managers should periodically check to ensure that access to taxpayer data is proper, based on employees' current assignments, Employees must be removed promptly from systems and applications which they do not need to access.

Twenty-four employees who separated from the District between April 1999 and March 2000, continued to have access to the LAN. Access was also not cancelled for 12 TAMIS users when they left the IRS or tral1sferred to other functions, Some managers were not aware that a form was required to cancel employees' accesses, other managers were not aware that their employees had access.

In addition, managers erroneously assigned TAMIS user accounts to 19 of the 40 users who did not need access to the system. None of the 19 had ever logged on to the system for periods up to 4 years. Managers did not detect the unneeded access privileges because the required annual certification reviews were not performed. However, we did not identify any inappropriate activity by any of these employees.

In some instances, TAMIS managers did not timely re-assign the separating employees' workload. They erroneously believed that the user accounts could not be cancelled as long as inventory was still assigned. The local Taxpayer Advocate is now aware that inventories of separating employees should be reassigned and user accounts cancelled as soon as employees no longer require access.

During our review of who had the ability to use the query capability of the system, we determined that all TAMIS users, regardless of permission 1evel, could use query software through the TAMIS menu, This software enabled users to research the database and create customized reports. It can be used when regular reports do not provide the required data.

Query software gives user access to personal information for over one million taxpayers on the TAMIS. Most other users having this access did not need it, in our opinion

The software also enables users to browse the personal information of over one million taxpayers, allowing the possibility of illegal activity. Managers did not give adequate weight to this risk by allowing employees this capability. We believe that most of the users had no need for this, application. It is especially critical to limit and monitor the use of query software because managers have no audit trails[5] to detect unauthorized use. The TAMIS application does not capture query software activity, and the operating system captures only system-level activity, such as when a user enters or exits the software. Because of the insufficient audit trail information, we were unable to detect whether any inappropriate usage of query software occurred.

Recommendations

The Chief Information Office, in conjunction with the appropriate IRS operations executive, should

1. Develop procedures to ensure that all managers annually review employee access to information systems and certify that the access and permissions are appropriate.
2. Remind managers of requirements for removing access privileges for departing employees.
3. Revise the current TAMIS so that query software capability is restricted only to those needing such access. Ensure that annual reviews of user account access and permissions include query software access.

Security Surveillance

Audit trails were run, but there was no evidence that they were reviewed.

An integral part of the controls for detecting improper activity on computer systems is the production and review of audit trails. Generally, they should show who took the action, what they did, where they did it, and when. Audit trails were available to detect activity on the LAN, on the TAMIS application running on the host server, and on the client minicomputer that supports the TAMIS. However, we noted that, in no instance, were audit trails being reviewed to detect improper activity

At the request of the National Headquarters, an outside consultant prepared a risk assessment report, dated August 1999, which stated that TAMIS audit logs were not distributed or reviewed at the IRS Center which maintains the national TAMIS database. The report concluded that, without review of the audit logs, activities of authorized users could not be determined, nor could access attempts by unauthorized users be detected. The report recommended that logs be distributed and reviewed. However, the security

[5] Pub. L No. 105-206, 112 Stat. 685.

analyst at the IRS Center advised us that this recommendation had not been implemented because a decision had been made that the risk was not sufficient to warrant review of audit trails.

The Internal Revenue Manual and other guidelines require that system administrators generate and distribute audit trails to appropriate managers for review Functional security coordinators, responsible for system security in the local field offices should review audit trails to ensure system integrity and to report anomalies. They should also review audit logs at least weekly and provide reports of security problems to the system administrators, the Chief, Information System (IS), and functional managers. User managers should ensure that audit trails are appropriately reviewed.

Although there are clear requirements for gathering and reviewing audit trail information, the requirements are often not specific regarding how to conduct the reviews and how they should be documented. In the absence of these guidelines, the former District's management did not devise interim or local procedures to ensure the reviews were completed and adequately documented.

The ability to log and monitor computer system activities is important because it provides a means to detect improper activities that could occur if other system controls are circumvented. When audit trails are not properly monitored, the ability to identify offenders and pinpoint weaknesses to prevent future occurrences is lost.

Recommendation

4. The Chief Information Officer and appropriate IRS operations executives should reinforce requirements to perform audit trail reviews on the LAN, on the TAMIS application running on the host server, and on the client minicomputer that supports the TAMIS. Also, they should provide training on how to perform reviews, including what to review and when, how to document reviews, and how to handle potential problems discovered.

Physical Security

Physical security is the most fundamental form of information systems control and is important because it is the first barrier in preventing unauthorized access and loss of taxpayer information. Physical security controls are implemented to protect sensitive areas; housing information systems equipment or data. Sensitive areas requiring physical controls include computer rooms and all work areas containing sensitive taxpayer information.

In general, we found physical security controls to be sufficient. We also determined that environmental controls, such as temperature and humidity indicators, were adequate to safeguard both computer hardware and taxpayer data.

We suggested increased access protection to the IS work area.

We did identify one physical security concern. The IS function, containing every major computer system in the former District, is housed on a floor that is frequented by taxpayers who conduct business with a Collection Division interview unit. These taxpayers are not under escort when entering or leaving the Collection Division area. Although access to the hallway leading to the IS Division facilities is controlled by a digital code, the keypad used for access is not shielded to prevent observation of the code input. A similar finding was reported by the National Headquarters Security, Evaluation & Oversight function during a district security review in 1998. We suggest that shields be used to increase access protection to the area.

Conclusion

Strengthening computer security controls could potentially reduce manipulation, destruction, theft, or improper use or disclosure of sensitive data.

Like other IRS offices, the former District's systems contain large amounts of sensitive information, and can be accessed by a large number of employees. Strengthening computer security controls can help ensure that access to this information is restricted to only those having a legitimate business need to list the information. Implementation of our recommendations will reduce opportunities to improperly manipulate or destroy data, vulnerabilities to theft, and the risk of improper use or disclosure of sensitive taxpayer data.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine whether the Internal Revenue Service's (IRS) former Brooklyn District had effective security controls over its computer systems to safeguard information against unauthorized access or USE, disclosure damage, modification, and loss. To accomplish this objective, we:

I. Determined if management had implemented sufficient user account management controls to ensure that access to taxpayer data on the local area network (LAN) was limited to authorized individuals on a need-to-know basis.

   A. Interviewed the Brooklyn Taxpayer Advocate, the system administrator, and user managers to identify and document the procedures in place for requesting, establishing, and closing the Taxpayer Advocate Management Information System (TAMIS) and LAN user accounts
   B. Obtained a master list of TAMIS users from the system administrator. Reviewed all 40 TAMIS user accounts from the master list to ensure access fights were documented, authorized, and reviewed.
   C. Determined if any Brooklyn District employees continued to have TAMIS or LAN access after separating from the IRS. Compared a list of employees who separated between April 1, 1999, and March 31, 2000, to the list of current TAMIS and LAN users.
   D. Determined if ad-hoc queries could be made to research the TAMIS
   E. Determined if management annually certified that system access for each employee had been reviewed and was appropriate database.

II. Determined whether controls were effective to ensure that all activity involving access to and modifications of sensitive or critical files was logged, effectively reviewed, and responded to if incidents occurred.

A. Evaluated the adequacy of the audit trail by determining whether the required information (log-ons, dates, times, places, applications and files used) was being recorded. Attempted to gain access to the system using a variety of unauthorized logon names (IDs) and passwords. Verified that the attempted logons are properly recorded on the audit trail. Reviewed guidelines to identify audit trail policies and procedures, including reporting security violations.
B. Determined if the audit trail was protected from unauthorized modification by interviewing the system administrator and functional coordinator to identify who had access, to the audit trc.ils and what level of permission was granted. Identified the criteria used by the security administrator to turn on the audit log, whether he/she backed up the audit trail, and how long it was retained.
C. Determined if data security personnel periodically reviewed security settings to ensure they were configured to provide sufficient audit trails.
D. Determined whether audit trails were being run and reviewed on the minicomputers, the LAN, and the TAMIS. If they were not being reviewed, determined the reason. Determined whether any security violation reports were issued, reported to management and investigated.
E. Determined the extent that system administrators, programmers, security analysts, functional coordinators and managers had access to the audit trails, if any guidelines had been developed for reviewing audit trails, if security logs were required to be reviewed on a regular-basis, and if they had received training to review audit trails.
F. Evaluated the effectiveness of the procedures for recognizing and handling computer security incidents. Determined whether the procedures identified roles and responsibilities; included criteria for documenting, determining the seriousness, reporting, investigating, and imposing disciplinary action; and provided the ability to respond quickly and effectively.
G. Determined what instruction, direction and training the Security Specialist received for reporting security incidents.

III. Determined whether logical security controls were effectively installed to protect the integrity and confidentiality of the information processed transmitted and stored.

A. Interviewed security/system administrators to identify authentication software in use, to obtain password policies, and to determine procedures for generating and communicating LAN/application passwords to users.
B. Determined if unique user IDs and passwords were issued and if any group/generic user IDs and passwords existed. Reviewed accounts that did not have an associated password.
C. Determined if any security software was used to proactively screen passwords. Identified any automated tools used to restrict system access and monitor the security and activity of the LAN application.
D. Determined if the duties of system administration and security monitoring were separated to deter and detect unauthorized access and changes to the

system.

E. Interviewed users and observed their work area; and logon process to determine if unique user IDs and passwords were issued, any group/generic user IDs and passwords existed, the user changed the password when initially logging on, the system prevented plain text display of the password when entered, and passwords were disclosed on any medium at the user's workstation.
F. Conducted an "after hours" security check of users' work areas for passwords posted at the workstation and computers where the user did not sign-off or lock the terminal.
G. Determined if controls were properly implemented to restrict access and prevent unauthorized changes to the LAN operating system, selected security software settings, and other sensitive or critical files and libraries. Observed non-administrator system users demonstrate whether they could gain access to these files and libraries and noted the type of access they had.
H. Determined whether encryption was used to protect passwords from disclosure and unauthorized modification. Determined if the system was set to erase the plain text memory of the password immediately after encryption, if the encrypted password was stored in a shadow file instead if there was a key that could be used to read the passwords, and whether the key was stored outside the system.
I. Reviewed security software access audit trail reports and related access rules and authorizations to ensure that individual security file accesses matched the level and type authorized.

IV. Evaluated the effectiveness of physical and environmental controls over the LAN and the TAMIS for physically restricting access to computer hardware and adequately safeguarding taxpayer data.

A. Conducted walk-throughs of TAMIS workstations. Determined whether physical entrances were restricted to authorized personnel.
B. Observed the main computer facility to ensure it was unlabeled so that a low profile was maintained. Determined whether area housing computer equipment met construction standards that deter access to unauthorized personnel.
C. Conferred with building security, local management, and the Treasury Inspector General for Tax Administration's Office of Investigations to verify whether any security breaches had been reported.
D. Determined if thermometers and humidity indicators were routinely monitored.

Appendix II

Major Contributors to This Report

Scott E. Wilson, Associate Inspector General for Audit (Information Systems Programs)
Stephen Mullins, Director
Gerald Horn, Audit Manager
Joan Raniolo, Senior Auditor
David Hodge, Auditor
James McCormick, Auditor
Theodore Tomko, Auditor

Appendix III

Report Distribution List

Director, Office of Security and Privacy Oversight IS :SPO
Area Director for Information Technology -Northeast Area I:S:F:NE
National Taxpayer Advocate TA Taxpayer Advocate,
Director, New York/New England Area C:TA:NYNE