New Jersey State Legislature
Office of Legislative Services
Office of the State Auditor

New Jersey Judiciary
Vulnerability Assessment-Court Vicinages

February 1, 2010 to October 31, 2010

Stephen M. Eells
State Auditor

New Jersey State Legislature

OFFICE OF LEGISLATIVE SERVICES
OFFICE OF THE STATE AUDITOR
125 SOUTH WARREN STREET
PO BOX 067
TRENTON NJ 08625-0067

ALBERT PORRONI
Executive Director
(609) 292-4625

OFFICE OF THE STATE AUDITOR
(609) 292-3700
FAX (609) 633-0834

STEPHEN M. EELLS
State Auditor

THOMAS R. MESEROLL
Assistant State Auditor

JOHN J. TERMYNA
Assistant State Auditor

The Honorable Chris Christie
Governor of New Jersey

The Honorable Stuart Rabner
Chief Justice of the Supreme Court

The Honorable Stephen M. Sweeney
President of the Senate

The Honorable Sheila Y. Oliver
Speaker of the General Assembly

Mr. Albert Porroni
Executive Director
Office of Legislative Services

Enclosed is our report on the audit of the New Jersey Judiciary, Vulnerability Assessment-Court Vicinages for the period of February 1, 2010 to October 31, 2010. If you would like a personal briefing, please call me at (609) 292-3700.

Stephen M. Eells
State Auditor
March 16, 2011

Table of Contents

Scope

We assessed and reviewed the adequacy of information technology (IT) policies and procedures for the Judiciary Court Vicinages for the period February 1, 2010 to October 31, 2010. Our audit evaluated selected IT general controls in place at the vicinages over their networks and systems that process and protect both public and private information. These controls included security management, access control, segregation of duties, configuration management, business continuity plans in the event of processing interruptions, protection of confidential information, and the help desk function.

Objectives

The objectives of our audit were to determine the adequacy of the selected IT general controls over the vicinage computer network to minimize the risk of unauthorized physical or logical access, to provide for business continuity, to adequately segregate incompatible functions, to ensure changes are properly implemented and documented, and to provide for adequate planning.

This audit was conducted pursuant to the State Auditor's responsibilities as set forth in Article VII, Section I, Paragraph 6 of the State Constitution and Title 52 of the New Jersey Statutes.

Methodology

Our audit was conducted in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States. Additional guidance for the conduct of the audit was provided by the *Federal Information System Controls Audit Manual* (FISCAM) issued by the Government Accountability Office, *Control Objectives for Information and related Technology* (CObIT) issued by the IT Governance Institute, and other industry-wide information technology security resources.

In preparation for our testing, we studied legislation, Judiciary operation plans, procedural guidelines and flow charts, and industry and governmental standards for computer security and operation. Provisions that we considered significant were documented and compliance with those requirements was verified through interviews of key personnel, observation and access of network infrastructure, and through other tests we considered necessary.

A nonstatistical sampling approach was used. Our samples were designed to provide conclusions about internal control attributes. Sample items were selected judgmentally.

Conclusions

Judiciary management has recognized the importance of security over the vicinage network, network infrastructure, and the services they provide. We found controls in place and functioning to minimize the risk of unauthorized physical or logical access, provide for business continuity, adequately segregate incompatible functions, ensure changes are properly implemented, and provide for adequate planning. However, in making these determinations, we noted certain control areas where additional improvement should be made. We have provided the Judiciary with a management letter containing a more detailed discussion of network security specifics.

Control Issues Reported Under Separate Cover

Information Technology controls should be strengthened in the specific areas noted.

Testing was performed on various vicinage controls and processes associated with granting, monitoring, disabling, and deleting access to the Judiciary logical network for specific user accounts. Testing was also performed on portable storage devices (PSD), software updates, and the monitoring of wireless signals within a vicinage. Based on our testing, controls should be strengthened in specific areas. Controls over user account management and PSDs should be improved. In addition, weaknesses in the software update process were noted and should be improved as well as controls to detect rogue wireless signals within a vicinage building. The control weaknesses noted increase the risk of unauthorized access and network disruption. We have provided the Judiciary with the necessary technical details for those items under separate cover.

Recommendation

We recommend reviewing user accounts to determine those that should be disabled or deleted, instituting procedures to ensure that vicinage machines are updated on a consistent and timely basis, and monitoring wireless connections more closely so that only Judiciary controlled wireless signals are within the vicinage building. We also recommend that a method of controlling PSDs be developed and their use limited to only a select group, and that these controls be incorporated into the policy to be used statewide.

Judiciary Response

We agree with the above recommendations and are taking steps to address those recommendations. We will be reviewing and monitoring user accounts with Vicinage IT personnel to ensure compliance. We will monitor Windows updates centrally using Microsoft's System Center Configuration Manager (SCCM) to ensure that system updates are being performed in a timely manner. We also plan to perform wireless monitoring as our budget allows. We will integrate a portable storage device (PSD) policy into our Judiciary Security Policy.

Security Management

Vicinage Developed Applications

Vicinage developed in-house applications may be redundant and conflict with existing security policies and procedures.

Thirteen of the 15 vicinages have developed and maintain their own applications outside those normally developed and maintained by the Judiciary's Information Technology Office (ITO). Our survey work determined there are 178 applications used for various purposes spread across these 13 vicinages. In April 2010, the Information Technology Initiative Review Committee (ITIRC) met to discuss these applications and determine their ultimate disposition.

Industry best practices state that to implement an effective security program, entities need to maintain a complete, accurate, and up-to-date inventory of their systems. Without one, the entity cannot effectively manage information system (IS) controls across the entity. For example, effective configuration management requires the entity to know what systems they have and whether the systems are configured as intended. Furthermore, the inventory is necessary for effective monitoring, testing, and evaluation of IS controls, and to support information technology planning, budgeting, acquisition, and management. A decentralized IT environment allows for vicinage IT staff to be on their own to develop vicinage specific applications outside the purview of the ITO.

Some developed applications may cause redundant data entry by court staff that may already have been entered into other systems and applications. For example, one vicinage application uses a Microsoft Access database to record and store bail orders received from probation officers or investigators. This information may already be inputted, stored, and recorded into Promis/Gavel. Among other things, detailed technical documentation may not be available to allow for another IT staff member to provide support. The source code for many of these applications is not reliably stored and secured. If the source code is lost, there is virtually no way to fix it or make changes to its design.

Recommendation

We recommend the ITIRC continue its efforts in determining the most effective and efficient use of these applications. The purpose of each application should be evaluated and, if necessary, brought under ITO for administration and support, and maintained in a more secure environment.

Judiciary Response

The Information Technology Initiative Review Committee (ITIRC) and its support staff are actively engaged in the process of collecting data on all locally developed applications and conducting needs/support/risk assessments for each of those applications. The product of this analysis will allow the ITIRC and ITO to eliminate some applications while standardizing the supportability model for others.

»»-«««

Access Control

Physical Security and Environmental Controls

Physical security controls related to access and environmental controls need to be improved at the vicinage facilities housing information technology infrastructure.

Organizations should establish adequate physical security controls to ensure proper protection of information technology assets from intentional or unintentional loss or impairment. Physical security controls include restricting physical access to computer resources to appropriate personnel, as well as environmental controls such as smoke detectors, fire alarms, extinguishers, humidity and temperature controls, and uninterruptible power supplies. The audit team performed physical security walkthroughs at each of the 15 vicinages and found numerous physical security issues.

In 3 of the 15 facilities visited, all individuals with access to the server room have not been identified. Two of the vicinages surveyed could not confirm that vicinage employees with access to the computer room have all been trained on the physical security policy. Seven of the vicinages did not periodically review the users with access to the facility. Eleven of the vicinages did not keep logs of individuals accessing the server facility or periodically review the logs. One of the two vicinages that used a keypad entry system for the server room could not determine if the code had ever been changed.

Regarding environmental controls, six of the vicinage facilities visited did not have smoke detectors in their server rooms and seven did not have fire extinguishers in the room. Of the eight that did have fire extinguishers, four of the extinguishers were either not inspected annually or were not tagged for inspection at all. Also, for three vicinages, we were unable to verify that an inspection had been done on the facility by a fire department official. Four vicinages did not have adequate temperature

and/or humidity controls in the computer facility, and seven vicinages do not have their environmental controls tested or inspected at least annually.

There exists a complex relationship in some cases between the actual owners of the buildings that the facilities are in, the county governments, and the vicinages. Often, changes to facilities must go through multiple approvals and be coordinated with the county, and there was a sentiment from Judiciary personnel that they were to do the best they could with what they were given. However, there are still compensating controls that can be put into place by the vicinages for some items.

Lack of physical access controls could lead to intentional or unintentional loss or impairment by either authorized or unauthorized persons. Proper audit trails help ensure that in the event of an issue, steps can be taken to find out the responsible party or parties. Missing or inadequate environmental controls can lead to equipment malfunction or destruction.

Recommendation

We recommend the vicinages identify all individuals with access to technology facilities, determine the appropriateness of such access, and ensure that all those individuals receive training on physical security of the facility. Logs should be kept of all individuals accessing the facility and those logs should be reviewed periodically. In addition, the vicinages with electronic keypad entry should ensure that periodic changes of the access code are done, as well as a change whenever a member of the IT staff leaves. We also recommend the vicinages ensure that smoke detectors and fire extinguishers are in place in all computer facilities, and that the equipment and facility is inspected and serviced annually. In addition, the vicinages should also ensure that adequate temperature and humidity controls are in place to protect infrastructure assets, and that those controls are inspected annually.

Judiciary Response

The Judiciary's Office of Management & Administrative Services (OMAS) and ITO will jointly engage the vicinage General Operations and IT Division Managers to address these identified issues. Appropriate location-specific access control protocols will be developed and published. Assessments will be made of server room environmental systems to ensure ongoing reliability and performance. The Judiciary will also ensure that routine inspections of fire suppression equipment are scheduled.

IT Security Incident Handling

The vicinages lack a consistent, effective, and approved information technology security incident-handling policy.

Audit and monitoring involves the regular collection, review, and analysis of auditable events for indications of inappropriate or unusual activity, and the appropriate investigation and reporting of such activity. Discussions with vicinage staff found that only seven of the vicinages reported having a vicinage-wide information technology security incident-handling policy. FISCAM states that an effective incident response program should be documented, approved, and implemented.

Judiciary personnel stated that they are currently in the process of drafting a Judiciary-wide incident-handling policy that will be disseminated to all vicinages. However, currently there is no policy in place and no requirement that vicinages draft one. We received a copy of the draft policy and verified its existence. If an incident were to occur, the vicinages may be unaware of the procedure to follow to not only alert the proper individuals, but to prevent further damage and preserve electronic evidence. This could allow a potential attacker to be successful in not only damaging the network, but in avoiding prosecution.

Recommendation

We recommend the Judiciary complete its official incident-handling policy and implement it in the vicinages as soon as possible. The vicinages that already have an incident-handling policy in place should work with the AOC to incorporate the Judiciary-wide policy, and deviations should be agreed to and documented.

Judiciary Response

The Judiciary acknowledges this finding and recommendation. The Judiciary's standardized incident-handling policy has been developed and is under review by the Administrative Council, which is expected to recommend statewide adoption of the policy.

Contingency Planning

Critical Personnel

Critical personnel and contact information should be current.

The Administrative Office of the Courts (AOC) issued a directive in the form of a list of 19 critical court functions that must be able to be resumed in the event of a disaster or disruption of services at a courthouse. Each vicinage was to develop a Continuity of Operations Plan (COOP) for each county they are responsible for, incorporating the 19 critical functions plus any vicinage specific essential functions. In addition to the COOP, the AOC issued the Model Court Security Plan in 2001, with an addendum in 2006, as a minimum set of guidelines and standards that must be implemented regarding physical security at each of the courthouses.

Our audit testing disclosed that although each of the vicinages had the required COOP and Model/Local Court Security Plans for each county under their direction, there were eight instances where the critical personnel to be contacted in the event of an emergency or disruption was not current. We also noted one instance where the COOP was not a formal complete document and did not list critical personnel, contact information, and alternate locations. Industry best practices suggest that contingency plan documentation be reviewed periodically to determine that key personnel are still employed by the entity and still have the same responsibilities that caused them to be in the plan.

COOPs are not updated periodically by the Vicinage Operations Manager for changes to critical personnel. The Court Access Services Unit employs an Access database as a master repository for the vicinages to upload their COOPs to the Judiciary. This application is being redesigned to capture additional COOP information from the vicinages that was not captured before. No cross check is performed comparing employee data within the Access database to a Judiciary employee master file for employees no longer employed within the Judiciary or a vicinage. As a result, the appropriate personnel may not be contacted in the event a disruption occurs.

Recommendations

We recommend the Office of Management and Administrative Services-Court Access Unit, as part of their review process, cross check employees to determine that they are still employed and in the position originally included in the plan.

Judiciary Response

Overall responsibility for updating the Vicinage COOPs ultimately rests with the local vicinage judiciary staff. The Court Access Services Unit in the AOC's Office of Management and Administrative Services reviews the vicinage COOPs to ensure that a COOP is in place for each vicinage, that the nineteen standardized Critical Functions are addressed within the COOP, that critical personnel are assigned to each function, that essential materials are listed for each function, and that the primary, secondary, and, where appropriate, tertiary alternate locations are listed. While not knowing vicinage-specific operational details, the Court Access Services Unit reviews the COOPs for reasonableness. The Court Access Services Unit will, on a quarterly basis, distribute a reminder to all vicinages to review and update their respective COOPs for any recently hired or separated staff listed or any other changes.

Formal Agreements

Formal agreements or contracts should be in place detailing the emergency arrangements.

Each county has in their COOP an alternate location(s) to resume court operations in the event that the current courthouse location becomes unusable. We noted five vicinages did not have shared service agreements or memorandums of understanding with their alternate locations.

Industry best practices state "contracts or reciprocal or inter-entity agreements should be established for backup and processing facilities that are in a state of readiness commensurate with the risks of uninterrupted operations, have sufficient processing and storage capacity, and are likely to be available for use."

Currently, the Judiciary does not require the vicinages to have shared services agreements or memorandums of understanding with their alternate location(s). As a result, an event or disruption could occur and the alternate location(s) may not be readily available for use within the statutory timeframe for the critical functions to be resumed.

Recommendations

We recommend the Judiciary require the vicinages have the requisite agreements in place to document the responsibilities of each party in order to avoid any misunderstandings should an event or disruption occur.

Judiciary Response

N.J.S.A 2B: 6-1 requires the county to provide adequate facilities and security for the Law and Chancery Divisions of the Superior Courts. The State Department of Treasury provides facilities for the Judiciary's central office. The Judiciary thus must rely on the county, for the vicinages, and the state, for the central office, to provide adequate facilities should an event occur that closes a structure housing Judiciary operations. The Judiciary encourages the completion of agreements but understands that the situations surrounding occurrences are fluid such that any such agreements may not be enforceable. Agreements currently in existence in any vicinages are not binding contracts.

External Security Surveys

External security surveys should be scheduled and completed within the three to five year requirement.

As part of their periodic security risk assessment process, each vicinage must schedule and complete an internal court physical security survey annually and an external court security audit every three to five years. Our review noted that 4 of the 15 vicinages did not have the mandatory external audit within the required timeframe, with one more than nine years overdue.

In 2001, the Administrative Office of the Courts developed The Model Court Security Plan and gave it to the vicinages as guidance for establishing minimum court security standards. The plan states "An external court security audit must be completed every 3-5 years and must be performed by a team provided jointly by the Sheriff's Association of New Jersey and the Administrative Office of the Courts, or by outside experts in the field such as the United States Marshal's Service." There was an addendum to the plan in 2006, but it did not affect this requirement.

The vicinage operations managers have amongst their duties the responsibility to schedule and coordinate the external court security audits with outside experts. As such, it does not allow for the timely scheduling and coordinating of the audit when required to be performed.

Changes in conditions to court facilities can lead to numerous and serious deficiencies in physical security that may not be identified, acted upon, and resolved in a timely manner. It may also pose a risk to state and county employees, and court users.

Recommendations

We recommend the Office of Management and Administrative Services-Court Access Services unit take over the scheduling and coordination of the external court security audits. We also recommend that they become part of the distribution list of the cover letters once the reviews and reports have been completed by the entities performing the audits.

Judiciary Response

Pursuant to statute (N.J.S.A. 2B: 6-1), security for vicinage Judiciary facilities is to be provided by the local Sheriff's Department. Vicinage staff works with the local Sheriff's Department to schedule the external security audits. The Court Access Services Unit in the AOC's Office of Management and Administrative Services believes this responsibility should continue to be at the vicinage level but with central oversight by Court Access Services. It is the responsibility of Court Access Services to follow up to be certain the security audits are conducted. Court Access Services now has a system in place that will allow them to do so. In addition, Court Access Services will request a copy of the first page of the audit so they may keep this on file at the Administrative Office of the Courts. Court Access Services will continue to communicate with outside agencies such as the Sheriff's Association of New Jersey, the U.S. Marshal's Service, and the District of Delaware to ascertain the availability of teams to conduct these audits and to communicate this information to the vicinages.

New Jersey Courts
Independence • Integrity • Fairness • Quality Service

Administrative Office of the Courts

GLENN A. GRANT, J.A.D.
Acting Administrative Director of the Courts

www.njcourts.com • Phone: 609-984-0275 • Fax: 609-984-6968

February 24, 2011

Mr. Stephen M. Eells
State Auditor
Office of Legislative Services
Trenton, New Jersey

Subj: Audit Report – "New Jersey Judiciary, Vulnerability Assessment-Court Vicinages (February 1, 2010 through October 31, 2010)"

Dear Mr. Eells:

Thank you for the opportunity to comment on the draft report on your office's vulnerability assessment of our vicinage technology environment and operations. The Judiciary's comments in response to the draft report's findings and recommendations are set forth in the relevant sections of the enclosed copy of that draft report.

You will note in reviewing our comments that the Judiciary has taken immediate steps to address the identified deficiencies and we will sustain such efforts through to resolution. We welcome the challenge to continuously improve our policies and practices and further acknowledge and appreciate the professionalism and thoroughness of your audit team.

If you require any additional information or clarification, please feel free to contact James R. Rebo, Judiciary Chief Information Officer, at (609) 984-4378. Again, thank you.

Very truly yours,

Glenn A. Grant, J.A.D.
Acting Administrative Director of the Courts

enclosure
cc: James R. Rebo, Director/CIO
Shelley R. Webster, Director, OMAS
Steven D. Bonville, Chief of Staff