STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

Arizona's Universities
Information Technology Security

REPORT HIGHLIGHTS
PERFORMANCE AUDIT

Subject

Information technology (IT) security practices at Arizona's three universities are important to protect the large amount of sensitive data stored on their computers. Such data can include social security numbers, credit card numbers, and other personal, financial, and educational information for more than 145,000 students, faculty, and staff.

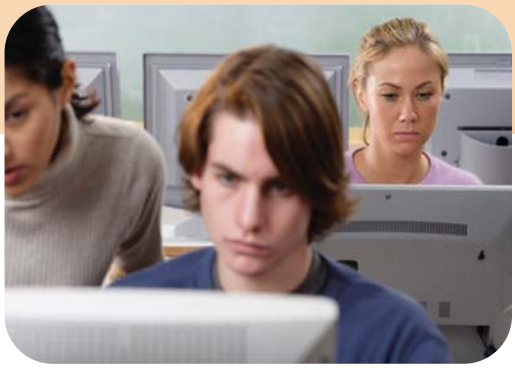
Our Conclusion

The universities' Web-based applications are vulnerable, and they have not fully implemented IT security programs. We were able to access sensitive information, including 10,000 names and social security numbers. The universities need to address their Web-based applications' security and implement comprehensive IT security programs.

2008

June • Report No. 08 – 04

Universities' Web-based applications are vulnerable



Serious security weaknesses exist in Arizona State University's (ASU), the University of Arizona's (UA), and Northern Arizona University's (NAU) Web-based applications, which may allow unauthorized persons to obtain, modify, or delete sensitive data.

Web-based applications—A Web-based application is a software program or system that allows a user to perform a transaction, such as register for classes or purchase a parking permit, over the Internet.

Arizona's universities make extensive use of Web-based applications for such services as student admissions, financial aid, parking, and processing financial, payroll, and other transactions. These applications often process sensitive data such as student records, social security numbers, credit card numbers, names, and addresses. We identified at least 205 significant Web-based applications at the universities: ASU has 71, UA has 97, and NAU has 37.

Testing found serious weaknesses—In order to test these Web-based applications' security, we conducted automated testing on 35 of the 205 applications. All 35 applications had commonly found security weaknesses. Detailed testing of 6 of these applications disclosed critical flaws that would permit an unauthorized user to:

- **Obtain personal information**—In one application, we were able to obtain 10,000 records containing names and social security numbers.
- **Manipulate records**—In two other applications, we were able to exploit a weakness that would have allowed us to take over a large number of user accounts and change information.
- **Attack and affect other users' computers**—In several of the six applications, auditors identified flaws that attackers often use to take over user accounts and install malicious software.

The security flaws identified in these six applications are likely to exist in other university Web-based applications.

Addressing Web-based application security weaknesses—This audit was the first security review performed on university Web-based applications. The universities do not conduct regular security assessments. IT best practices recommend that critical applications be regularly subjected to security reviews. Therefore, the universities need to develop and implement a plan for regularly assessing their Web-based applications.

In addition, the universities need to develop university-wide policies and procedures for updating and maintaining their Web servers. A Web server is a computer that hosts a Web site or Web-

based application. We tested 42 of the universities' Web servers and discovered that 30 of the servers had potential vulnerabilities because of outdated software or insecure settings.

The universities also need to establish university-wide security standards for developing Web-based applications. The standards should ensure security features are built into new Web-based applications as they are being developed and that the security of the applications is tested. According to an IT best practice, building security into the development process is more cost-effective and secure than applying it afterward.

In addition, the universities need to ensure that the Web-based-application developers receive training on how to apply security controls during the development process.

Finally, because the Arizona Board of Regents (Board) oversees the universities and assists with IT issues, the universities should work with the Board to establish timelines for implementing the audit recommendations and should report to the Board on the progress of their implementation efforts.

Recommendations

The universities should develop and implement:

- A plan for conducting regular security assessments of Web-based applications.
- University-wide policies and procedures for updating their Web servers.
- University-wide standards for developing secure Web-based applications.
- Security training for Web-based-application developers.

The universities should establish timelines and report implementation progress to the Board.

Universities need to develop comprehensive IT security programs

In addition to addressing the security of their Web-based applications, the universities need to develop comprehensive university-wide information security programs. These programs are important for identifying and controlling information security risks and ensuring compliance with legal and regulatory requirements.

Information security officers hired—Similar to many other higher-education institutions, each of Arizona's universities now has an Information Security Officer (ISO). Each of the ISOs is responsible for directing and coordinating information security efforts university-wide. Although the universities previously had IT staff who spent a portion of their time working on information security issues such as maintaining firewalls, the ISOs are the first staff who have sole responsibility for all aspects of information security across the university.

IT security programs—The universities are in the early stages of developing and implementing IT security programs. However, none have developed all the standards or procedures needed for a complete IT security program. According to IT standards and best practices, the security program should have at least four key features:

1. Data classification, which identifies and labels information based on its sensitivity and determines the degree of protection needed. None of the three universities have a complete process yet, but each is taking steps to address this area. For example, ASU and UA have drafted documents that require protecting information based on confidentiality, and NAU has inventoried its data.
2. Risk assessment, which identifies threats that may occur and their consequences. Only ASU has drafted a risk assessment standard, and none of the universities have started performing regular university-wide risk assessments. However, all three universities conducted risk assessments in either late 2006 or early 2007 and are developing plans for regularly conducting risk assessments.
3. Security awareness education and training, which keeps students, faculty, and staff aware of information security threats and concerns as well as their responsibilities with regard to IT security. All three universities lack an adequate, university-wide security awareness education and training program that is mandatory for all users; however, each has taken some steps in this area. For example, all three of the universities have security awareness resources available through their Web sites.

4. **Incident response**, which includes procedures for detecting, reporting, and responding to security incidents such as a breach of confidential information due to computer hacking. Without adequate incident response standards or procedures in place, the universities cannot ensure that incidents are responded to consistently and effectively. The universities need to finalize or improve their incident response standards.

Identifying resource requirements—The universities also need to identify the resources necessary for implementing a complete IT security program. Although none of the universities have determined specific resources needed, ASU and UA believe that they need additional resources, such as additional staff or funding for the ISOs to fulfill all of their necessary responsibilities for IT security.

Monitoring compliance—One of the ISO's key responsibilities is to monitor compliance with the IT security program. The monitoring at each university is still in the planning stage. ASU plans to monitor compliance by first conducting risk assessments. UA plans to monitor compliance through its risk assessment process, which will include questions about compliance. NAU intends to use its security analyst to conduct spot-checks in response to a risk assessment questionnaire. The universities should continue with their plans to develop and implement compliance monitoring processes.

Because the Board oversees the universities and assists with IT issues, the universities should also work with the Board to establish timelines for implementing the audit recommendations and should report to the Board on the progress of their implementation efforts.

Recommendations

The universities should:

- Continue their efforts to develop and implement IT security programs that address the four key features.
- Determine their resource needs for implementing their information security programs.
- Continue to develop and implement plans for monitoring information security program compliance.
- Establish timelines and report implementation progress to the Board.

TO OBTAIN MORE INFORMATION

A copy of the full report can be obtained by calling
(602) 553-0333

or by visiting our Web site at:
www.azauditor.gov

Contact person for this report:
Dot Reinhard

Arizona's Universities
Information Technology Security

REPORT
HIGHLIGHTS
PERFORMANCE AUDIT
June 2008 • Report No. 08 – 04