ARIZONA
AuditorGeneral
Making a Positive Difference

REPORT HIGHLIGHTS
Performance Audit
June 2018

Arizona's Universities

Information Technology Security

CONCLUSION: Arizona State University (ASU), Northern Arizona University (NAU), and the University of Arizona (UA) have implemented several information technology (IT) security practices consistent with IT standards and best practices, but these practices can be improved. Specifically, relatively few university employees were susceptible to our simulated social engineering attacks, but some employees took actions that could have provided an attacker with access to sensitive data, indicating a need to improve security awareness training. In addition, although the universities' security controls limited our attempts to gain unauthorized access to their IT systems, we were able to exploit some vulnerabilities to access sensitive data. The universities should enhance their existing policies and procedures in five key areas to further reduce these potential vulnerabilities. Further, each university has established components of an IT security governance framework, but NAU and UA should continue to develop and implement their frameworks. The Arizona Board of Regents (ABOR) should also expand its oversight of the universities' IT security efforts. Finally, each university can improve its data classification processes, and NAU and UA should improve their IT risk assessment and incident response processes.

Universities responsible for safeguarding IT systems and data

ASU, NAU, and UA use computerized electronic systems to support numerous functions such as payroll and student admission applications. To perform these functions, the universities use IT systems to store and process various types of sensitive data, including social security numbers, financial and health information, and educational records for approximately 34,000 faculty and staff, approximately 161,000 students, some of the more than 850,000 alumni, and others, such as prospective students applying for admission. The volume of sensitive data the universities obtain and maintain makes them a potential target for attacks by malicious individuals or organizations, and federal and state laws and regulations specify the universities' responsibility in handling and protecting sensitive data.

Universities should improve security awareness training efforts and enhance IT security controls to further protect IT systems and data

Relatively few employees susceptible to simulated social engineering attacks but security awareness training efforts can be improved—Social engineering attacks attempt to persuade an entity's employees to provide information about, or direct access to, the entity's network using specially crafted means. Although a relatively small number of university employees were susceptible to our simulated social engineering attacks, some employees disclosed information or took other actions that could have provided an attacker with unauthorized access to the universities' IT systems and sensitive data. For example, one attack strategy provided us the means to potentially access IT systems and sensitive data at ASU and UA, and information obtained through another attack strategy allowed us to gain unauthorized access to NAU's internal network, which could have allowed us to potentially view, modify, or delete sensitive student information. Information security awareness training is important for reducing successful social engineering attacks. Although each university requires their employees to complete some security awareness training, not all university employees have done so. Specifically, as of March 2018, training completion rates were 68 percent at ASU, and as of April 2018, 61 percent at NAU, and 40 percent at UA. The lack of completed training at all three universities may have contributed to employees' susceptibility to simulated social engineering attacks.

Universities' security controls slowed simulated attacks, but vulnerabilities allowed unauthorized access to some IT systems and sensitive data—We conducted simulated attacks on the universities' IT systems, but our ability to gain unauthorized access to these systems was limited because the universities employ automated security tools and have separated portions of their respective networks into smaller, protected subnetworks. However, after ASU removed some controls to allow us to more quickly identify and exploit vulnerabilities, we gained unauthorized access to sensitive data at ASU, including names, contact information, and grades. At NAU, we identified some vulnerabilities that allowed us to gain unauthorized access to legally protected data such as records related to medical issues. We also exploited vulnerabilities to gain unauthorized access to some IT systems and sensitive data at all three universities that could have led to university service disruptions and further attacks. For example, we gained the ability to enter and void transactions at a cash register at ASU, take control of an IT system that manages some water and electrical services at NAU, and upload malicious software to financial and administrative systems at UA. Although all three universities have established policies and procedures for five key IT security controls that help prevent or detect unauthorized access to IT systems and data—vulnerability management, configuration management, patch management, web application development, and log monitoring—weaknesses in these IT security controls contributed to the vulnerabilities we identified and exploited.

Recommendation

ASU, NAU, and UA should improve their security awareness training compliance and enforcement policies and procedures and, where appropriate, further strengthen and align their existing IT security policies and procedures with IT standards and best practices for vulnerability management, configuration management, patch management, web application development, and log monitoring.

NAU and UA should continue to improve and develop IT security governance frameworks and ABOR should enhance its IT security governance by expanding its oversight activities

NAU and UA can improve IT security governance frameworks—IT standards and best practices indicate that organizations should develop an IT security governance framework that includes several components, including an IT security strategic plan, documented roles and responsibilities, policies and guidance, and processes for monitoring the effectiveness of institutional IT security practices. ASU has developed an IT security governance framework that includes all four recommended components, whereas NAU has developed three of the four recommended components and UA has developed two of the four recommended components. However, some of the framework components developed by NAU and UA are not fully aligned with best practices.

ABOR can enhance its IT security governance by expanding oversight activities—Higher education governing boards play an important role in ensuring universities' IT security risks are adequately addressed by providing oversight. Although ABOR provides some IT security guidance and oversight to the universities, its oversight efforts do not include several recommended practices for providing effective IT security governance. Implementing these practices may have helped ABOR and the universities identify and address several of the IT security issues we identified.

Recommendations

NAU and UA should either continue developing or develop and implement IT security governance frameworks.

ABOR should expand its oversight of the universities' IT security efforts using existing processes.

Universities should improve processes in three key information security program areas

Although each university has either wholly or partially implemented appropriate data classification, risk assessment, and incident response processes, which are important for adequately protecting their IT systems and the data contained in them, each university should take steps to improve in one or more of these areas. For example, ASU's data classification policies and procedures do not include a requirement for its individual colleges, departments, and other business units to develop a data inventory as part of its data classification process; NAU has not yet implemented its data classification policies and procedures; and UA's data classification policy also does not include a requirement for individual units to develop a data inventory. Additionally, NAU and UA have not fully implemented their IT risk assessment policies and procedures. Finally, NAU's and UA's incident response policies and procedures do not include information about training or testing as recommended by IT standards and best practices.

Recommendation

Where appropriate, ASU, NAU, and UA should revise or develop and implement policies and procedures for data classification, risk assessment, and incident response.

A copy of the full report is available at: www.azauditor.gov | Contact person: Jeff Gove (602) 553-0333