

How Secure is Higher Ed?

Why are half of all personal identity breaches in higher education? Will the decentralized structure of universities create additional vulnerabilities to information security breaches? How do you keep social security number use minimized and locked down where they are required? With limited budgets and competing initiatives, how does a university secure its critical identity information and institutional assets?

These are some common questions being asked by not only university CIOs, CSOs, and CISOs, but also by university presidents and provosts. Over the past two years there have been some very high profile security breaches at Universities. In December 2006, it was widely reported that hackers obtained personal information on approximately 800,000 students, faculty and staff members at a major university whose officials said the attack exposed records containing the names, Social Security numbers and birth dates. This incident received the most press, but there have been hundreds of similar incidents across the United States where higher education institutions have suffered identity and security breaches costing them millions of dollars and damaging their reputations.

Higher education institutions possess some of the richest identity data available to skilled hackers. The value of the identity information at a University is similar to information at a financial services organization – college students are the present and future consumers of America. What makes universities more attractive to malfeasance is that they typically have fewer safeguards to protect identity due to their organizational structures, less available budget, and their population is less aware of identity theft risks. A key reason for the high number of incidents in higher education is due to the open and decentralized environment of universities; essentially, the same features that are necessary to promote education and research also invite malicious activity. Due to the inability of universities to centralize and lock down their infrastructure, the measures and approaches utilized by corporations to meet governmental compliance standards prove ineffective within Higher Education. However, effective application of technology and leverage of industry best practices can allow institutions to maintain their collaborative and decentralized environments while also protecting their assets from malicious as well as inadvertent breaches.

A Roadmap to Campus Security

In order to create a reliable, enterprise wide identity management and data security infrastructure, a university must take a long term view of the problem and identify near term building blocks to reach their goals. They must develop a roadmap to campus security that examines a higher ed environment, applies security and compliance best practices, and develops recommendations for a roadmap that will enable the institution to prevent a security breaches and stop them from becoming the next headline.

In order to develop a comprehensive identity management and data security strategy, several areas must be investigated, including:

- Governance and Compliance – Critical review of institution policies and procedures and conformity to US regulatory and privacy standards, such as HIPAA, Gramm-Leach-Bliley, FERPA, HIPAA, PCI, Sarbanes-Oxley, etc.
- Enterprise Identity Management – Developing a solution architecture for an enterprise identity management framework consisting of:

- Access Management – Role-based access control policies and processes.
 - Authorization & User Management – Creation and management of identities, including account provisioning, on-going maintenance of the users' access rights, role changes, passwords and accounts, and de-provisioning.
 - Privacy Management – Policies, processes and standards that ensure compliance with relevant privacy regulation and institution security policies.
 - Role Management – Rationalization and efficient management of university roles and the fluid nature of roles.
- Enterprise data and information security assessment, including:
 - Data Security – Review of institution information stored in university databases.
 - Database Security – Identification of risks associated with database configuration and deployment, and effective leverage of database security features and functionality for the proper protection of information and compliance to policy and legislation.
 - Unstructured Data Control – Effective strategies at analyzing and controlling sensitive information that resides outside of databases – file servers, desktops, laptops, wikis, etc.

Oracle Corporation has developed a Roadmap to Campus Security which provides higher education institutions with an enterprise-architecture-level roadmap. The Oracle Roadmap has been developed by leveraging industry standards such as the IT Compliance Institute's Unified Compliance Project, EduCause, NMI-EDIT, Internet2, as well as others. The process includes a thorough review of business requirements, current security policies, current and planned security initiatives, and comparison to industry standards. The Roadmap assesses and balances risks, threats and vulnerabilities enabling an institution to determine where improvements or changes to its security architecture may be necessary and where further analysis is desirable. A critical component of the Roadmap is effective engagement of both business and enterprise IT management and staff to assist in developing a comprehensive and cost-effective overall strategy for maintaining information and identity security. A specific example of a frequently recommended initiative from this process is implementing a "SSN Vault" strategy at the institution to protect from improper release of highly sensitive data such as Social Security number.

Although each Higher Education environment is ultimately unique, a Roadmap to Campus Security will provide a path to an optimized identity and information security architecture in order to minimize risk of a security breach. This is achieved by identifying and prioritizing areas of maximum potential and providing innovative ideas for security improvement that are mapped to specific business goals and objectives resulting in near term and long term strategies. As a result, many higher education institutions are in the process of implementing Roadmap to Campus Security recommendations today.

"Please pass along our thanks to the Oracle team for their fine work on the Security Management Workshop. They did a very good job of synthesizing our comments and concerns into an actionable set of recommendations that will greatly improve the security of Caltech's administrative systems. We truly appreciate the efforts in making this happen." -- Rich Fagen, Chief Information Officer, California Institute of Technology

Richard Schad, Jr. is a Senior Director for Higher Education Technology Solutions at [Oracle Corporation](http://www.oracle.com). He can be reached at mailto:richard.schad@oracle.com?subject=INQUIRY:Campus_Technology.

For more information on data security and identity management, go to <http://www.accelacommunications.com/microsite/oracle/dws.html>

Oracle Corporation
500 Oracle Parkway
Redwood Shores, CA 94065

To unsubscribe from future mailings please email: unsubscribe@oracle-mail.com