

Universities Struggle with Information Technology Security & Confidentiality

Brendan Guenther

Michigan State University

FS06-EAD991B-001

Abstract

The decentralized organizational structure and varied goals of most universities present unique challenges for ensuring the security of information systems. Because of universities broad exposure to their constituents, community, and customers they collect an incredible volume and variety of data often longitudinally. Individuals divulge sensitive and private data to universities, while government legislation regulates and protects much of the data collected and retained. Since universities continue to consolidate their data and cross-reference data stores, the risk of data loss increases. Because of rising consumer awareness and increased media coverage, there is tremendous external pressure to ensure confidentiality of sensitive data. A breach of confidentiality resulting from poorly secured information technology holds consequences such as damage to institutional reputation, soured relationships with key institutional stakeholders, and even reduction in institutional autonomy.

To confront these risks institutions need to respond to the external expectations and confront the reality that presently most universities are failing to protect data adequately. Recognizing shortcomings, institutions must evolve practices and organizational structure to mitigate these confidentiality concerns. To do so universities must confront their unique characteristics and the evolutionary path of their technology development. This paper will consider these issues and combine suggestions from leading practitioners in risk management, information technology security, and privacy protection. Institutions should enact reforms that honor their core values and remain conscious of the way a university works while aiming for systemic changes to ensure confidentiality and security.

Context of Organizational Structure and Character

Information technology security presents an interesting challenge to most higher education administrators because it exists in extreme tension with traditional values of many institutions. Openness, privacy, freedom are words traditionally associated with the American university (Birnbaum, 1988). Closed, monitored, and restricted are terms common to the security field. When looked at from the traditional business-oriented perspective held by corporate auditors, higher education appears to be vulnerable perhaps to the point of incompetence or negligence (Conner & Coviello, 2004). Baldrige, Curtis, Ecker, and Riley (1977/1999) describe universities to have several distinguishing characteristics. Among them “goal ambiguity”, “client service”, and “environmental vulnerability” are particularly challenging to providing a secure technology infrastructure that protects confidentiality. In other words, universities attempt to be many things to many people, while interfacing with a large diverse set of clients holding a voice in decision making, while struggling to sustain their autonomy from external influences. The decision-making structure, varied goals, and constrained resources found in most universities create conditions in which information security is difficult to achieve yet critically important to institutional reputation (Cate, 2006).

Because of universities broad exposure to their constituents, community, and customers they collect an incredible volume and variety of data often longitudinally. Individuals divulge sensitive and private data to universities, while government legislation regulates and protects much of the data collected and retained. Since universities continue to consolidate their data and cross-reference data stores, the risk of data loss increases. Institutions need to confront the reality that most universities are presently failing to protect sensitive data adequately. Recognizing shortcomings, institutions must evolve practices and organizational structure to

mitigate these confidentiality concerns. Institutions should enact reforms that honor their core values and remain conscious of the way a university works while aiming for systemic changes to ensure confidentiality and security.

Increasing Sensitivity

Cyber-crime and identity theft increasingly headline news stories. Businesses, government agencies, academics, and non-profit groups increasingly target consumers with information on how to protect themselves (Privacy Rights Clearinghouse, 2006). Clients of the university, aware of the risks universities expose them to, have filed class-action lawsuits against institutions in response to confidentiality breaches (Foster, 2005; Wasley, 2006;). Universities are responsible for almost a third of recently disclosed losses of sensitive personal data. (Privacy Rights Clearinghouse, 2005). Increasingly universities are also falling under the constraints of legislation designed to protect privacy and hold organizational stewards of data accountable. Several states have added legislation requiring full disclosure of data loss in addition to federal regulations that affect data sensitivity and information technology (Adler, 2006; Holub, 2003; Foster, 2005;).

Because of increased sensitivity to privacy and the decision-making influence held by clients of universities, conditions are ripe for security problems to lead to exposure of sensitive data leading to a full-blown public relations crisis. Privacy and computer related risks are among the top 10 most significant risks facing universities (Mitroff, Diamond, & Alpaslan, 2006; Query, 2001;). Indeed, recent events at Ohio University led to an uproar amongst students, parents, lawmakers, and alumni. The repeated lapses in security and related scandal resulted in the dismissal of two information technology administrators and the resignation of a high-level administration figure (Wasley, 2006). The evidence cited justifying these actions and

assignment of blame to network administrators derives from corporate models of networks, security, and information technology funding not entirely relevant to universities. Many universities share the traits and characteristics of Ohio University and remain fundamentally exposed to a similar risk of criticism.

Contrasting views of Universities and Business

Businesses expect to expend resources as needed to build infrastructure and mitigate risks. Businesses can choose a cash flow management strategy to allow for shifting needs and large infrastructure expenditures to ensure security. Universities on the other hand, face a limited flexibility of funds, with the vast majority of their income already allocated to specific purposes (Birnbaum, 1988). To fund new initiatives, especially in the administration, Universities routinely accrue their limited flexible resources to save for large expenditures in future years. Furthermore, where business can shift resources across the whole organization by executive action, the university administration only holds partial decision-making authority with many resources committed to decision making at a college or departmental level.

Furthermore, universities have experienced an evolution of technology adoption and uptake that differs from the norm outside of academia and results in significant implementation challenges for security. Conditions exist routinely within universities that other types of organizations consider dangerous (Boes et-al, 2006). Universities pioneered development of computer internetworking and remain at the cutting edge of internet technology (Decker & Neas, 2003). Businesses require modest internet bandwidth and secure their network to the extreme, blocking all traffic that is not required. Universities and researchers meanwhile require enormous bandwidth, to the extent that they can usually only block traffic they know to be

malicious. Internally such decisions seem sensible while externally the situation, decisions, and personnel responsible seem very questionable.

In addition to holding unique characteristics that make universities very complex, they also organize bureaucratically in a decentralized manner. While many businesses operate in functional hierarchies, universities consist of many autonomous departments with duplicative structures (Birnbaum, 1988; Mallon, 2004). McCredie (2006) cites Weill and Ross (2005, p. 26) that in corporations “just one in three senior managers knows how IT is governed in his company”, noting that higher education’s problems are not unique. Universities do tend to have a more complicated set of organizational structures and relationships. McCredie (2006) describes several locations where Information Technology (IT) resources tend to be located at universities: independent research projects; departmental computing organizations; colleges and professional schools; campus-wide organizations; system-wide coordination; national and regional organizations. McCredie goes on to explain the “gaps and overlaps” effect of this distribution: “the inevitable result is that overlapping, wasteful services are developed while important services remain underfunded or inadequately resourced as a result of a lack of campus-wide coordination.”(p. 7) Autonomy exercised departmentally, institution-wide and between institutions leads to university level paralysis on critical security practices and policies.

Developing a Path Forward

Evidence suggests that many universities are beginning to respond to the threat environment and take steps to mitigate confidentiality concerns. EDUCAUSE members took the unprecedented step of listing security as it’s top IT priority relative to “strategic importance to the institution” (Dewey, DeBlois, & EDUCAUSE Current Issues Committee, 2006). A recent ECAR research study by Kvavik and Voloudakis (2006) indicates that while organizational

change has been slow to take hold, many institutions are implementing technology aimed at mitigating security threats. Cate (2006) recommends that institutions move beyond technology solutions and implement a five steps approach to improving the situation:

- Take privacy and security seriously
- Develop practical tools for considering privacy in all activities
- Clarify purpose of using personal data with uniform institutional policies
- Create privacy and security czars reporting to presidents and governing boards
- Join and lead debate over government and industry access to personal data.

Steinfeld and Archuleta (2006) support the strategy of appointing a Chief Privacy Office (CPO) to oversee legal compliance and appropriate use of data. They describe the critical factors for successful privacy management to be senior management support, the skill set and organizational placement of the privacy professional, strategic partnerships and collaboration. Ideally, a CPO would work closely with an organization's Chief Security Officer (CSO), the information technologist responsible for implementing a comprehensive security plan for an institution. Peterson (2006) describes the CSO role as difficult to develop and properly implement in higher education because of the disdain for creating executives and the unclear lines of communication among IT staff. Voludakis (2006) and Peterson (2006) both find that although CSOs are comfortable with technology and have the authority to implement technology solutions, they must also focus on people and process to achieve significant results. Creating new positions, rather than adding responsibilities to existing staff, encourages the development of professionalism while ensuring adequate attention is devoted to these oversight roles.

Even if the university creates new roles to focus on security and privacy within an institution, the decisive work that determines whether security is sufficient to protect privacy

occurs all over the university by front-line staff. Practitioners and experts stress the importance of developing a unified framework that develops comprehensive policies with representation from across the institution (Adler, 2006; McCredie, 2006;). Many processes, practices, and routines will be disturbed in the process of reaching compliance with new policies. Local autonomy may suffer during the transition and departmental staff may inherit new responsibilities. If the ultimate goal remains greater awareness and understanding among all IT staff, institutions may rightly question why they should create new positions that report at such a high level. This may explain why some institutions have yet to appoint both a CPO and CSO or have instead chosen to distribute these responsibilities among existing staff. However, ECAR data measuring organizational structure between 2003 and 2005 shows that, due to the increased importance of security, institutions are moving responsibilities towards CSOs (55% rate of change) and Chief Information Officers (113% rate of change) from lower level positions (Kvavik et al., 2006).

Given the number of distinct organizational cultures that exist within universities, practitioners in CPO or CSO positions should consider the literature on organizational change. Keup, Walker, Astin, and Lindholm (2001) provide a good overview of literature related to the readiness, resistance, and responsiveness of organizational sub-cultures in reaction to new initiatives. Expect that some elements of an institution will initially resist or ignore a campus wide security or privacy initiative. In the academic environment, CSOs and CPOs must focus on building relationships and understanding while allowing local autonomy to adopt campus wide confidentiality protection initiatives.

Conclusion

Under pressure from external expectations university governance becomes less collegial and depends more on centralized administration based on management ideas borrowed (perhaps improperly) from the business world (Waugh, 2003). Many universities are already grappling with adjustments to shared governance as described by Gayle, Tewarie, and White (2003) and subsequently illustrated in their case study of George Mason University. Inability to provide proper protections for sensitive data and information technology provides critics of traditional university decision-making evidence supporting the need for reform, favoring corporate models or governmental regulation. Cate (2006) notes that if universities “do not figure out how to behave responsibly towards personal data, and how to demonstrate that fact convincingly and publicly, the government is likely to do the job for us.” Adequately facing this challenge may require relational and structural changes to correct the disjointed decision making and authority within institutions related to data privacy and security. Universities have an ethical responsibility to their clients to provide confidentiality and an imperative to act if they wish to preserve their reputation, core values, and academic decision-making autonomy. Acting proactively, before a serious breach occurs, allows institutions to choose strategies and solutions that fit their local culture and organization instead of having solutions imposed from external forces. Regardless of the degree to which universities conform to expectations, constituents will judge results on absolute terms. Did a breach occur? Did you lose my private information?

References

- Adler, P. M. (2006). A Unified Approach to Information Security Compliance. *EDUCAUSE Review*, 41(5), 46-59.
- Baldrige, J. V., Curtis, D. V., Ecker, G. P., & Riley, G. L. (1999) Alternative Models of Governance in Higher Education. In J. L. Bess & D. S. Webster (Eds.), *Foundations of American Higher Education* (pp. 483-498). Boston: Pearson Custom Publishing. (Reprinted from *Governing Academic Organizations: New Problems, New Perspectives*, edited by G. L. Riley & J. V. Baldrige, 1977, McCutchan Publishing Group).
- Birnbaum, R. (1988). *How Colleges Work: The Cybernetics of Academic Organization and Leadership*. San Francisco: Jossey-Bass.
- Boes, R., Cramer, T., Dean, V., Hanson, R., & McKenna, N. (2006). Campus IT Security: Governance, Strategy, Policy, and Enforcement. *Educause Center for Applied Research Research Bulletin*. 2006(17). Retrieved 9/20/2006 from: http://www.educause.edu/ir/library/pdf/ECAR_SO/erb/ERB0617.pdf
- Cate, F. H. (2006). The Privacy and Security Policy Vacuum in Higher Education. *EDUCAUSE Review*, 41(5), 19-28.
- Conner, F. W., Coviello, A.W. (2004). Information Security Governance: A Call to Action. *National Cyber Security Partnership Corporate Governance Task Force Report*. Retrieved 9/20/2006 from: http://www.cyberpartnership.org/InfoSecGov4_04.pdf
- Decker, B., & Neas, B. (2003). Research Universities and the Central IT Organization: Rebuilding the Partnership. *EDUCAUSE Review*, 38(3), 12-22.
- Dewey, B. I., DeBlois, P. B., & EDUCAUSE Current Issues Committee. (2006). Current IT issues survey report, 2006. *EDUCAUSE Quarterly*, 29(2), 15.

- Foster, A. L. (2005). When Databases Leak. *The Chronicle of Higher Education*, 52(17), A.31.
- Gayle, D. J., Tewarie, B., & White, Q.A., Jr. (2003). Governance in the Twenty-First-Century University. *ASHE-ERIC Higher Education Reports*, 30(1).
- Holub, T. (2003). *College Student Records: Legal Issues, Privacy, and Security Concerns*. (Report No. ED480467). Washington, DC: ERIC Clearinghouse on Higher Education. (ERIC Document Reproduction Service No. ED480467)
- Keup, J. R., Walker, A., Astin, H. S., Lindholm, J. A. (2001). *Organizational Culture and Institutional Transformation*. (Report No. ED464521). Washington, DC: ERIC Clearinghouse on Higher Education. (ERIC Document Reproduction Service No. ED464521)
- Kvavik, R. B., Voloudakis, J. (2006). Safeguarding the Tower: IT Security in Higher Education 2006. EDUCAUSE Center for Applied Research (2006). Retrieved 12/1/2006 from: <http://www.educause.edu/ers0606>
- Mallon, W. (2004). Disjointed governance in university centers and institutes. *New Directions for Higher Education*, 2004(127), 61-74.
- McCredie, J. (2006). Improving IT Governance in Higher Education. *EDUCAUSE Center for Applied Research Research Bulletin*. 2006(18). Retrieved 9/20/2006 from: http://www.educause.edu/ir/library/pdf/ecar_so/erb/ERB0618.pdf
- Mitroff, I. I., Diamond, M. A. , & Alpaslan, C.M. (2006). How Prepared Are American Colleges and Universities for Major Crises? *Change*, 38(1), 60-67.
- Query, J. T. (2001). Managing Risk on College Campus. *Risk Management on College Campuses*, 48(6), 38-43.

Petersen, R. Safeguarding Information Assets in Higher Education: The Role of the CSO.

EDUCAUSE Review, 41(5), 72-82.

Privacy Rights Clearinghouse. (2005). *A Chronology of Data Breaches*. Retrieved 12/04/2006

from: <http://www.privacyrights.org/ar/ChronDataBreaches.htm>

Privacy Rights Clearinghouse. (2006). *Fact Sheet 29: Privacy in Education*. Retrieved

12/05/2006 from: <http://www.privacyrights.org/fs/fs29-education.htm>

Steinfeld, L., & Sutherland Archuleta, K. (2006). Privacy Protection and Compliance in Higher

Education: The Role of the CPO. *EDUCAUSE Review*, 41(5), 62-70.

Voloudakis, J. (2006). The Continuing Evolution of Effective IT Security Practices. *EDUCAUSE*

Review, 41(5), 30-44.

Waugh, W. L., Jr. (2003). Issues in University Governance: More "Professional" and Less

Academic. *The Annals of the American Academy of Political and Social Science*, 585(1), 84-96.

Wasley, P. (2006). 'More Holes Than a Pound of Swiss Cheese' Computer-protection problems

at Ohio U. spark complaints from alumni – and firings. *The Chronicle of Higher Education*. 53(6) pA39.

Weill, P., & Ross, J. (2005). A Matrixed Approach to Designing IT Governance. *MIT Sloan*

Management Review, 46(2), 26-34.