Association for Information Systems
AIS Electronic Library (AISeL)

SAIS 2012 Proceedings

Southern (SAIS)

2012

Higher Education Leaders' Roles in Access Security Management

Lisa J. Stamper
Georgia Southern University, ls02524@georgiasouthern.edu

HIGHER EDUCATION LEADERS' ROLES IN ACCESS SECURITY MANAGEMENT

Lisa J. Stamper
Georgia Southern University
lisa_j_stamper@georgiasouthern.edu

ABSTRACT

Technology transformed the paper world in which FERPA was initiated. Access to student records extends beyond the Registrar's Office, but the Registrar is typically the compliance officer. Policies and procedures need to match the expanse of electronic access. Senior management is often unfamiliar with, but accountable for, the safe-keeping procedures of identity information. To reduce the gap between unfamiliarity and accountability, this two-phase, sequential mixed methods study will investigate the role of higher education leaders in the management of security for access to identity information. The first phase will be a qualitative analysis of interview responses from security experts about the expected role. Survey statements developed from the interview responses will be rated on a Likert scale by Georgia higher education leaders in the quantitative second phase. A comparison of the analyzed results with a framework may help leaders with practical applications of their role toward effective access security management.

Keywords

Higher education leadership, information security, FERPA, ERP, Personally identifiable information (PII), identity management (IdM)

INTRODUCTION

In 1990, I accepted a new teaching position. The principal was passionate about the potential of technology in instruction. She hired me because of my interest and use of technology in the classroom. The job interview was almost completely focused on the power of technology in the classroom so I assumed the principal was a skilled computer user. A few days in to the school year I happened by the office and saw her re-typing a letter from a hard-copy. I asked her why she could not just pull up the old one, make the edits, and print. She was ecstatic at the concept and wanted to know more about how to recover documents she had previously typed. After asking where she kept her disks for saving data, I learned she had never saved a document. She was using the word processing software like a typewriter. She typed and printed. She used the same procedures with a word processer that she had with a typewriter with a few adaptations. Although the process was functional, it was costly in time and energy. The return of investment for the computer and software was, at most, minimal and the benefit to the school community was reduced since effort that could have been spent on innovative projects was being invested in the propagation of mundane paperwork. Similarly, higher education leaders cannot think that minor adjustments to identity information security policies and procedures that were set in place in the paper-based records world of 1974 for FERPA compliancy will be effective today in a society of electronic Internet access.

BACKGROUND

To understand the need for comprehensive renovation of procedures and policies, one must realize the disparaging differences between the world when FERPA was enacted, 1974, and now, 2012, as well as the evolutionary adaptations that have happened consequently.

The Family Educational Rights and Privacy Act of 1974 gave American students three basic rights in respect to their educational records (FERPA, 1974). Students gained the right of ACCESS - to inspect, review, and access education records. Students also received the right of CONTROL - to challenge the content of education records, and students gained the right of CONSENT - to allow disclosure of education records to others (US DOE, 2011). Most significant amendments to FERPA over the years have had to do with the release of information in reference to criminal investigations; although, in 2008, there was added information on how to handle some access to electronic records according to FERPA. The ruling was not specific and depended on the words, "reasonable methods" (Federal Register, 2008).

When FERPA was originally enacted, personal computing was in its infancy and it took another decade and a half before the Internet was available for commercial use. Student records in higher education institutions were physically housed in locked filing cabinets or vaults in the Registrar's Office. The users of the student records worked in the Registrar's Office and, at that time, it made sense for the Registrar to be the FERPA compliance officer on most campuses (McConahay, Hanson, West and Woodbeck, 2009).

From Paper to Personal Computer (PC)

Two decades ago, higher education institutions began the move from paper to electronic records on local databases. Then databases became available on the school network. The Internet, originally created to share computer resources by long-distance in support of research by the US government and higher education (Sterling, 2001), then enabled the access of identity information via Web accessible Enterprise Resource Planning (ERP) database systems (Impagliazzo, 2004). In 1974, the Registrar personally worked with everyone who had access to identity information and managed who had access. The records were only available during office hours. Now, access is usually available any time, any day, from any remote location around the world via the Internet. There are many more users with access and the access configuration changes frequently with new hires, terminations, and transfers. Often databases interface with other databases and that access must be managed too (Krempl, 2006).

IT Involvement Increased

Student records are the foundation of the higher education institution. A university's financial, administrative, and research systems as well as medical records, Human Resource records, other intellectual property-related records and, of course, student records are accessible through the campus network. Exposure of confidential information places institutions at not only legal risk, but baring the costs of resources and reputation as well (Rasmussen, 2011).

Although the Admissions Office will create and handle records first along with the Financial Aid and Housing Offices, the Registrar's Office will maintain the records from the matriculation of the first class through graduation and thereafter as well. The advent of electronic records aids processing speed and reduces the storage space needed considerably. Moreover, electronic records enable the ability for many people to read the same record at the same time. Access to important information is no longer bottlenecked to the one folder in the Registrar's vault. Therefore, the role of IT has increased in importance to data security.

Initially, electronic data access was a generic login to local databases. Then security became more individualized and personnel specific; therefore, users were given unique logins. Later, access limited, customized logins allowed users to see only specified screens or database forms. Present day users are now assigned a role in the database based on their job title (Suess and Morooney, 2009). Users are sometimes only allowed access to parts of fields such as the date and month from the date of birth or the last four of the Social Security Number. These roles are requested by the data steward (Registrar, Bursar, Directors of Admissions, Financial Aid, etc.) in a narrative form to the database administrator. The database administrator recreates what the data steward explains by grouping objects into classes and classes into a role in the software. Some scripting or programming may be required. The role is then assigned to users by IT personnel. Other department directors and IT have become more and more involved even though compliancy still remains the responsibility of the Registrar (McConahay et al., 2009).

In 2008, there were updates to FERPA in respect to electronic access, but an analysis of the amendments indicated data stewards may not be sure how to operationalize the mandates even with the increased involvement of IT. Many electronic student record systems enable all school faculty and/or officials unrestricted access to all records. The 2008 update states that only those with "legitimate education interests" for each record should have access. "Institutions themselves have expressed uncertainty about what methods they should use to comply with this requirement when establishing or upgrading their recordkeeping systems" (U.S. DOE, 2008, Controlling access section, para. 1).

Communication Between Campus Departments Diffident

ERP vendors assure higher education leaders that identity information can be secure and that FERPA compliancy is possible, but the set up of the structure is open. Each school has to establish the classes and roles that will be used and that customization costs labor and resources (Grayson, 2010; Hughes and Beer, 2007). In an EDUCAUSE access security baseline survey sent to primarily Chief Information Officers (CIOs) of member institutions, the responders rated that security was very important, but the participants also marked that the capability for security was much lower. There is a gap between what can be done with security and what needs to be done. In the same survey, 56 percent indicated that their senior management did not understand the costs of identity management. Also, the 'Don't know' response was pervasive and indicated that the baseline offers lots of opportunity for improvement (Yanosky and Salaway, 2006).

Additionally, although academicians are interested in keeping identity information secure, they are far more adamant in access to information since it is in their very nature to pursue knowledge (Titus, 2008). Developing a cooperative campus-wide framework for generating access management policies and procedures according to Srinivasan (Komanduri, 2008) is "…a basis for vital understanding between business management and technical managers of all identity management initiatives" (p. 84). The crux of the matter seems to be communication. Security and risk management is a language with which business leaders are not familiar. Business leaders also communicate through financial facts and figures that security professionals do not use on a daily basis (Wheatman, 2011). According to Wheatman (2011), this disconnect is a key risk where security is concerned.

Collaboration is Encouraged

Although no higher education institution has lost federal funding due to FERPA noncompliance (McDonald, 2008), in the annual survey to primarily CIOs of EDUCAUSE member institutions, respondents have ranked security within the top three of the ten most significant IT topics for over a decade. In fact, identity and access management was originally within the topic of security, but as of 2007, identity and access management became its own topic possibly due to increased significance reflecting the concern of education data breaches in the news. Also in 2007, 25% of the reported data breaches were from education which was second only to Business with 29% out of the five categories--Banking/Credit/Financial, Business; Educational, Government/Military, and Medical/Healthcare (ITRC, 2007). Keep in mind, there is currently no requirement for reporting a data breach so it seems likely there are more records exposed than are reported.

In 2008, identity and access management ranked fifth out of the ten most significant topics to IT leaders in addition to security in general (Allison, DeBlois, and EDUCAUSE, 2008). One harbinger, the President of EDUCAUSE urged higher education leaders to work together on identity and access management to avoid negative media including public terminations and lawsuits. Hawkins stated that there are high costs to being reactive rather than proactive as EDUCAUSE had propounded (2007). He also indicated that institutions that have an identity and access management plan in place save time, effort, and money in dealing with typical access management issues. The American Association of Collegiate Registrars and Admissions Officers (AACRAO) and EDUCAUSE have begun collaborating for resolution. AACRAO recommends including the expertise of the data stewards and indicates that policy and leadership are key. Even though governance is often behind technological advancements, having policies in place can ease access management issues even as they grow more complex (McConahay et al., 2009). Going even one step further is Elhindi's (2010) research from the IT perspective on how to set up an identity and access management system with cross-campus cooperation.

Training and Leadership Standardization

Georgia's Governor, Sonny Perdue signed an Executive Order (Exec. Order, 2008) as a step toward closing known security gaps. This order required that security job descriptions and the State audit reporting format be standardized. As a result, the Georgia Technology Authority (GTA) requested that The University System of Georgia (USG) create classes to teach security measures according to Federal Information Security Management Act (FISMA) including information security job requirements. According to the GTA, the idea behind security and security leadership training is to standardize understanding and expectations ("Georgia," 2010). There are six classes that focus primarily on the responsibilities and efforts of the Information Security Officer (ISO) which is a position normally under the Chief Information Officer (CIO) in the IT Department. However, at least three of the six classes are slated to invite both IT and non-IT participants including leaders and executives (SATE, 2011).

Another leadership position that would benefit from standardization is the Chief Information Security Officer (CISO). Although the majority of CISOs report to a Chief Information Officer (CIO) currently, there is some discussion about internal conflict of interest. Literature suggests that in order to truly represent and guide both the IT and non-IT leaders toward the best possible access security plan, the CISO needs to report to the Chief Financial Officer (CFO), the Chief Operations Officer (COO), or even the Chief Executive Officer (CEO) since risk ownership belongs to senior management ultimately (Harris, 2008; NASCIO, 2006).

Renovation on Campus

The move from paper to PC begs the renovation of organizations that manage identity information to match the transformation due to electronic access. Such dramatic changes to the higher institutional structure and environment create the need for the renovation of policies and procedures. In order to establish new policies and procedures to prevent and mitigate the wave of recent violent attacks on college campuses, the US Department of Education (US DOE) developed an action guide. The guide's purpose and its goals have much in common with the rationale for this study. Both affirm there is an obligation to provide safety for students. The Action Guide refers to physical safety, but the protection of identity information prevents bodily harm as well as fiscal and credential corruption by keeping home address, phone number, Social

Security number, etc. unavailable to those who have no need to access such information. The Action Guide states that environments have changed and require a thorough process to prepare for and manage emergencies on campus. Furthermore, the document explains that institutions of higher education (IHE) are unique organizations. The culture is open due to the nature of education, but the population is always changing and yet needs to be protected in spite of the independent attitudes of both students and faculty. Authority is not centralized; therefore, decision-making can be difficult and sluggish.

According to the Action Guide for Emergency Management at Institutions of Higher Education (2009, p. 3), "Effective emergency management begins with senior leadership on campus." Organizations are not likely to adapt themselves effectively to the changes that electronic access has caused without intervening leadership. Campus leaders who can actually transform business processes on campus are the individuals who need to be involved (Berg, Kraemer, Raatz and Devoti, 2009; Bradford, 2010). Leaders need to know more than just that security is needed (Yanosky and Salaway, 2006). ERP research shows that the better the coordination and task efficiency, the better the data quality and overall ERP benefits (Gattiker and Goodhue, 2005). Higher Education leaders need to know what their role is in access security management so that the policies and procedures essential to effective identity information protection can be established. Not unlike Emergency Management, planning requires collaboration, it must be comprehensive, and yet customized (DOE, 2009).

STATEMENT OF THE PROBLEM

Almost four decades ago, the Family Educational Rights and Privacy Act (FERPA) established the federal guidelines for the security of student identity information. However, technology has transformed completely the paper world in which FERPA was initiated. The 2008 update to FERPA recognizes electronic records and adds to the foundational policy (the need for security, but with access); however, many higher education leaders are not sure how to operationalize the amendments. Security is not a popular topic nor is the need easily communicated. Support from Information Technology has changed to a requirement. The users are no longer isolated to a physical location in the Registrar's Office, instead they are interconnected all over the globe. The number of users has increased exponentially and the security roles must be adapted with each hire, termination, and transfer; however, the Registrar, alone, is still considered the compliance officer. Access security management policies and procedures must be renovated as completely as the paper processes have converted to electronic processes. Change in institutions is effected by leaders. Higher education leaders need to understand their role in access security management in order to conduct the innovation needed. Senior management is accountable for the safe-keeping of student identity information. In order to reduce the gap between unfamiliarity and accountability, this study will investigate the role of higher education leaders in the management of security for access to identity information.

RESEARCH QUESTIONS

This study seeks to answer the overarching question as well as the sub-questions that follow: What is the role of higher education leaders in the management of security for access to identity information?

1. What is the role of USG higher education leaders in the management of security for access to identity information according to USG InfoSec and State DOAA security auditors?
2. What types of training, support, and/or learning resources are available for higher education leaders in reference to access security management?
3. What facets of the expected role are USG higher education leaders aware of and fulfilling?
4. What are the areas of the role with which USG higher education leaders are least familiar?
5. How could the United States Department of Education Action Guide for Emergency Management in Institutions of Higher Education help define the roles of leaders in access security manangement?

METHODOLOGY

According to Creswell (2007), Pragmatism focuses on practical implications of the research and uses both qualitative and quantitative methods. The intent of this two-phase, sequential mixed methods study is to investigate the role of higher education leaders in the management of security for access to identity information. The first phase will be a qualitative exploration of the expectations of higher education leaders in reference to the management of security for access to identity information according to USG information security experts and officials from the Georgia State Department of Audits and Accounts.(DOAA) Using a semi-structured interview form with questions about the role of higher education leaders in reference to job descriptions, performance outcomes, security leadership training, and support resources as well as Georgia's newly standardized security audit reporting procedures, the experts will describe role facets. The interviewees will be asked about how they believe the US Department of Education Action Guide on Emergency Management in Institutes of Higher Education can help define the role too. Interviews with University System of Georgia (USG) Information Security (InfoSec) representatives, and State (Georgia) auditors will be collected. After an analysis of the responses using the qualitative data analysis software called Atlas.ti, the interview responses will become an online survey for the second phase and distributed to higher education leaders in Georgia institutions. Higher education leaders with a classification on the level of Registrar or higher will be invited to participate. The leaders will rate the statements that describe the elements of the role of higher education leaders in the management of security for access to identity information according to their understanding of what their role should be using a 1-4 Likert scale. The survey results will be analyzed with SPSS software for possible relations and correlations to describe alignment with expectations and potential gaps. The results of the analysis will be compared to the DOE Action Guide for a practical frame of reference to help bring to light the facets of the role that leaders already fulfill toward renovation of data access security policies and to identify what they could do additionally to bridge potential gaps.

SIGNIFICANCE OF THE STUDY

Governor Sonny Perdue signed an Executive Order to strengthen Georgia's Information Technology Security (Executive Order No. 03.19.08.01, 2008). The order is an action toward closing security gaps and for providing a standardized State audit reporting format as well as a standardized understanding of information security job descriptions. However, only the job descriptions of information security positions were examined and taught for standardization. Security of access to identity information is paramount and will only increase as technology advances. Not just IT professionals, but Higher Education Leaders across campus, no matter if the campus is local or global, are responsible for the protection of student and employee identity information. This study is designed to be an initial effort of a non-IT complement of the Executive Order which includes the goal of supporting the standardizing annual State security audit reports. However, and most importantly, this study is an effort to improve the protection of identity information of each university's greatest resource--its students by describing the role the higher education leaders' role expectations according to experts, comparing the current perspective by non-IT USG leaders themselves, and encouraging the use of the US DOE Emergency Management Action Guide for practical examples of how to renovate policies and procedures from paper to electronic records' access.

LIMITATIONS

It has been mentioned that this study is severely limited by the fact that there have been minimal repercussions for data breaches of identity information by universities to date and that reporting of data breaches is not required. Although every higher education leader would probably state that security of student identity information is significant, it is likely that time and funding is directed to line items with a more pragmatic return of investment. It may be that the cost of a data breach at this time is cheaper than preventing one ("The Higher Ed CIO", 2012).

SUMMARY

Technology completely transformed the paper world in which FERPA was initiated. Access to student records extends well beyond the confines of the Registrar's Office and yet the Registrar, alone, is typically considered the compliance officer. Policies and procedures need renovation to match the expanse of electronic access. Senior management is unfamiliar with, but accountable for, the safe-keeping of student identity information. In order to reduce the gap between unfamiliarity and accountability, this two-phase, sequential mixed methods study will investigate the role of higher education leaders in the management of security for access to identity information. The resulting, extracted role will be compared with the U.S. Department of Education Action Guide for Emergency Management at Institutions of Higher Education. The comparison with the framework may help leaders know practical steps as part of their role toward effective access security management.

REFERENCES

1. Allison, D. H. and DeBlois, P. B. (2008) Current issues survey report, 2008, *EDUCAUSE Quarterly*, *31*(2). Retrieved from http://www.educause.edu/ir/library/pdf/EQM0823.pdf
2. Berg, J. E., Kraemer, R., Raatz, C. and Devoti, S. (Winter 2009) Building an identity management governance process: A case study. *College and University*, *84*(3), 20-25. Retrieved from http://www.aacrao.org/publications/members_only/winter2009.pdf
3. Bradford, M. (2010) Modern ERP: Select, implement and use today's advanced business systems (2nd ed.). Raleigh, NC: Lulu.
4. The Higher Ed CIO. (2012, February 14) College data breaches: The privacy hypocrisy of higher ed [Web log post]. Retrieved from http://blog.thehigheredcio.com/2012/02/14/college-data-breaches-the-privacy-hypocrisy-of-higher-ed/
5. Creswell, J. W. (2007) Qualitative inquiry and research design (2nd ed.). Thousand Oaks, CA: Sage Publications, Inc.
6. Elhindi, M. A. (2010) Design and development of an identity management system: The Minnesota State College-Southeast Technical case study. Minnesota State College-Southeast Technical, Winona, MN.
7. Exec. Order No. 03.19.08.01, Retrieved from http://gov.georgia.gov/vgn/images/portal/cit_1210/32/5/10933575903_19_08_01.pdf. (2008).

8. Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g; 34 CFR Part 99 (1974). Retrieved 04/17/2011 from http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html
9. Federal Register: Part II. (2008) Family educational rights and privacy; Final rule 34 CFR part 99 Department of Education December 2008. Retrieved from http://www2.ed.gov/legislation/FedRegister/finrule/2008-4/120908a.pdf
10. Gattiker, T. F. and Goodhue, D. L. (2005). What happens after ERP implementation: Understanding the impact of interdependence and differentiation on plant-level outcomes, *MIS Quarterly*, *29*(3), 559-585. Retrieved from http://www.jstor.org/ stable/25148695?origin=JSTOR.pdf
11. Grayson, K. (2010). Ready the pipes, *Campus Technology*. Retrieved from http://campustechnology.com/articles/2010/03/01/ready-the-pipes.aspx
12. Harris, S. (2008) All in one CISSP exam guide (4th ed.). New York: McGraw Hill.
13. Hawkins, B. (2007) What higher ed leaders need to know about IdM. *EDUCAUSE Review*, *42*(5), 84-85. Retrieved from http://www.educause.edu/EDUCAUSE+Review/EDUCAUSEReviewMagazineVolume42/WhatHigherEdLeadersNeedtoKnowa/161915
14. Hughes, J. R. and Beer, R. (2007) A security checklist for ERP implementations, *Educause Quarterly*, *4*, 7-10. Retrieved from http://net.educause.edu/ir/library/pdf/EQM0741.pdf
15. Identity Theft Resource Center (ITRC) (2007) *2007 Data Breach Stats*. Retrieved from http://www.idtheftcenter.org/artman2/uploads/1/ITRC_Breach_Stats_Report_20071231_1.pdf
16. Impagliazzo, J. (2004) A brief history of database systems, *Learning Computing History*. Retrieved from http://www.comphist.org/computing_history/New_page_9.htm
17. Komanduri, P. (2008) A framework for regulatory compliance concerning identity management in an educational institution. University of Houston, Houston, TX.
18. Krempl, S. (2006) Universities need lessons in IT security, *Infosecurity Today*, *3*(5), 24-26.
19. McConahay, M., Hanson, K., West, A., and Woodbeck, D. (Summer 2009). The electronic FERPA: Access in the digital age. *College and University*, *85*(1), 12-19. Retrieved from http://www.aacrao.org/publications/members_only/CUJ8501.pdf
20. McDonald, S. J. (2008) The family rights and privacy act: 7 myths – and the truth, *The Chronicle of Higher Education*, *54*(32), A53. Retrieved from http://chronicle.com/weekly/v54/i32/32a05301.htm
21. Rasmussen, R. (2011, April 28) The college cyber security tightrope: Higher education institutions face greater risks. Security Week: *Internet and enterprise security news, insights and analysis*. Retrieved from http://www.securityweek.com/college-cyber-security-tightrope-higher-education-institutions-face-greater-risks
22. Suess, J. and Morooney, K. (2009) Identity management and trust services: Foundations for cloud computing. *EDUCAUSE Review*, *44*(5), 24-43. Retrieved from http://www.educause.edu/blog/vvogel/IdentityManagementandTrustServ/179881
23. Sterling, B. (2011) Short history of the internet. *The Internet Society*. Retrieved from http://www.internetsociety.org/internet/internet-51/history-internet/short-history-internet
24. Titus, A. (2008 October 24) 5 key ways your electronic data may be at risk. *The Chronicle of Higher Education*, *55*(9), A35. Retrieved from http://chronicle.com/article/5-Key-Ways-Your-Electronic/18613
25. U.S. Department of Education (DOE). (2009) Action Guide for Emergency Management at Institutions of Higher Education. Retrieved from http://www2.ed.gov/admins/lead/safety/emergencyplan/remsactionguide.pdf
26. U.S. Department of Education (DOE). (2011) FERPA: A brief, annotated history. Retrieved from http://www.higheredcenter.org/thisweek/ferpa-brief-annotated-history
27. Wheatman, J. (2011 February 16) Why communication fails: Five reasons the business doesn't get security's message. Retrieved from http://www.gartner.com/DisplayDocument?id=1549927
28. Yanosky, R. and Salaway, G. (2006) Identity Management in Higher Education: A Baseline Study. EDUCAUSE: Center for Applied Research. Retrieved from http://www.educause.edu/ir/library/pdf/EKF/EKF0602.pdf