SAFEGUARDS FOR PROTECTING PRIVATE DATA - SERVICE PROVIDERS AND CONTRACTORS

THE UNIVERSITY OF NEW MEXICO

Report 2013-15
October 17, 2013

Audit Committee Members

J.E. "Gene" Gallegos, Chair
Lt. General Bradley Hosmer, Vice Chair
James Koch

Audit Staff

Manilal Patel, Internal Audit Director
Chien-Chih Yeh, Internal Audit Manager
Lisa Wauneka, Information Systems Auditor
Brandon Trujillo, Internal Auditor II

CONTENTS

ABBREVIATIONS

CIO	Chief Information Officer
COBIT	Control Objectives for Information and related Technology (Published by the Information System Audit and Control Foundation, IT Governance Institute)
Commission	Federal Trade Commission
FERPA	Federal Educational Rights and Privacy Act
FTC	Federal Trade Commission
GLBA	Gramm-Leach-Bliley Act
HSC	Health Sciences Center
Internal Audit	University of New Mexico Internal Audit Department
IT	Information Technology
UAPPM	University Administrative Policies and Procedures Manual
University	The University of New Mexico
UNM	The University of New Mexico

EXECUTIVE SUMMARY

The Federal Trade Commission (FTC) has determined colleges and universities are considered financial institutions under the Gramm-Leach-Bliley Act (GLBA) because these institutions are significantly engaged in lending funds to consumers. GLBA requires that financial institutions implement safeguards to ensure the security and confidentiality of personal information collected from customers, including names, addresses, phone numbers, bank account numbers, credit card numbers, income and credit histories, and social security numbers.

In response to these rules, the University of New Mexico (University) (UNM) developed University Administrative Policies and Procedures Manual (UAPPM) Policy 2550 – Information Security.

An audit of UNM's compliance with sections of the UAPPM Policy 2550 – Information Security is included on the Internal Audit Department's Fiscal Year 2013 Audit Plan. The audit is a review of service providers and contractors, and the process in place to monitor the University's Information Security Program.

Information Security Plan Coordinator and Program

The Chief Information Officer (CIO), main campus computing, has developed a UNM Information Security Program that includes the University Controller, the University Provost, and the CIO as the Information Security Plan Coordinators. The CIO needs to ensure the UNM Information Security Program is implemented. The CIO agreed with the finding and will implement the UNM Information Security Program.

University Information Security Function

The UNM information technology environment is based on a decentralized computing system model. The CIO is responsible for main campus enterprise computing systems. The CIO of the Health Sciences Center (HSC) is responsible for the Health Sciences Library & Informatics Center systems. Departments and branches of the University are responsible for their departmental computing systems. In the absence of a University-wide information technology security function, the University takes the risk that information technology security is implemented and managed inconsistently, depending on the organization in charge of the information technology system. This may lead to gaps in information technology (IT) security and may result in a breach. The President should give the CIO the explicit authority and responsibility to manage information security University-wide, including the decentralized computing services. The President should also ensure that the CIO has the budget to develop, implement, and enforce security policies.

Confidential Data Contracting and Security Review Procedures

The University Purchasing Department is responsible for reviewing prospective service providers and/or contractors to ensure they have and will maintain appropriate safeguards for protected information. The Purchasing Department identifies contracts that relate to confidential data. The Purchasing Department works with the subject matter experts such as the University Information Security Officer and the HSC Information Security Officer to ensure the confidential data is appropriately protected. The process is occurring, but the Purchasing Department has not developed written procedures.

CONCLUSION

The University of New Mexico is progressing toward full compliance with the GLBA. The purpose of the GLBA is to implement safeguards to ensure the security and confidentiality of personal information collected from customers. The University can accomplish this by implementing and monitoring an Information Security Program. The University also needs to put in place information security University-wide governance processes to ensure information security is included in the day-to-day operations of the University.

INTRODUCTION

BACKGROUND

Gramm-Leach-Bliley Act

The University is required to comply with portions of the GLBA. The University must comply with the Standards for Safeguarding Customer Information Safeguards Rule, effective May 23, 2003, but not with the Privacy of Consumer Financial Information Rule.

16 CFR Part 313 Privacy of Consumer Financial Information; Final Rule, published May 24 2000 Federal Register, p. 33648 states: "The Commission also received several comments from colleges and universities and their representatives requesting that institutions of higher education be excluded from the definition of financial institution. The Commission disagrees with those commenters who suggested that colleges and universities are not financial institutions. Many, if not all, such institutions appear to be significantly engaged in lending funds to consumers. However, such entities are subject to the stringent privacy provisions in the Federal Educational Rights and Privacy Act (''FERPA''), 20 U.S.C. 1232g, and its implementing regulations, and 34 CFR part 99, which governs the privacy of educational records, including student financial aid records. The Commission has noted in its final rule, therefore, that institutions of higher education that are complying with FERPA to protect the privacy of their student financial aid records will be deemed to be in compliance with the Commission's rule."

16 CFR Part 314, published May 23 2002 Federal Register, p. 36484 states: "The Federal Trade Commission (''FTC'' or ''Commission'') required by section 501(b) of the Gramm-Leach-Bliley Act (''G–L–B Act'' or ''Act'') to establish standards relating to administrative, technical and physical information safeguards for financial institutions subject to the Commission's jurisdiction. As required by section 501(b), the standards are intended to: Ensure the security and confidentiality of customer records and information; protect against any anticipated threats or hazards to the security or integrity of such records; and protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer."

There are no written guidelines for enforcement of the GLBA. The FTC relies on its own discretion when enforcing the GLBA.

The FTC has developed guidance for institutions to comply with the safeguards rule. The FTC publication Financial Institutions and Customer Information: Complying with the Safeguards Rule, published April 2006, states:

> "The Safeguards Rule requires companies to develop a written information security plan that describes their program to protect customer information. The plan must be appropriate to the company's size and complexity, the nature and scope of its

activities, and the sensitivity of the customer information it handles. As part of its plan, each company must:

- designate one or more employees to coordinate its information security program;
- identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks;
- design and implement a safeguards program, and regularly monitor and test it;
- select service providers that can maintain appropriate safeguards, make sure your contract requires them to maintain safeguards, and oversee their handling of customer information; and
- evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring."

In response to these rules, the University developed UAPPM Policy 2550 Information Security. Section three and four of the policy state:

"3. Compliance by Service Providers
Service providers and/or contractors who provide services that may allow them to access protected information must comply with the GLBA safeguard requirements, the University's Information Security Program, and applicable University policies listed in Section 6. herein. The University Purchasing Department is responsible for reviewing prospective service providers and/or contractors to ensure they have and will maintain appropriate safeguards for protected information.

4. Monitoring and Testing
The Director of Information Assurance will regularly monitor the UNM Information Security Program and periodically test the required and recommended safeguards. Based on these assessments, the Director of Information Assurance will work with all appropriate individuals to implement, correct, design, or improve safeguards.

The University Internal Audit Department will include as part of its routine audit procedures a review for compliance with the UNM Information Security Program. This review will include an evaluation of the effectiveness of controls, systems, and procedures. Any findings, discrepancies, and/or violations will be reported to the Director of Information Assurance who will investigate the problem and work with all appropriate individuals to develop a remedy."

PURPOSE

The purpose of this audit is to ensure the University is requiring service providers and contractors with access to protected information to comply with GLBA safeguard requirements, the University's Information Security Program, and applicable University policies. The audit will also ensure the University is regularly monitoring compliance with the UNM Information Security Program. This audit was included as part of the UNM Internal Audit 2013 Audit Plan.

SCOPE

Determine that written agreements with service providers and contractors include provisions to comply with GLBA safeguard requirements, the University's Information Security Program, and applicable University policies.

Review the process to ensure that service providers and contractors have and will maintain appropriate safeguards for protected information to determine it is working appropriately.

Review the Information Assurance process in place to regularly monitor the UNM Information Security Program and periodically test the required and recommended safeguards to ensure the Information Assurance process is working as designed.

Review IT best practices to ensure the University is managing the IT security function appropriately.

PROCEDURES

Our procedures included interviewing personnel, reviewing the contracting process between the University and service providers and contractors, reviewing contract provisions, reviewing documentation of the review of service providers' and/or contractors' safeguards for protected information, reviewing best practices for information technology security, reviewing federal regulations and University policies, and reviewing the UNM Information Security Program and monitoring process.

OBSERVATIONS, RECOMMENDATIONS AND RESPONSES

Information Security Plan Coordinator

The University Director of Information Assurance was designated as the Information Security Plan Coordinator. The Director of Information Assurance is a position that no longer exists. The University may not be in compliance with the GLBA without the required Information Plan Coordinator.

UAPPM 2550 – Information Security, issued June 1, 2008, Section 2.2 Information Security Plan Coordinator states: "The University Director of Information Assurance is designated as the Information Security Program Coordinator, a specific role required by the GLBA. This position is responsible for:

- Developing and implementing the UNM Information Security Program;
- Identifying risks to confidentiality, integrity, and availability of protected information;
- Designing and implementing appropriate safeguards;
- Evaluating the security program; and
- Making adjustments to reflect relevant developments or circumstances that may materially affect these safeguards, including changes in operations or the results of security testing and monitoring."

During the course of the audit, UAPPM 2550 – Information Security was updated to assign the Information Security Plan Coordinator position to the CIO.

UNM Information Security Program

The CIO developed the UNM Information Security Program, updated June 10, 2013, and published the program on the CIO's website. The University Controller, the University Provost, and the CIO are the Information Security Plan Coordinators.

UAPPM 2550 – Information Security states:

"2. UNM Information Security Program
The UNM Information Security Program is designed to protect the confidentiality, integrity, and availability of protected information; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of protected information that could result in substantial harm to any student, parent, employee, or customer of the University. This program includes the process for identification of risks and defines responsibilities for safeguarding information, monitoring the effectiveness of the safeguards, evaluating service providers, and updating the program itself. The UNM Information Security Program is published on the Office of Chief Information Officer (CIO) website."

Internal Audit interviewed the Associate Vice President, Division of Enrollment Management, because the Division of Enrollment Management operates a data center that contains sensitive student records. The Associate Vice President of the Division of Enrollment Management is aware of and knowledgeable about UAPPM 2550 – Information Security. He has not developed a GLBA policy for this division. His understanding of the policy was that it was the responsibility of the areas affected by the policy to adopt the plans included in the UNM Information Security Program. The Division of Enrollment Management worked with the Information Assurance Office, but there was never a concrete outcome from the meetings. Various sections of UAPPM 2550 – Information Security support the Associate Vice President, Division of Enrollment Management's statement that the areas were to follow the guidance provided by the Director of Information Assurance (now the CIO or the CIO designee).

UAPPM 2550 – Information Security states:

"2.5. Employee Management and Training
The success of the Information Security Program depends largely on the employees who implement it. The Chief Information Officer or designee will coordinate with deans, directors, and heads of departments that have access to protected information to evaluate the effectiveness of departmental procedures and practices relating to access to and use of protected information."

The effective implementation of the UNM Information Security Program is critical to University-wide Information Security. The University may not be in compliance with GLBA without the required Information Security Program.

Recommendation 1

The CIO needs to implement the UNM Information Security Program University-wide.

Response from the Chief Information Officer

Action Items
Targeted Completion Date: *30 days after the direction provided by the President.*
Assigned to: *CIO with direction from the senior administration via the IT Executive Council.*
Corrective Action Planned: *The CIO will continue implementation of the Information Security Program with the advisory structure approved by the President. The CIO submitted a recommendation to the IT Governance Council UNM Policy 2560 (President, EVPs, and Chancellor) to create a University wide security council. The existing and operational UNM Information Security Program will be assigned to the appropriate advisory structure.*

University Information Security Function

The UNM IT environment is based on a decentralized computing system model. The CIO, who reports to the Executive Vice President for Administration, is responsible for main campus enterprise computing systems. The CIO of HSC is responsible for HSC Library & Informatics Center systems, and departments and branches of the University are responsible for departmental computing systems. The President (departmental computing services for UNM Branches), the Provost & Executive Vice President for Academic Affairs (departmental computing services for Anderson School of Management, School of Engineering, Division of Enrollment Management…) and the Executive Vice President for Administration (departmental computing services for Financial Services, UNM Human Resources, UNM Bookstore, Parking and Transportation Services…) have departmental computing services under their organizations. The departmental computing services do not report to the CIO. As a result of the decentralized model and reporting authority, the CIO has had difficulties developing, implementing and enforcing security provisions for University-wide information security including GLBA compliance requirements.

Development of and enforcement of IT security policy should be supported at the highest level of management. COBIT 4.1 DS5.01 states "Manage IT security at the highest appropriate organisational *[sic]* level, so the management of security actions is in line with business requirements."

In the absence of a University-wide IT security function, the University takes the risk that IT security is implemented and managed inconsistently because the areas have developed different security standards. These security standards may not be sufficiently rigorous to protect University systems and data and may result in a breach. COBIT 5 illustrates the consequences of a breach. COBIT 5 for Information Security Executive Summary states:

> "Information security is essential in the day-to-day operations of enterprises. Breaches in information security can lead to a substantial impact within the enterprise through, for example, financial or operational damages. In addition, the enterprise can be exposed to external impacts such as reputational or legal risk, which can jeopardise *[sic]* customer or employee relations or even endanger the survival of the enterprise.
>
> The need for stronger, better and more systematic approaches for information security is illustrated in the following examples:

- A national critical infrastructure depends on information systems, and successful intrusions can result in a significant impact to economies or human safety.
- Non-public financial information can be used for economic gain.
- Disclosure of confidential information can generate embarrassment to enterprises, cause damage to reputations or jeopardise *[sic]* business relations.

- Intrusion in commercial networks, for example, to obtain credit card or other payment-related data, can lead to substantial reputational and financial damage due to fines, as well as increased scrutiny from regulatory bodies.
- Industrial espionage can enable trade secrets to be imitated and increase competition for manufacturing enterprises.
- Leakage of national or military intelligence can result in damage to political relationships.
- Personal data leaks can result in financial loss and unnecessary efforts to rebuild an individual's financial reputation.
- Significant unplanned costs (both financial and operational) related to containing, investigating and remediating security breaches can impact any enterprise that has suffered a breach."

Recommendation 2

The President should give the CIO the explicit authority and responsibility to manage information security University-wide, including the decentralized computing services. The CIO's responsibilities should include:

- Developing an organizational structure and reporting line for information security University-wide;
- Developing a process to prioritize security initiatives, including policies, standards, and procedures;
- Enforcing security and computing policies and standards; and
- Developing security management reporting to inform the board, operational management, and IT management of the status of information security.
- Completing an annual effectiveness evaluation of the UNM Information Security Program.

The President should also ensure that the CIO has the budget to develop, implement, and enforce security policies.

Response from the President

Action Items
Targeted Completion Date: *December 31, 2013*
Assigned to: *President's Office*
Corrective Action Planned: *We concur with this recommendation. Our office is working with the EVP for Administration, the Provost and EVP for Academic Affairs, and the Chancellor for Health Sciences on the appointment of an appropriate advisory structure.* *In regards to day-to-day University-wide IT security functions, the University currently has an Information Security Office within IT and a full-time Information Security Officer who reports to the CIO. We will work with the EVP for Administration and the CIO to evaluate whether this office has sufficient budget and authority to develop, implement, and enforce security policies. The Information Security Office, through the CIO, has established a security management reporting mechanism and makes quarterly reports to senior management on the status of information security at UNM.*

Confidential Data Contracting and Security Review Procedures

Internal Audit reviewed seven contracts with service providers or contractors that involve confidential data. In performing the review, Internal Audit noted departments requesting the purchase are not informing the Purchasing Department that the purchase may involve confidential data. The Purchasing Department buyers are making the determination that the purchase may involve confidential data based on their own knowledge and experience.

When the Purchasing Department identifies contracts that involve confidential data, they work with the subject matter experts such as the University Information Security Officer and the HSC Information Security Officer to ensure the confidential data is appropriately protected. The process is occurring but the Purchasing Department has not developed written procedures.

According to UAPPM 2550 Information Security Section 3 "The University Purchasing Department is responsible for reviewing prospective service providers and/or contractors to ensure they have and will maintain appropriate safeguards for protected information."

Purchasing may not be identifying all University contracts involving confidential information. If they do not identify these contracts, the information security review and the inclusion of contract clauses addressing confidential information may not be taking place.

Written procedures are used to establish what should be done, as well as how, when, and by whom. The procedures normally identify the step-by-step processes of how to implement and carry out the policy, including identifying the specific tasks and clarifying roles and

responsibilities. The procedures should be used to provide consistency in the processes, which can increase overall efficiency. Procedures can also be used to improve communications and establish strong internal controls for regulatory compliance. In addition, they can reduce the risk of confusion, the potential for litigation, and provide documentation for auditors and reviewers. During a staff transition, written policies and procedures are essential.

Recommendation 3

The Purchasing Department needs to work with the University Information Security Officer and the HSC Information Security Officer to develop written procedures for the review of service providers and contractors with access to confidential data. These procedures should include:

- Disclosure by the department requesting the purchase when the contracted service providers and/or contractors will have access to confidential data;
- Notification via a flag in the contract management system indicating the purchase involves confidential data; and
- Certification from the service provider or contractor that at the end of the contract period the service provider either returned or destroyed the University's confidential data.

Response from the Chief Procurement Officer

Action Items
Targeted Completion Date: *March 31, 2014*
Assigned to: *Chief Procurement Officer*
Corrective Action Planned: *We will work with the University Information Security Officer and HSC Information Security Officer to develop written procedures for the review of contractors with who have access to confidential data.* *Through policy and process, the Purchasing Department will work to identify a method in LoboMart for Departments to flag requisitions that provide vendors with access to confidential data. Purchasing staff will also be trained to investigate matters in which a purchase may grant vendors access to confidential information. Contracts that give vendors access to confidential data will be flagged when entered into Contract Director. We will look to enhance this process in the future as programming resources become available.* *Purchasing will also develop a process that will require the service provider to certify at the end of a contract that all confidential data is either returned to UNM or destroyed. The contract owner listed in Contract Manager will be responsible for obtaining this certification at the end of the contract. Purchasing will also modify our standard PO terms and conditions to require vendors to agree to this certification and destruction process.*

APPROVALS

Manilal Patel, CPA
Director, Internal Audit Department

Approved for Publication

Chair, Audit Committee