**AGENDA ITEM:** C.1.c.

**AGENDA TOPIC:** Internal Audit Report on Security of Personally Identifiable Information

**CONTACT(S):** Representatives from Packer Thomas

**BACKGROUND:** An audit of Security of Personally Identifiable Information was recently completed by Packer Thomas.

**SUMMARY AND ANALYSIS:** Personally identifiable information (PII), defined as data that can in full or part be used to identify an individual, is subject to laws and regulations intended to protect unauthorized disclosure. PII can include SSN, date of birth, tax information, and medical records. Our audit examined PII in electronic format and included a review of University policies and procedures surrounding data protection and a review of key security controls.

From our inquiry and examination of policies, it was discovered that the University does not conduct periodic risk assessments, which increases the risk that PII data will not be effectively secured. In addition, a risk assessment can help increase the effectiveness of allocating IT resources by concentrating more resources to higher risk areas. We recommend periodic risk assessments.

From our inquiry and examination of procedures, it was determined that University does not implement its data classification policy. A data classification policy is an important part of the process to protect PII. Data classification will identify where PII resides within the system and processes and allow targeted security measures to be implemented to add extra security to highly sensitive data.

From our inquiry and examination of procedures and framework for Banner access, it was discovered that PII is stored throughout Banner and logical access to PII is not restricted only to individuals with a business function that requires privileges to the sensitive data.

Our interviews with the IT department revealed that system audit logs are not routinely monitored, creating the risk that a hacker could breach the system and gain unauthorized access for an extended period of time. We recommend that tools be used to automatically search the audit logs for predefined system anomalies and alert the IT department for investigation.

From our interviews and review of University policies, it was revealed that there is no mandatory security awareness training for personnel. Staff actions can play a crucial role in preventing security incidents that can lead to the loss of PII. We recommend mandatory security awareness training and formal acknowledgement from personnel before they are granted access to system data.

From our inquiry and review of records, it was discovered that the University does not maintain a list of authorized hardware and software and routinely compare to devices and software that connect to the network. This creates vulnerability that unauthorized connections will not be discovered and will create weaknesses in the system, such as infections from malware and unauthorized access to sensitive data.

Our interviews revealed that there is no security protection against copying PII onto a USB drive. The risk to the University is that if an unauthorized individual gains access to PII, they would be able to download the information. In addition, if sensitive data were downloaded to a USB drive in an authorized manner, but the USB drive was lost, the PII data would be unsecured. We recommend the system be configured to encrypt PII data when downloaded to a USB drive.

**RESOLUTION: N/A – DISCUSSION ITEM ONLY**

**REVIEWED AS TO FORM AND CONTENT:**

James P. Tressel

James P. Tressel, President

Youngstown
STATE UNIVERSITY

# SECURITY OF PERSONALLY IDENTIFIABLE INFORMATION

## INTERNAL AUDIT REPORT

November 7, 2014

DISTRIBUTION

| | |
|---|---|
| Audit Subcommittee: | Ms. Delores E. Crawford, Chair<br>Mr. David C. Deibel, Vice Chair<br>Mr. Leonard D. Schiavone<br>Mr. Eric A. Shehadi |
| Chairman of the Board of Trustees: | Ms. Carole S. Weimer |
| Management: | Mr. Ken Schindler |

PACKER · THOMAS
Certified Public Accountants & Business Consultants
PROVEN TRUE.

# YOUNGSTOWN STATE UNIVERSITY

## SECURITY OF PERSONALLY IDENTIFIABLE INFORMATION INTERNAL AUDIT REPORT

### CONTENTS

PACKER · THOMAS
Certified Public Accountants & Business Consultants

6601 Westford Place
Suite 101
Canfield, OH
44406

330-533-9777
1-800-943-4278
Fax: 330-533-1734
www.packerthomas.co

Youngstown State University
One University Plaza
Youngstown, Ohio 44555

This report summarizes the results of our internal audit of the University's controls surrounding security of personally identifiable information within the Banner system. Please review this report. If you have any questions, please call us at (330) 533-9777.

Management has provided their responses to our findings and those responses are included within this report.

We wish to thank the staff of the Information Technology department for the cooperation that was extended to us during the course of this audit.

PACKER THOMAS

Packer Thomas

November 7, 2014

## OVERVIEW

An audit of the University's controls surrounding the security of personally identifiable information was recently completed by Packer Thomas. Our procedures were performed as a result of the internal audit risk assessment which was approved by the Audit Subcommittee.

Personally (or Personal) Identifiable Information (PII) is formally defined as information, in electronic or any other form, that can be used:

- Directly to uniquely identify, contact or locate a single person
- With other sources to uniquely identify, contact or locate a single individual

The objective of our audit was to obtain and document the policies and procedures with respect to security of PII. We limited the scope of this audit to focus on the following PII: social security numbers, birth dates, medical records, and tax information. Because the movement and storage of PII within the system is extensive, the scope of this audit is limited to PII in electronic format only and will include:

- Policies and procedures to protect PII and other private data in any of its forms and storage locations, including the deployment and effectiveness of an organization-wide data classification scheme
- Policies and procedures relating to action needed to detect and remediate a breach of PII confidentiality
- Policies and procedures to restrict logical access to PII to authorized individuals
- Training and awareness of employees in the handling and processing of PII and data privacy

The business impact of the loss, disclosure or inappropriate use or modification of PII can be legal, regulatory or reputational in nature leading to significant financial and operational costs. The business risks include:

- Loss of customer confidence due to the release or compromise of PII
- Lawsuits by aggrieved owners of lost or compromised PII
- Fines and penalties assessed by regulators
- Limitation of business opportunities if the privilege to accept credit cards is revoked due to a PII related disclosure
- Unflattering or negative publicity due to press coverage which damages the organization's brand
- Disclosure of administrator passwords, which may cause the organization severe or catastrophic loss

The procedures performed during our internal audit included verbal and written interviews with IT staff, a review of existing University policies, and an examination of data for selected key security controls. It should be noted that our review of the security of PII would not necessarily identify all deficiencies or inefficiencies. However, we have listed a summary of findings and have made recommendations for improvements based upon the weaknesses reported.

AUDIT FINDINGS & RECOMMENDATIONS - REQUIRING IMMEDIATE ACTION

1. The University does not conduct periodic risk assessments. In order to develop and maintain an effective cybersecurity program, it is essential to identify the critical information that needs protection, identify the threats to its security, and then develop a strategic cybersecurity defense plan. The purpose of a risk assessment for cybersecurity is to discover what the risks are to PII security, where they are in the system, and how to mitigate the identified risks to an acceptable level for the University. The risk assessment should be periodically reviewed and updated to reflect changes within the University system, identified security events, and new existing technology tools and threats.

   The University should conduct a risk assessment, which would include an identification of PII data and methods to secure the highly sensitive data. This assessment could be started with a survey of data owners to identify the location of PII. The data and systems would then be classified according to risk and then methods for securing the systems and data could be developed. Some advantages to periodic risk assessments would be to allocate IT resources according to levels of risk – more resources could be shifted to areas of higher risk, such as PII. This risk assessment should be periodically updated based upon changes to the system, processes, and reported security incidents.

   MANAGEMENT RESPONSE

   The University considers this audit report in and of itself a risk assessment as it has pointed out several areas for PII security improvement.

   However the University will explore conducting its own formal risk assessment and the option of engaging a consultant to lead this effort.

2. Although the University has a written data classification policy (contained in the "Sensitive Information Policy"), the policy is not implemented in practice. According to the federal cybersecurity standards, asset and data classification is the keystone to building proper protective schemes. Simply, if you don't know what you have, you can't apply the appropriate levels of value and importance. Classifying data is the process of categorizing data assets based on nominal values according to its sensitivity. For example, data might be classified as: public, internal, confidential (or highly

confidential), restricted, etc. Data and information assets are classified respective of the risk of unauthorized disclosure (e.g., lost or stolen inadvertently or nefariously). High risk data, for example "Sensitive", requires a greater level of protection, while lower risk data, for example "Public", requires proportionately less protection. Once the data has been classified and identified within the system, a plan can be developed to allocate appropriate protections and resources to the highly sensitive data.

As part of the risk assessment process, the data classification policy in the University's "Sensitive Information Policy" should be implemented. Highly sensitive PII data should be located in the processes and data system and evaluated for additional cybersecurity protection measures.

MANAGEMENT RESPONSE

The University agrees. Network and Data security is in the process of evaluating areas known to utilize PII as well as the storage and accessibility of such data on a department by department basis.

3. Logical access to Banner is not granted in a manner to restrict access to PII only to authorized individuals. Forms containing PII are grouped with forms in Banner profiles that do not contain PII. This configuration does not make it possible to approve access in a manner to restrict PII only to personnel who require access to sensitive data due to their job function. In addition to creating the risk of an unauthorized University personnel accessing PII, the risk of a hacker gaining access to PII increases. In the event that a hacker is able to gain access to the system, he could potentially gain access to PII along with public or less sensitive data.

Banner forms should be reviewed and all forms that contain PII should be identified. Access to forms containing PII should be restricted and segregated in Banner roles that are designated "sensitive". Management should assign access to sensitive roles only when required by job function.

MANAGEMENT RESPONSE

A standing ITS project has existed for the express purpose of refining the restrictions on PII access to authorized individuals within the Banner/Oracle environment. A three-phased approach has been defined for achieving this goal. The first phase restricts access to specific Oracle forms exposing PII details to all but a limited number of Banner power users. Phase I also calls for the masking of SSN and DOB on the remaining forms containing personally identifiable information.

Phase II of the initiative facilitates the review and modification of Oracle user roles external to the Banner environment while Phase III addresses access to PII data associated with non-Banner Oracle applications such as Microsoft Excel and Access as well as third-party applications such as Starfish, StarRez, PeopleAdmin, etc.

Over the next twelve months, priority attention will be given to the completion of the first phase of this project along with the development of a Phase II and III implementation plan.

4. Audit logs are not routinely reviewed for potential security incidents or breaches. This increases the risk that a security breach could go undetected for a significant length of time and allow a hacker to operate within the system for an extended period of time.

   The University should consider using tools to create automatic reports from system activity logs that would identify system anomalies. These exception reports would be sent to IT personnel for investigation and timely follow up.

   MANAGEMENT RESPONSE

   The University agrees. However, ITS must first implement a central log file repository and retain system logs for a consistent length of time. Once that is achieved, routine scanning of all logs will be explored. Packages that exist for this purpose will be evaluated at that time.

5. The University lacks a policy or procedure of security awareness training for personnel. Although the IT Department holds periodic security awareness meetings, the meetings are not mandatory to staff. The University security policies are available on the University website, but there is no requirement that users acknowledge having read the policies before accessing the system. Employee behavior is one of the biggest factors in cyber security and can play a critical part in the success or failure of an organization. Some of the most recent public successful attacks reported in the media this past year have been due to the actions of personnel. No data security approach can begin to address cyber risk without a means to address this fundamental issue. Empowering people with good cyber defense habits can significantly increase readiness and help protect the PII data handled by the University.

   A security training policy and program should be developed and adopted by the University. It should include the requirement that personnel must receive initial awareness training before accessing the system and refresher training at least annually. In addition, the University should require formal written acknowledgement of its security policies upon hire. The University could consider different levels of security training based upon job functions and access to PII. The training and acknowledgement of University security policies should be formally tracked and documented.

MANAGEMENT RESPONSE

The University agrees that security awareness training for employees needs to be improved. ITS will work with Human Resources to develop a plan that addresses both the training of new employees and ongoing training for current staff.

AUDIT FINDINGS & RECOMMENDATIONS - REQUIRING IMMEDIATE ACTION (CONTINUED)

6. The University does not maintain an inventory of authorized software and hardware, and there is no periodic network scan to identify whether unauthorized hardware or software has connected to the system. The University maintains a list of authorized laptop computers that are able to be "wiped" remotely in the event that they are lost or stolen, but does not ensure that only authorized devices are connected to its network. This increases the risk that unauthorized equipment or software may be compromised and infect internal system resources. Such a security breach could result in unauthorized access to PII through tools such as malware. In addition, unauthorized laptops may not be configured to encrypt PII data properly.

   A list of authorized hardware and software should be compiled. The University should employ scanning tools that will periodically scan the network for unauthorized software and devices and create action alerts.

   MANAGEMENT RESPONSE

   YSU has deployed the Altiris Desktop management system. Not only does it push software, it inventories almost all software packages installed by users with administrator accounts. In addition, Altiris inventories authorized hardware connected to the wired network. YSU is exploring solutions that will identify and send an alert when unauthorized hardware is connected to the wired network.

7. The University's system allows data to be copied to a USB drive without being encrypted. In the event that a USB drive containing PII is lost, this increases the risk of an authorized individual gaining access to PII.

   The University could configure the system to prohibit the copying of sensitive data onto USB drives, once the highly sensitive data has been identified in the system. In the event that there is a legitimate business need to use a USB drive, the University could configure the system to encrypt sensitive data when copied, or supply selected employees with hardware encrypted USB flash drives for use when copying PII.

MANAGEMENT RESPONSE

The University will review its policies & procedures with regard to extracting PII to any mobile media or local storage in light of improved access restrictions being implemented in response to item #3 above. This review will include consideration of scanning local storage for PII as we believe PII stored locally poses a more significant security threat than mobile storage.