Information Technology:
Data Security, Cybersecurity Training, & Business Continuity Planning
Continuous Audit Project, Report I

From the Office of the Internal Auditor AUD.FY16-08

BACKGROUND

Information technology (IT) security is vital to the College. In order to conduct operations efficiently and effectively, departments rely heavily upon IT systems. The College faces many new and emerging IT cybersecurity threats, in addition to numerous routine and critical day to day IT responsibilities. There has been a high rate of IT personnel turn-over in 2016. IT has limited resources that must meet many needs; the College Information Security Officer position was upgraded in March 2016 to the Director of Cybersecurity to help more effectively prioritize resources to address IT risks. In addition, IT management is planning to begin a new College Cybersecurity Taskforce during May 2016 to help better address IT issues; Internal Audit will participate in the taskforce.

The College must comply with numerous, complex IT security requirements established by federal and state laws and other outside regulatory bodies. The Office of the Internal Auditor (Internal Audit) continuously monitors key components of Information Technology. The scope of this report includes Part I of Information Technology: Cybersecurity training, Data Breach Response Plan, and the Business Continuity Plan/Disaster Recovery Plan. *Detailed conditions (findings) and management responses follow the conditions and recommendations in each section of the report; Internal Audit will follow-up as necessary to determine if conditions noted have been addressed.*

DEFINITIONS[1]

Cybersecurity:
The protection of information assets by addressing threats to information processed, stored, and transported by internetworked information systems.

Business Continuity Plan (BCP):
A plan used by an organization to respond to the disruption of critical business processes. Effectiveness depends in part on the plans created in advance of an emergency for restoration of critical business systems.

Disaster Recovery Plan (DRP):
A set of human, physical, technical and procedural resources to recover, within a defined time and cost, an activity disrupted by an emergency or disasters.

[1] ISACA *Cybersecurity Fundamentals Glossary*

SUMMARY OF CONDITIONS AND RECOMMENDATIONS

Overall, we found that critical cybersecurity planning issues exist at the College including:

- Cybersecurity training is not provided annually to all employees.
- A comprehensive written Data Breach Response Plan does not exist.
- A comprehensive written Business Continuity Plan/Disaster Recovery Plan does not exist.

To address the conditions identified in the report, Internal Audit recommends that the Assistant Vice Chancellor of Information Technology work with applicable IT staff and management to:

- Provide annual Cybersecurity training to all College employees and document the completion of training.
- Develop periodic hands-on Cybersecurity workshops for employees.
- Develop a comprehensive written Data Breach Response plan that meets federal, state and other compliance requirements.
- Review available IT resources containing detailed guidance for developing Data Breach Response plans, e.g. the *National Institute of Standards and Technology (NIST) U.S. Department of Commerce Computer Security Incident Handling Guide Special Publication 800-61*.
- Place the RFP for the BCP/DR Plan out for bid after appropriate approvals are completed.
- Periodically test the BCP/DR plan to help ensure it is readily available in event of a disaster.

DETAILED CONDITIONS AND MANAGEMENT'S RESPONSE

➢ CYBERSECURITY TRAINING

Background

Cybersecurity vulnerabilities are continually evolving and education is needed to stay informed about these risks. Cybersecurity training provides guidance to employees on the latest and most persistent IT threats and helps protect the College's important information assets.

The Director of Cybersecurity provided six (6) "Pima Cybersecurity" presentations to selected College departments and senior administration during 2015 and 2016; however these efforts did not include all College employees.

Condition 1:

Annual comprehensive Cybersecurity training for all College employees does not exist.

Cybersecurity training is an important preventative measure to help limit IT risks to the College that can occur when employees take actions that could be potentially harmful to IT systems. In addition, the *PCI Security Standards Council Payment Card Industry (PCI) Data Security Standards 3.1*. requires annual Cybersecurity training for employees.

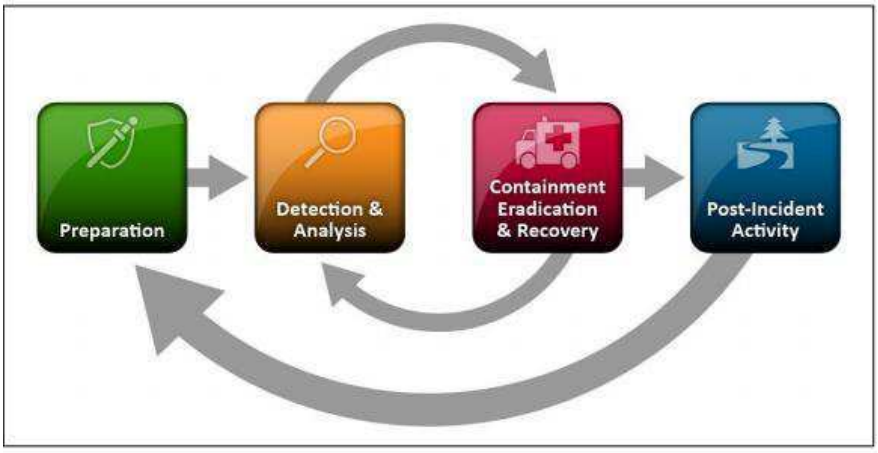
Management Corrective Action Plan 1:
The College Director of Cybersecurity recognizes the critical importance of providing current cybersecurity information to all employees and protecting the College's information assets. Specific plans for College-wide training are currently in process. The current plans include:

- *Presenting a "Cybersecurity Survival Guide" at "All College Day" (on August 19, 2016). The presentation will include techniques employees can utilize to protect information assets at the College and also on personal level on their home computers.*
- *Identifying online cybersecurity training to be provided to all College employees. Research to identify the appropriate cybersecurity training is scheduled to be completed by December 31, 2016. The Director of Cybersecurity will work closely with the Human Resources Department and Organizational Effectiveness and Development when selecting the training. The planned roll-out of this training will occur during early 2017.*
- *Cybersecurity training will be identified specifically for on-boarding new College employees to ensure they receive cybersecurity training prior to starting their work duties. The Director of Cybersecurity will work closely with the Human Resources Department and Organizational Effectiveness and Development when selecting the training. The identification of the on-boarding cybersecurity training will be completed by October 31, 2016. The planned roll-out of this training will occur during late 2016.*
- *A meeting will be scheduled with senior College administration and senior IT management regarding requiring mandatory annual cybersecurity training for all employees. The tentative target date for scheduling the meeting is January 31, 2017.*

➢ DATA BREACH RESPONSE PLAN

Background

Data Breach Response plans are important in the event of an IT security incident. Preparing for the worst is the best defense. The average cost for an organization for a data breach is $5.4 million per *The Institute of Internal Auditors*. The *Verizon 2016 Data Breach Investigations Report* states that 3,141 confirmed data breaches occurred during 2015 impacting many types of organizations, including educational institutions. An incident response life cycle is illustrated below listing steps in an incident (*National Institute of Standards and Technology*).



Condition 2:
A written comprehensive Data Breach Response Plan does not exist.

The lack of a Data Breach plan places the College at increased risk for reputation damage, potential credit monitoring costs for individuals' impacted by a breach, and monetary penalties in the event of a breach.

The State of Arizona civil penalties are $10,000 per breach incident and the requirement to provide notification to individuals impacted from a data breach. In addition, Health Insurance Portability and Accountability Act (HIPAA) penalties can be significant, ranging from $100 to $50,000 per violation.

Management Corrective Action Plan 2:
The Director of Cybersecurity will begin researching required components of an incident response plan for the College. Research regarding incident response plans will be starting from scratch because IT staff has been engaged in other College IT activities and IT has not prioritized resources to conduct research on this topic. In addition, high IT staff turnover during 2016 has contributed to further delays. Research for developing an incident response plan is scheduled to begin by August 31, 2016.

Meetings will be scheduled with IT management and departments at the College that can provide input for developing an incident response plan. Departments currently on this meeting list include: College General Counsel and Office of the Internal Auditor. Meetings are planned to begin by September 30, 2016.

➢ BUSINES CONTINUTIY PLAN/DISASTER RECOVERY PLAN

Background
A viable College Business Continuity Plan/Disaster Recovery Plan is critical to help the College to recover quickly in the event of a disaster, e.g. electrical power outage/disruption. A BCP/DR plan is a College-wide issue that will involve input from all departments in developing a plan. IT has taken the lead on developing an RFP to hire a consultant to develop a BCP/DR plan college-wide.

Condition 3:
A complete and comprehensive written Business Continuity Plan/Disaster Recovery Plan has not been developed.

An RFP was developed; however it has not been placed out for bid due to a misunderstanding within IT about RFP ownership/approval process next steps.

Standard IT controls dictate that a comprehensive BCP/DR plan be developed and periodically tested. The lack of a BCP/DR plan could result in delays in restoring needed business services, disruption of services to students, and increased costs and risks of errors when restoring IT systems.

Management Corrective Action Plan 3.
A Business Continuity Plan, its associated Business Impact Analysis (BIA), and Disaster Recovery Plan will be developed. The BCP and BIA and are required first steps to develop a Disaster Recovery Plan. A Request for Proposal (RFP) is being developed by IT to obtain consulting services to assess the current state of Pima College's Business Continuity capabilities. The RFP should be released by September 30, 2016. IT management will work closely with the consultant selected to ensure that a Business Continuity Plan, Business Impact Analysis and Disaster Recovery Plan are developed by January 31, 2017.