CYBERSECURITY

KERI WRIGHT, CPA
DEPUTY STATE AUDITOR

MISSOURI STATE AUDITOR'S OFFICE

Agenda

- About the Missouri State Auditor’s Office
- Cybersecurity Initiative
- Common Data Security Findings
- Report Examples
- Resources

Missouri State Auditor's Office

- Nicole Galloway, CPA, CFE
  - The 38th State Auditor of Missouri
- Staff of 85 auditors
- 4 locations
  - Jefferson City
  - Springfield
  - St. Louis
  - Kansas City
- We are Missouri's independent watchdog agency
  - Proper use of public funds
  - Improve efficiency and effectiveness in Missouri's governments

Missouri State Auditor’s Office

Types of Audits:

- We audit government entities in the State of Missouri
  - State agencies, including state colleges and universities
  - Statewide elected officials
  - 3rd class counties
  - School districts
  - Courts
  - Others by petition or governor request

Cybersecurity Initiative

“..We must ensure criminals near and far do not access your personal data in your children’s schools or within state or local government. Government must be held accountable to keep that private data safe and secure.”

- Nicole Galloway

Cybersecurity Initiative

- Review computer controls closer on all audits
- Review system controls for selected state agency systems
- Launched Cyber Aware School Audits

Cybersecurity Initiative

- Cyber Aware School Audits
- Focus:
  - Effectiveness of the schools’ cybersecurity safeguards
  - Review the district’s ability to detect a cybersecurity breach and the planned response for a breach
  - Review student personal information accessibility and protections
  - Assess technology use policies
  - Review student and staff privacy and security awareness training

Cybersecurity Initiative

- Cyber Aware School Audits
  - 5 School Districts selected:
    - Boonville School District
    - Cape Girardeau School District
    - Orchard Farm School District
    - Park Hill School District
    - Waynesville School District

- Current status of audits

Summary of Common Audit Findings

- Top 5 most common basic data security issues identified during our audits in fiscal year 2015:

1. User Access Management
2. User Authentication
3. Security Controls
4. Backup and Recovery
5. Data Management

Issue #1: User Access Management

1.1 Access Rights and Privileges

- What we found:
  - Access to certain systems was not adequately restricted
  - Adequate supervisory reviews were not performed
- Why this matters:
  - Limits what a user can do after being allowed into the system.
  - Reduces the risk of unauthorized changes to records

Issue #1: User Access Management

1.2 Access Request forms

- What we found:
  - Access request forms were not used for requesting or approving access to systems
- Why this matters:
  - Limits access to only those authorized & needing access
  - Provides proper documentation of access

Issue #1: User Access Management

1.3 Terminated employees

- What we found:
  - User access of former employees was not disabled timely
- Why this matters:
  - Reduces the risk of unauthorized access, modification, or destruction of data

Issue #2: User Authentication

2.1 Passwords not changed

- What we found:
  - Passwords were not required to be changed on a periodic basis.

- Why this matters:
  - Reduces the risk of unauthorized access to and use of systems and data

Issue #2: User Authentication

2.2 Sharing passwords

- What we found:
  - User accounts and passwords for accessing computers and various systems were shared by users.
- Why this matters:
  - The security of a password system is dependent upon keeping passwords confidential
  - Sharing password cause losing individual accountability for system activity
  - Unauthorized system activity could occur
  - Unauthorized individual gains access to sensitive information

Issue #2: User Authentication

2.3 Passwords not required

- What we found:
  - Passwords were not always required to logon and authenticate access to a computer/system
- Why this matters:
  - No assurance the data or system is protected.

Issue #3: Security Controls

3.1 Inactivity controls

- What we found:
  - A computer or system wasn’t locked after a certain period of inactivity.
  - Users did not log off computers when unattended

- Why it matters:
  - Inactivity controls decrease the risk of unauthorized access, use, modification, or destruction of data.

Issue #3: Security Controls

3.2 Unsuccessful login attempts

- What we found:
  - A computer or system was not automatically locked after a specified number of unsuccessful attempts.
- Why it matters:
  - Unauthorized individuals could have unrestricted access to information
  - Increased risk of unauthorized access, use, modification, or destruction of data.

Issue #4: Backup and Recovery

4.1 Backups

- What we found:
  - System data was not periodically backed up.

- Why this matters:
  - Data will not be available for recovery if a disruptive incident occurs.

Issue 4: Backup and Recovery

4.2 Offsite Storage

- What we found:
  - Backup data is stored at the same location of the original data instead of offsite.

- Why this matters:
  - In case of a disruptive incident, backup data may also be lost, data is not available for recovery.

Issue #4: Backup and Recovery

4.3 Testing

- What we found:
  - Backup data is not tested regularly

- Why this matters:
  - Management cannot ensure that they will be able to recover the lost data from backup data.

Issue #4: Backup and Recovery

4.4 Disaster Recovery Plan

- What we found:
  - A detailed disaster recovery plan had not been developed by management
  - Recovery plans were not up-to-date or tested
- Why this matters:
  - Tested & up-to-date disaster recover plans provide assurance computer operations can be promptly restored after a disruption.

Issue #5: Data Management

5.1 Data Integrity

- What we found:
  - Data integrity controls guard against the improper change or destruction of data and information.
  - Audit trail controls provide evidence transactions are proper
- Why this matters:
  - Without these controls, the risk of manipulation of data without detection increases.
  - Audit trail controls recorded evidence of how a transaction was processed.

Issue #5: Data Management

5.2 Numerical Sequence

- What we found:
  - The numerical sequence of transaction numbers assigned by the computerized accounting system was not accounted for.
- Why this matters:
  - There is an increased risk of loss, theft, or misuse of funds

Cyber Aware School Audits

- Audit Process
  - Entrance Conference
  - Fieldwork
  - Pre-Exit
  - Reporting
  - Exit
  - Reponses
  - Audit Release

- Report Format
  - Background
    - Cyber Aware School Audits Initiative
    - Importance of cybersecurity & controls
  - Scope & Methodology
  - State Auditor's Findings
  - Organization & Statistical Information

Cyber Aware School Audits

- Base our evaluation on various accepted standards, best practices, and controls from:
  - National Institute of Standards and Technology
  - Government Accountability Office
  - ISACA (previously known as the Information Systems Audit and Control Association)
  - USDE, Privacy Technical Assistance Center (PTAC)

Report Example: Boonville

Data Governance

An organizational approach to data and information management that is formalized as a set of policies and procedures encompassing the full life cycle of data from acquisition to use to disposal

- Improvements needed in the following areas:
  - Responsibility of data management
  - Data stewardship
  - Inventory & classification of data
  - Source and content of data
  - Monitoring unauthorized disclosure of PII
  - Archival and/or destruction of data at end of its lifecycle

Report Example: Boonville

Security Controls

- Types:
  - Logical security (user accounts & passwords)
  - Physical security (locked rooms, inventory)
- Improvement needed in the following areas:
  - Having a dedicated Security Administrator
  - Password controls
  - Access controls
    - Logon banners
    - Concurrent users
  - Security logs
  - Physical security
  - Documentation of security controls

Report Example: Boonville

User Accounts

Controls over the creation and maintenance of user accounts for accessing system resources

- Improvement needed in the following areas:
  - Account requests
  - Inactive account monitoring
  - Review of user access

Report Example: Boonville

Incident Response and Continuity Planning

- Improvement needed in the following areas:
  - Incident response policy

    Security incident- an occurrence that actually or potentially jeopardizes information

  - Data breach response policy

    Data breach- a security incident where data has been potentially accessed, stolen or used by an unauthorized person.

  - Continuity plan

Report Example: Boonville

Security Awareness Training Program

With proper security and privacy awareness training and clear communication of data and device use policies, employees can become the first line of defense against cybersecurity incidents.

Vendor Monitoring

- Process for ensuring outsourced software from vendors compliance with industry data security principles.
- Maintaining all software vendor contracts

Report Example: Boonville

While improvements are needed, there were several controls already in place

- Technology use policy
- Policies & Procedures for data disclosure & usage to be in compliance with FERPA
- Controls and processes required to be in compliance with the Children's Internet Protection Act
- Certain controls designed to help ensure privacy of data and maintain the data's confidentiality, integrity, and availability

District worked in collaboration with our office to make improvements

Report Example: Attendance Records

- Attendance Records
  - System did not adequately track changes made to attendance records
  - System did not limit the time frame during which changes can be made
  - No review by district officials to ensure changes were appropriate
- Rapid Response Audit in 2011
  - Attendance records were falsified to significantly overstate attendance
  - Impact:
    - State and federal funding received
    - State and federal compliance
    - At-risk kids wouldn’t be flagged for intervention services

Report Example: Attendance Records

- What went wrong?
  - The electronic attendance system:
    - Did not limit when changes could be made
    - Did not track when changes were made or by whom
    - Did not require approval by the teachers for changes made to attendance in their classrooms

Report Example: DESE

- In 2015 we issued a report over DESE's Missouri Student Information System
  - The main reporting system used by DESE to collect student-level data from school districts

- Four main issues:
  1. User Account Management
  2. Data Collection
  3. Breach Response Policy
  4. Business Continuity Plan

Report Example: DESE

1. User Account Management
   - User account management policies not fully established or documented
   - Multiple users are allowed access to the system via shared accounts and these accounts are not regularly monitored
2. Data Collection
   - Collecting SSN of students without a business purpose for them
   - Puts students at risk in the event of a data breach
3. Breach Response Policy
   - DESE had not established a comprehensive data response policy
4. Business Continuity Plan
   - Established in 2004; however, it has not been updated or tested

How do you compare?

- Do you have the most basic system controls in place?
  1. User Access Management
  2. User Authentication
  3. Security Controls
  4. Backup and Recovery
  5. Data Management
- Are your policies up-to-date and complete?
- Do you test your backups & recovery plans?
- Do you have protections over your most sensitive data?
- Do you have sensitive data that isn't necessary for business purposes?

Resources

- USDE Privacy Technical Assistance Center
  - Best Practice resources to help educational agencies
  - PTAC Toolkit: http://ptac.ed.gove/toolkit

- MOREnet
  - Multiple resources available along with best practices

Missouri State Auditor’s Office

QUESTIONS??