# Data Security and Identity Management

Leading Change Data Pre-Conference
June 16, 2014

Ed Jung
Chief Technology Officer
Arizona Department of Education

# DATA SECURITY

Arizona Department of Education

# Are you prepared

- Likelihood of a data breach is high
  http://www.databreachcalculator.com/

Likelihood of experiencing a data breach in the next 12 months: 9.5%

Average cost per record: $ 190

Average cost per breach: $ 94,833

## You are a target

# Really, you are a target

Hack Forums - Request: Hack **Powerschool**
www.hackforums.net › ... › Requests for Hacking
Jan 10, 2011 - 6 posts - 3 authors
I was just wondering if anyone could either hack **powerschool** for me or, preferably, ...
pm me if you want direct link to

**Fayette schools alert parents of Infinite Campus scam**

Sunday, April 28, 2013 - 6:20pm
Submitted by Ben Nelms
Board of Education Government Fayette County
Share / Save

**"Some districts have reported that staff or parents have received emails from people purporting to work for Infinite Campus, requesting usernames, passwords and email accounts to confirm ownership of their Infinite Campus account."**

**Catholic schools close Friday following data breach**

By KOMO Staff | Published: Mar 13, 2014 at 10:06 PM PDT

**"The notice says hackers have been able to steal personal information, file fake tax returns and redirect the money to themselves."**

# Do you know your data

Impact definitions (National Institute of Standards and Technology FIPS-199)

- LOW: The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
- MODERATE: The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
- HIGH: The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

# Sample data classification

| | Restricted (highest, most sensitive) | Sensitive (moderate level of sensitivity) | Public (low sensitivity) |
|---|---|---|---|
| Legal Requirements | FERPA, HIPAA, state statute | Contractual obligations, privacy norms | At discretion of institution |
| Reputation Risk | High | Medium | Low |
| Other Risks | Information which provides access to additional resources | Subsets of protected data | General information, embarrassment |
| Access | Explicit authorized access only, signed agreements | Need to know based on role | General LEA information |
| DATA | Student education records, SSN, educator performance classifications, discipline | Salaries, staff personal contact information, library lending records | Procurement records, calendar of events, school records for sports |

# Do you know where your data is

- What applications do you manage in-house? (e.g. SIS/SMS)
- What applications are vendor managed or cloud hosted? (e.g. SIS, learning management)
- Are there well understood policies over the use of third-party applications? (e.g. gradebooks, lesson planners, online courses)

# It’s the people

**Negligent staff are the top cause of data breaches in the United States**

– 2011 Cost of a Data Breach Study: United States, Symantec Corp. and Ponemon Institute.

**Data Breach Exposes 6,000 High School Students' Personal Data**

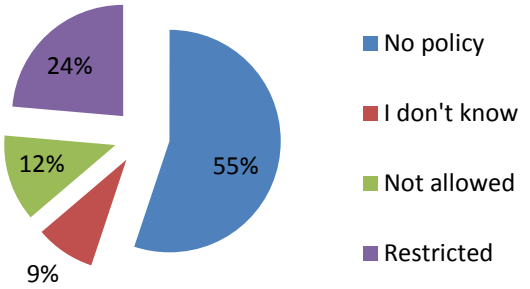
The students' names, birthdates, genders, final grades, learning skills and work habit assessment scores were mistakenly made available online.

By Jeff Goldman | Posted March 21, 2014

**Spear Phishing Attacks are Often the Root Cause of Security Breaches**

More than one third (**34%**) of respondents who reported experiencing a spear phishing attack in the past year believe that such an attack resulted in the compromise of user login credentials (e.g., usernames passwords) or unauthorized access to corporate IT systems.

**Policies on working in public places**



# Detection

- 66% percent of breaches took months or even years to discover
  - Verizon Data Breach Investigation Report
- On average, it is taking companies three months to discover a malicious breach and then more than four months to resolve it
  - Ponemon Institute report

**How can we speed this up?**

# Who is responsible

- Does your organization have a designated Information Security Officer
- Who develops information security related policies
- Who enforces policies

# Communications and Action Plan

- Security Awareness Training
- FERPA and Privacy Training
  - General training for all your users
  - Differentiated by role

- Communications and Action Plan
  - Develop, train, test, repeat
  - Who needs to know and when
  - Crisis response team
    - Impact on other work
  - Legal, law-enforcement, public

# IDENTITY MANAGEMENT

Arizona Department of Education

# Your users

- Who are they
- Roles
- How do you know who they are

| | Student | Staff | Parents |
|---|---|---|---|
| Roles | Student | Teacher, Finance, Administrator | Parent, Volunteer |
| Systems they access | SIS | SIS, ERP, HR, Finance, Gradebook | SIS, Website |
| Identity Verification | In-person, documentation | In-person, documentation | |
| Re-verification | Annually | None | |

Where is all of this stored, how is it managed?

# Your policies

- What systems do your users have access to
  - Not just the systems you manage
- How are roles and permissions set on each one
- Consistency across systems
- What happens when a users access needs to be changed
  - How do you know when a users access rights need to be changed
- How often do you audit access to systems

Policies and procedures for onboarding new applications and users should capture the data required to manage identity and access.

# ADE Entity Management

Problem:

- Setting up and maintaining Common Logon accounts is tedious and error prone
- Program areas use different paper user authorization forms completed by LEA
- When access changes at LEA there is no automated process to update ADE records, resulting in delays giving or removing access to sensitive data

Solution:

- Empower LEAs with the ability to manage their own users
- Super-user at each LEA

# Federation with ADE Systems

Problem:

- Entity management at LEAs is a duplication of effort
- Users still need to log onto ADE systems with the credentials created by the LEA Entity Administrator

Solution:

- Enable direct access from LEA systems with no additional user account management required
- Industry standard security protocol
- Works with leading SIS vendors

# Useful resources

- Estimate the likelihood and cost of a data breach
  - http://www.databreachcalculator.com/
- Security Breach Response Plan Toolkit
  - https://www.privacyassociation.org/community/security_breach_response_plan_toolkit
- Model Data Security Breach Preparedness Guide
  - http://www.americanbar.org/content/dam/aba/administrative/litigation/materials/sac_2012/22-15_intro_to_data_security_breach_preparedness.authcheckdam.pdf
- Data Breach Response Guide
  - http://www.experian.com/assets/data-breach/brochures/response-guide.pdf
- Cyber Security training resources
  - https://msisac.cisecurity.org/resources/videos/free-training.cfm
- Verizon Data Breach Investigation Report
  - http://www.verizonenterprise.com/DBIR/
- Fordham Law School report on Privacy and Cloud Computing in Public Schools
  - http://ir.lawnet.fordham.edu/clip/2/
- Fundamentals of Identity and Access Management
  - http://www.theiia.org/intAuditor/itaudit/archives/2008/april/the-fundamentals-of-identity-and-access-management/

# Thank You

Contact

Ed Jung

Chief Technology Officer

(602) 542-3545

Ed.Jung@AZED.gov