Utah State Board of Education

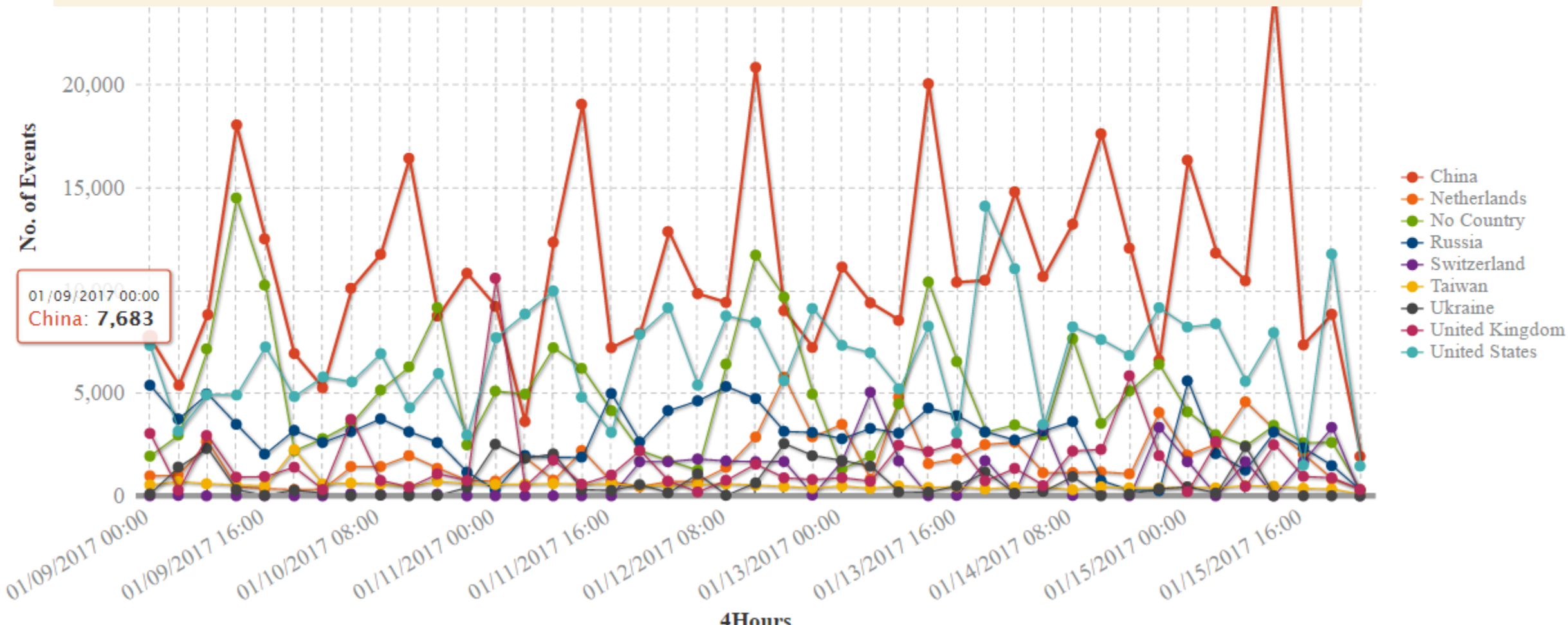
Student Data Protection Act

Whitney Phillips, Ph.D.
Chief Privacy Officer
Utah State Board of Education
Whitney.phillips@schools.Utah.gov
801-538-7523


HawaiiReporter
Who can access K-12 students' personal data? No one really knows
emergencies.
MICHELLE MALKIN
Look who's data-mining your toddlers
biometric data collection.
The New York Times
With Tech Taking Over in Schools, Worries Rise
Teachers use behavior management systems to dole out positive and negative feedback in real time. Each child's status may be visible to the class. Behavior data can be used to create reports for administrators.
student IDs, can make it possible to track students' movements on and off the bus and in sc
potentially sensitive information.
Data analytics programs record
key stroke, and
nts make while
digital materials.
used to create
Common Core: Data Collection from Cradle to Adulthood
weaknesses that can be tailored
to individualized needs.
POLITICO
Data mining your children
MODEL VIEW CULTURE
Technology, culture and diversity media.
nce, grades, at-risk status,
cal and psychological
also be included.
photos, to some companies, including yearbook publishers and class-ring
Grooming Students for A Lifetime of Surveillance
HUFF POST EDUCATION
Student Privacy in Peril: Massive Data Gathering With Inadequate Privacy and Security
Basic student data is sent to state education departments. Some states also gather info on pregnancy, homelessness, and bullying. Some
The New York Times
Student Data Collection Is Out of Control

A hacked computer can be used to...

- Pivot into other systems
- Siphon critical/sensitive data
- Record Keystrokes and steal passwords
- Send spam and phishing emails
- Infect other systems
- Illegally distribute copyrighted material
- Overwhelm resources of a target
- Hide programs that launch attacks
- Anything a hacker wants



January 29, 2017

EDUCATION WEEK

Published Online: October 19, 2015

Published in Print: October 21, 2015, as **Lessons Learned From Security Breaches**

DATA: Sharing + Privacy

Complete Coverage ▸

Schools Learn Lessons From Security Breaches

By Michelle R. Davis

ARTICLE TOOLS

Printer-Friendly

Email Article

Reprints

Comments

When an employee of the **Provo, Utah, school district** mistakenly clicked on a phishing link in an email last year, the private data of about 500 employees were put at risk.

District officials personally went to every school and district department to meet with employees face to face and explain what occurred. The district also paid the bill for a year of credit monitoring for employees. Afterwards, the district altered its practices on sharing sensitive information to improve data security, and employees were retrained to better recognize suspicious links and other scams.

http://www.edweek.org/ew/articles/2015/10/21/lessons-learned-from-security-breaches.html

EdSurge News

Data Privacy | Policy

Preparing Schools for Ransomware—the Next Big Threat to Education

By **Jonathan Levine** Jun 11, 2016

Martial Red for Shutterstock

Schools must brace themselves for an onslaught of new cyber attacks. Today's most pervasive cyber threat is "crypto-ransomware", a type of malware that encrypts and scrambles files (usually in the form of confidential data) to hold them for ransom. As a recent victim of ransomware, Horry County Schools, the third largest school district in South Carolina, was forced to shut down more than 100 servers to stop the malware from spreading.

https://www.edsurge.com/news/2016-06-11-preparing-schools-for-ransomware-the-next-big-threat-to-education

9/21/2016
06:05 AM

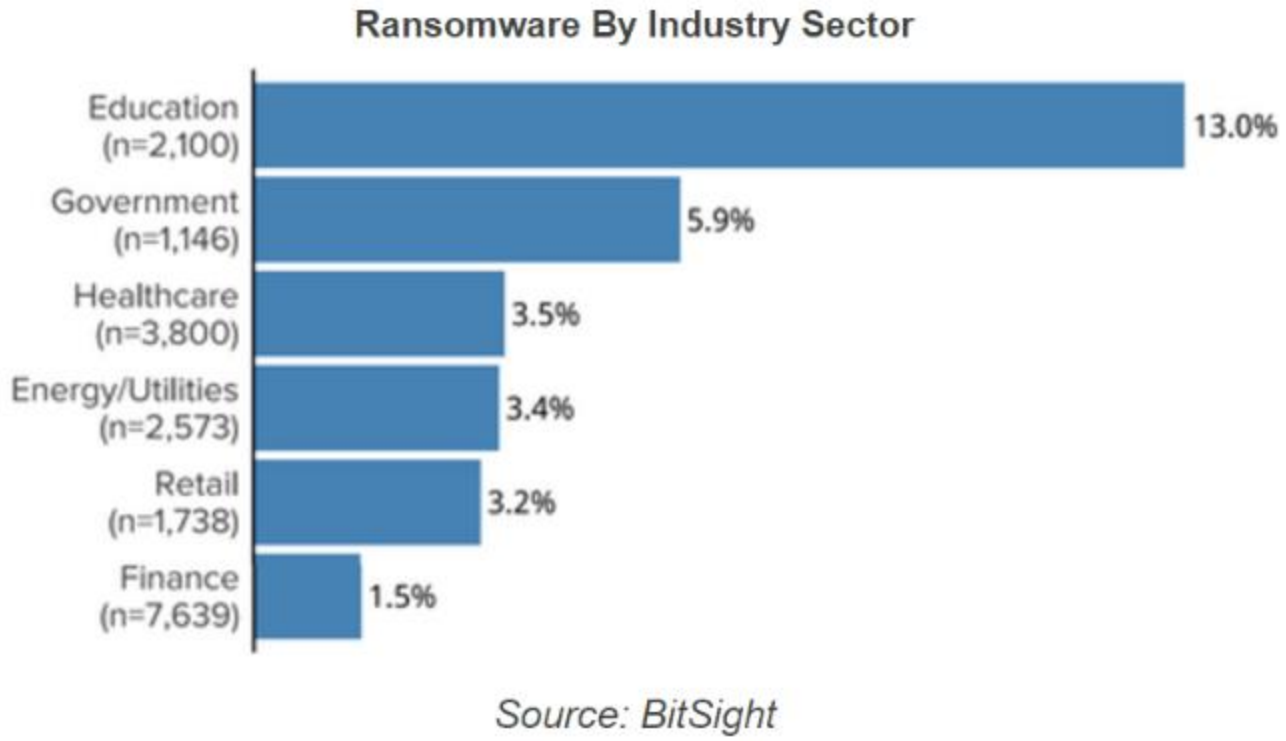
Education Now Suffers The Most Ransomware Attacks

Kelly Jackson Higgins
News

Connect Directly

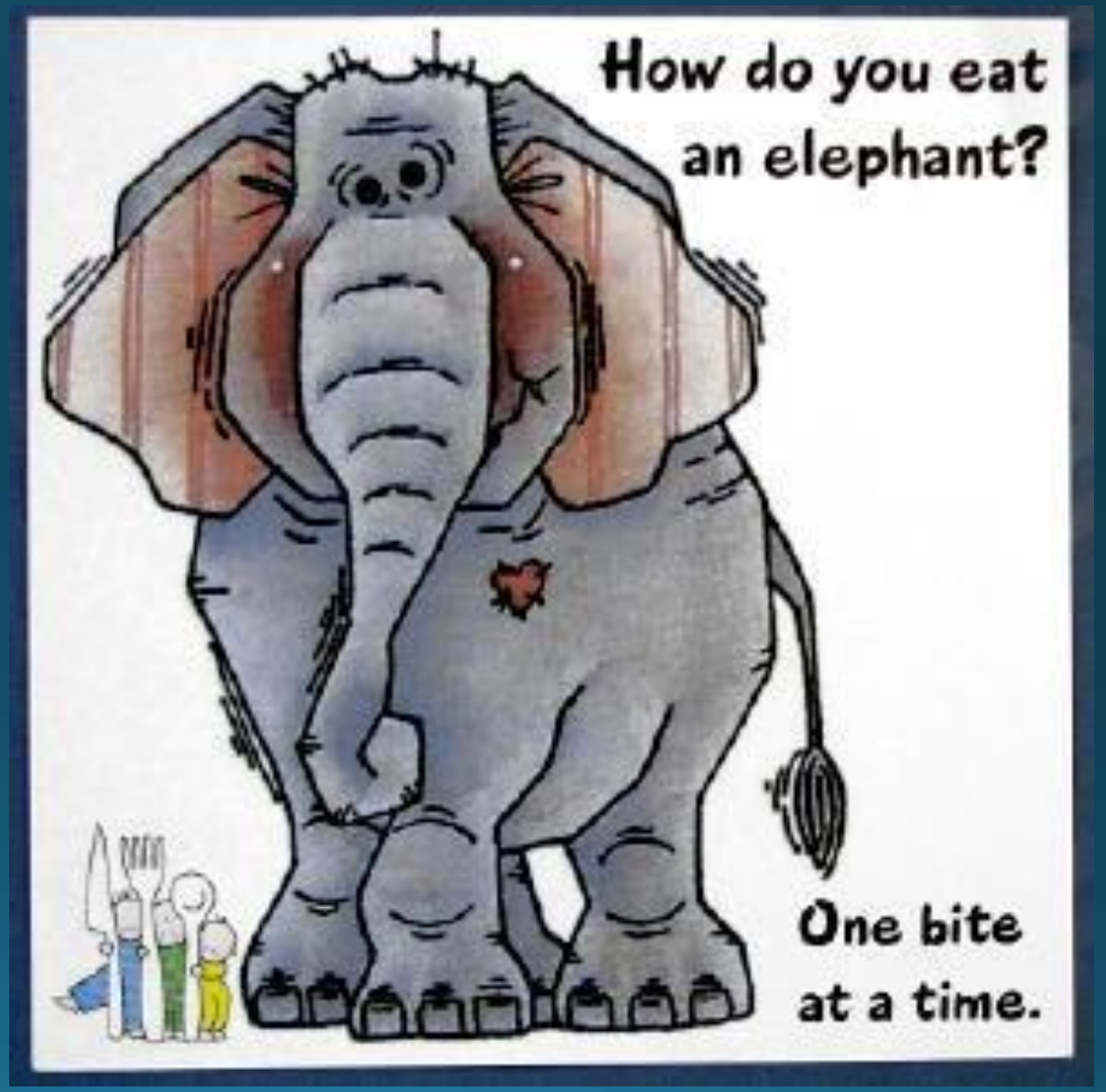
0 COMMENTS
COMMENT NOW

New data shows ransomware rates worldwide doubling and tripling in past 12 months.



http://www.darkreading.com/attacks-breaches/education-now-suffers-the-most-ransomware-attacks-/d/d-id/1326960

Student Data Protection Act



To Do List:

1. An LEA shall **adopt policies** to protect student data in accordance with this part and board rule, taking into account the specific needs and priorities of the LEA.

2. An LEA shall designate an individual to act as a **student data manager** to fulfill the responsibilities of a student data manager.

3. An LEA shall create and maintain an LEA:
    a. **data governance plan;** and
    b. **metadata dictionary**.

4. An LEA shall establish an **external research review process** for a request for data for the purpose of external research or evaluation.

Student Data Manager

If possible, an LEA shall designate the LEA's records officer as the student data manager.

IT Director

Assessment Director

Administrator

Responsibilities: Authorize and manage the sharing, outside of the education entity, of personally identifiable student data from a cumulative record for the education entity

Are you the Student Data Manager?:
https://lists.uen.org/mailman/listinfo/leastudentdataofficers

What can we share?

A student data manager MAY share a student's personally identifiable student data from a cumulative record with:

1. a school official;
2. a subpoena issued by a court
3. Directory Information
4. an authorized caseworker or other representative of the Department of Human Services;
5. If a student data manager receives a request to share data for the purpose of external research or evaluation, the student data manager shall:

(i) submit the request to the education entity's external research review process; and

(ii) fulfill the instructions that result from the review process.

The Department of Human Services, a school official, or the Utah Juvenile Court

….may share education information, including a student's personally identifiable student data, to improve education outcomes for youth:

(a) in the custody of, or under the guardianship of, the Department of Human Services;

(b) receiving services from the Division of Juvenile Justice Services;

(c) in the custody of the Division of Child and Family Services;

(d) receiving services from the Division of Services for People with Disabilities; or

(e) under the jurisdiction of the Utah Juvenile Court.

What cannot be shared?

Except as provided in this section or required by federal law, a student data manager may not share, outside of the education entity, personally identifiable student data from a cumulative record without a data authorization.

FERPA Exceptions

1. School Official
2. State or Federal program audit
3. Improve education (with signed agreement and assurances in place)

What is a Data Governance Plan?

"Data governance plan" means an education entity's comprehensive plan for managing education data that:

- incorporates reasonable data industry best practices to maintain and protect student data and other education-related data;
- provides for necessary technical assistance, training, support, and auditing;
- describes the process for sharing student data between an education entity and another person;
- describes the process for an adult student or parent to request that data be expunged; and
- is published annually and available on the education entity's website.

Data Security and Privacy Training: Best Practice Considerations

http://ptac.ed.gov/sites/default/files/Data%20Security%20and%20Management%20Training.pdf

Each person in an organization must understand why security is important both to them and the organization.

Who should be Trained?

Data Security and Management Training:

Best Practice Considerations

Make sure **ALL** employees are trained:

- new employees,
- current employees,
- contract workers,
- temporary workers,
- and even volunteers.
- At a minimum, any member of the staff, regardless of role, who has access to personally identifiable information (PII), should be trained to protect data confidentiality and preserve system security.

Use Existing Training Systems

Data Security and Management Training:

Best Practice Considerations

1. Integrate data security training within the context of broader employee education efforts.
2. Develop role-based training courses.
3. Incorporate breach detection and escalation in training
4. Include data security messages in all employee communications channels.
5. Create a culture of security in the organization.

What is a Meta Data Dictionary?

- "Metadata dictionary" means a complete list of an education entity's student data elements and other education-related data elements, that: (*lines 298-313)*
  - defines and discloses all data collected, used, stored, and shared by the education entity, including:
  - designates student data elements as necessary or optional
  - designates student data elements as required by state or federal law; and
  - without disclosing student data or security information, is displayed on the education entity's website.

Resources

- **USBE's Data Security and Privacy Webpage**

http://www.schools.utah.gov/data/Security-Privacy.aspx

- **Privacy Technical Assistance Council (PTAC)**

http://ptac.ed.gov/

- **Data Security and Privacy Webinar 2:**

March 1, Wednesday

10:00-11:00

https://uen.webex.com/uen/j.php?MTID=m7c5d6b275828aa6a3b460df61ce9e0f5