Pennsylvania Association of School Business Officials

Mailing Address:
P.O. Box 6993
Harrisburg, PA 17112-0993
Telephone 717-540-9551

www.pasbo.org

Office Location:
2608 Market Place
Harrisburg, PA 17110
FAX 717-540-1796

2015-2016 Workshop Series

SCHOOL RECORD RETENTION*

March 22, 2016

Webcast (9:30 – 11:00 AM)

Records management, retention, and destruction is an urgent security concern for many school districts. From data breach concerns, to compliance with Right To Know requests, to migrating from paper files to cloud-based databases – records management has been changing dramatically over the past ten years. This webcast will walk participants through the current legal landscape addressing the following essential questions:

- What constitutes a "record"?
- How long must records (Student, HR, Finance) be maintained? Which records?
- When must records be produced pursuant to a Right-To-Know request, or because of litigation?
- Is e-mail treated as an educational record? How long should e-mails be retained?
- What must a school district do in the event of a data breach?
- What should school officials look for in contracts where sensitive data is stored by a contractor?
- How should school districts protect sensitive data on personal cell phones and computers?

INTENDED AUDIENCE:
Business Managers, Department Directors

SPEAKER:
Mark W. Cheramie Walz, Esquire, Sweet, Stevens, Katz & Williams LLP

ANNOUNCEMENTS:

- All participants must sign-in on the Webcast Attendance Form found at the back of the handout packet for attendance/credit tracking. The site coordinator is asked to collect and submit information on every participant at your site. For credit to be given, forms must be returned to PASBO by March 29**.**
- Your webcast experience will be only as good as your Internet connection. If you are having technical difficulties, close all other browsers on your desktop and reconnect, or restart your computer. If you are disconnected at any time during the program, please repeat the log-on procedure to reconnect.
- You can submit a question at any time using the "Chat" function at the left side of your screen – type your question in the message box and click on "Enter" to send.
- Please track your CEU credits for PASBO Professional Registration. (*Professional Registration CEUs = 1)*
- Your evaluation of this program is important to us. The primary contact will receive an evaluation link via email. Please provide feedback to ensure that PASBO programs are meeting your needs.
- This program is being recorded to provide access to those not able to participate in the live program and serve as a review tool. Find information in your handout and check out the PASBO Store at http://www.pasbo.org/store_home.asp for other webcast titles.

Thank you for your participation!

Pennsylvania Association of School Business Officials

School Record Retention

March 22, 2016 Webcast

- For Internet audio - go to the "Start" tab and click "CONNECT"
- If you prefer to listen by phone - go to the "Start" tab, dial-in using the numbers provided, then click "I AM DIALED IN"

PASBO

1

Smart Business + Informed Decisions = Great Schools

Presenter

- Mark Cheramie Walz, Partner, Sweet, Stevens, Katz & Williams, LLP

PASBO

2

Smart Business + Informed Decisions = Great Schools

The 10 Commandments of Data Security and Data Management

Presented by:
Mark Cheramie Walz

tinyurl.com/pasbomarch22

SWEET | STEVENS | KATZ | WILLIAMS

3

(c) 2016

Key Term: Sensitive Data

- Any data that must be kept confidential by law, or that would otherwise be harmful to the IU if released publicly. Includes all sensitive employee records (payroll, disability, workers comp, discipline, etc.) and all FERPA records for students.

SWEET | STEVENS | KATZ | WILLIAMS

4

Commandment 1 - Nearly All Records Are Subject To Release

- FERPA = Allows students & parents to inspect "educational records."
- "Educational Records"
  - Contains "personally identifiable information" about a student or students
  - "maintained" by the agency or a person acting on behalf of that agency.
- Very broad

SWEET | STEVENS | KATZ | WILLIAMS

5

Examples of FERPA Records

- Student's cumulative file
- Special education documents (IEPs, progress monitoring, NOREP, evaluations, etc.)
- Health records
- Disciplinary records
- Emails about a student
- Student's work product that is maintained
- Counseling notes
- Report cards
- Attendance Records

SWEET | STEVENS | KATZ | WILLIAMS

6

NOT an education record:

- Records kept in the sole possession of the maker, are used only as a personal memory aid, and are not accessible or revealed to any other person except a temporary substitute for the maker of the record.
- Relevant as we consider e-mails and documents stored by individual users.

SWEET | STEVENS | KATZ | WILLIAMS

7

More on FERPA

- Doesn't matter:
  - Where the record is physically located
  - Why or for what purpose the record was created
  - Who created the record
  - Whether the record has anything to do with "education"
  - Whether the record is electronic or maintained in hard copy

SWEET | STEVENS | KATZ | WILLIAMS

8

Nuts and Bolts of FERPA

- Request must be in writing
- Right to inspect and copy
- May request to change / alter record
- Must respond within reasonable time
- May charge fee to copy, but not to inspect
- May only request and inspect Student's own records

SWEET | STEVENS | KATZ | WILLIAMS

9

Potential Records?

- What about student performance data stored online through a website?
- What about bulletin boards on Blackboard, or a moodle site?
- What about student work product through an educational website?

SWEET | STEVENS | KATZ | WILLIAMS

10

Educational Records Request

- Very common
- Often related to special education litigation
- In general, simply a request for a copy of all of a student's records
- Who determines what to send? Who pulls all the data? Do redactions have to be made? What about records teachers have maintained?

SWEET | STEVENS | KATZ | WILLIAMS

11

FERPA Applied

- Parent suspects that a Principal has been speaking poorly about boy Student behind his back, and may even be bullying Student himself for being "a girl." Parent sends a handwritten note to school with Student requesting all emails about Student.
- How do we address the request?

SWEET | STEVENS | KATZ | WILLIAMS

12

- No reference to FERPA in the request, should we treat it as a FERPA request?
- Leaving paper records aside, what e-mails should be provided?
  - Emails stored on District servers?
  - District determines the search terms
  - Emails stored by users? (Maintained by district?)
  - Emails in deleted folders?
  - Emails from teacher's personal account?
- Redactions required for other students' information
- Printed out emails?

SWEET | STEVENS | KATZ | WILLIAMS

13

Right To Know Law

- All agency records are public unless the agency can prove that they are exempt.
  - Exceptions such as privilege, security, trade secrets, etc.
- Records in possession of a party with whom the agency contracts to perform a governmental function are not exempt, and therefore are public records.
- Written request must identify the record sought with sufficient specificity to enable the agency to ascertain which records are being sought.

SWEET | STEVENS | KATZ | WILLIAMS

14

Is it a record?

- Requestor must prove that the request is for a "record" as defined by RTK. Two part test:
  - Information must document a "transaction or activity of the agency"; and
  - Information must be "created, received, or retained" in connection with the activity of the agency.

15

Notes on RTK

- Not required to create records or compile, format, or organize a record.
- Redaction may be required.
- Don't have to provide information that would jeopardize network security.
- Timeline for response is a mere 5 days. (May be extended with written notice to the requestor).
- Record shall be provided in the medium requested if it exists in that medium, otherwise provided in the medium in which it exists.

SWEET | STEVENS | KATZ | WILLIAMS

16

RTK Examples

- Surveillance video of student sit-in
- Training documents for bus drivers
- Configuration of Internet filters

SWEET | STEVENS | KATZ | WILLIAMS

17

Commandment 2 - All Stored Data Must Be Preservable

- Litigation Hold - means that all data related to that employee, or related to a student, or related to an incident, must be preserved AS IS.
- How to undertake? Who is responsible? How is it "held"?
- Consequences for non-compliance are substantial.
- Here again, doesn't matter where it is stored or by whom it is stored if a contractor is involved.

SWEET | STEVENS | KATZ | WILLIAMS

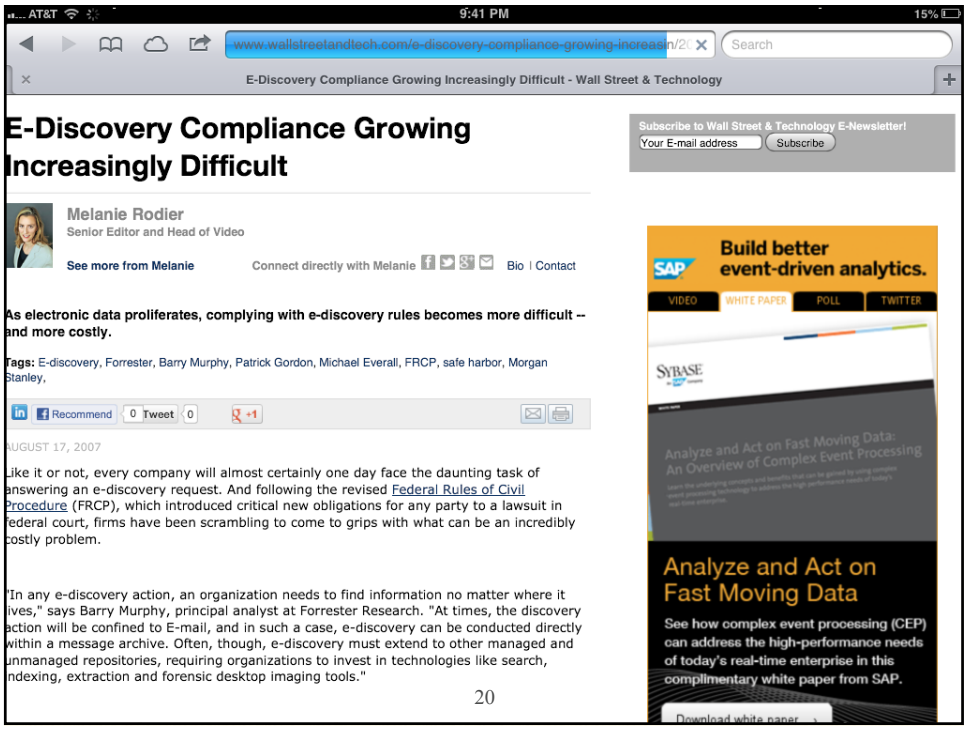
18

Spoliation

- AKA - Adverse Inference Instruction
- If records were supposed to be maintained, but we destroyed them of failed to maintain them, the jury is instructed to essentially "assume the worst" about the missing evidence.
- Makes winning very difficult!
- Can be safe harbor for routine deletion so long as it is according to policy and is rigorously adhered to, and there were good faith efforts to preserve the data sought.

SWEET | STEVENS | KATZ | WILLIAMS

19



20

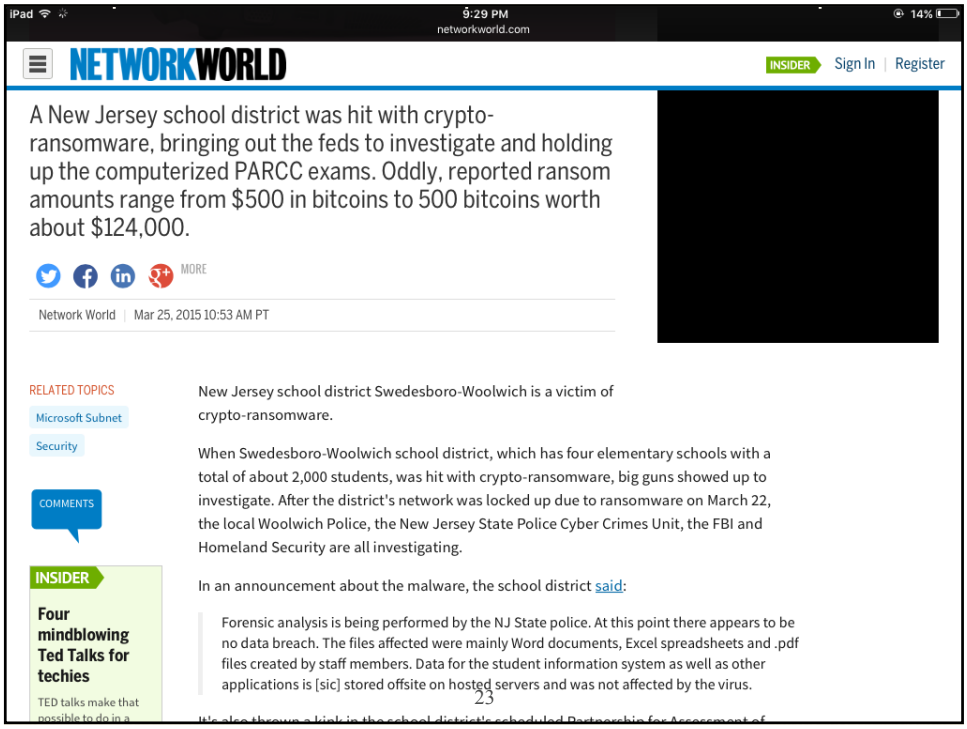
Commandment 3 - Back Up All Sensitive Data

- Critical in case we need to restore following data breach, loss, outage, etc.
- Individual files stored in unauthorized locations are NOT backed up (e.g. Thumb drive, unauthorized cloud storage, etc.)
- Back-ups play a key role in determining what is lost in the event of a theft or loss of a device.

SWEET | STEVENS | KATZ | WILLIAMS

21

22



iPad 9:29 PM networkworld.com 14%

NETWORKWORLD

INSIDER Sign In | Register

A New Jersey school district was hit with crypto-ransomware, bringing out the feds to investigate and holding up the computerized PARCC exams. Oddly, reported ransom amounts range from $500 in bitcoins to 500 bitcoins worth about $124,000.

MORE

Network World | Mar 25, 2015 10:53 AM PT

RELATED TOPICS

Microsoft Subnet

Security

COMMENTS

INSIDER

Four mindblowing Ted Talks for techies

TED talks make that possible to do in a

New Jersey school district Swedesboro-Woolwich is a victim of crypto-ransomware.

When Swedesboro-Woolwich school district, which has four elementary schools with a total of about 2,000 students, was hit with crypto-ransomware, big guns showed up to investigate. After the district's network was locked up due to ransomware on March 22, the local Woolwich Police, the New Jersey State Police Cyber Crimes Unit, the FBI and Homeland Security are all investigating.

In an announcement about the malware, the school district said:

> Forensic analysis is being performed by the NJ State police. At this point there appears to be no data breach. The files affected were mainly Word documents, Excel spreadsheets and .pdf files created by staff members. Data for the student information system as well as other applications is [sic] stored offsite on hosted servers and was not affected by the virus.

23

Commandment 4 - Must Vet All Contractors Storing Sensitive Data

- Ensure that contractors utilize appropriate data security precautions and backups.
- Review contracts to ensure legal compliance.
- Seek provisions assuring FERPA compliance per educational official exception, where student data involved.
- Ensure contractor is obligated to notify IU in event of a data breach.

SWEET | STEVENS | KATZ | WILLIAMS

24

Commandment 5 - Have Data Breach Response Plan

- Common Data Breaches
  - Lost laptop
  - Lost mobile device
  - Lost thumb drive, or other portable media
  - Content mistakenly posted publicly
  - Contractor data breach
  - Errant e-mail sent to wrong party

SWEET | STEVENS | KATZ | WILLIAMS

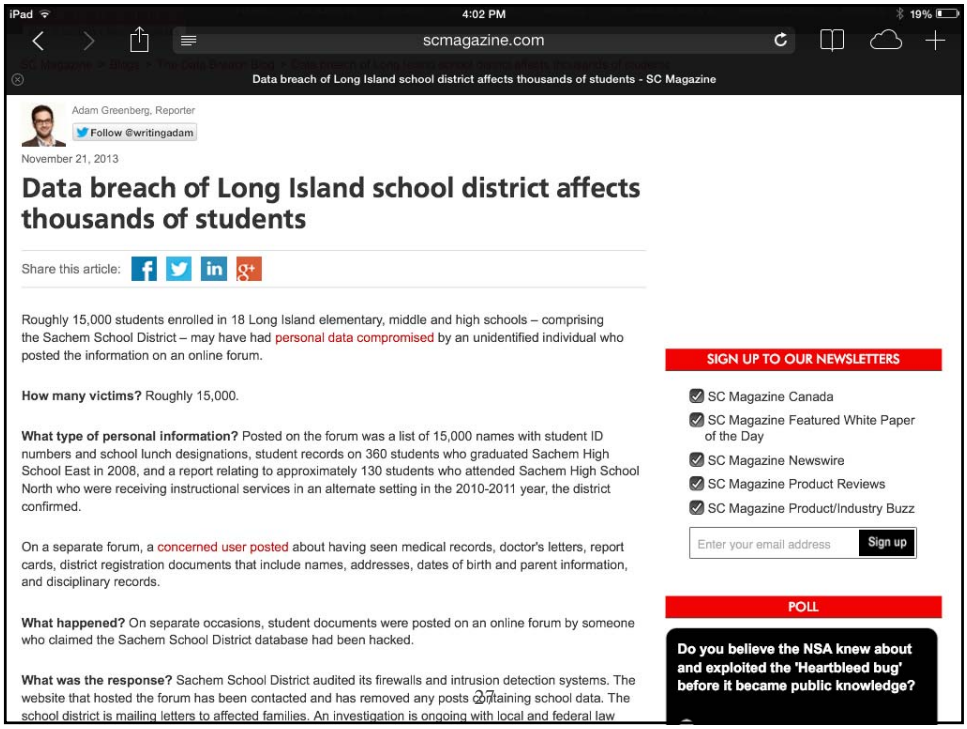
25

Less Common Data Breaches

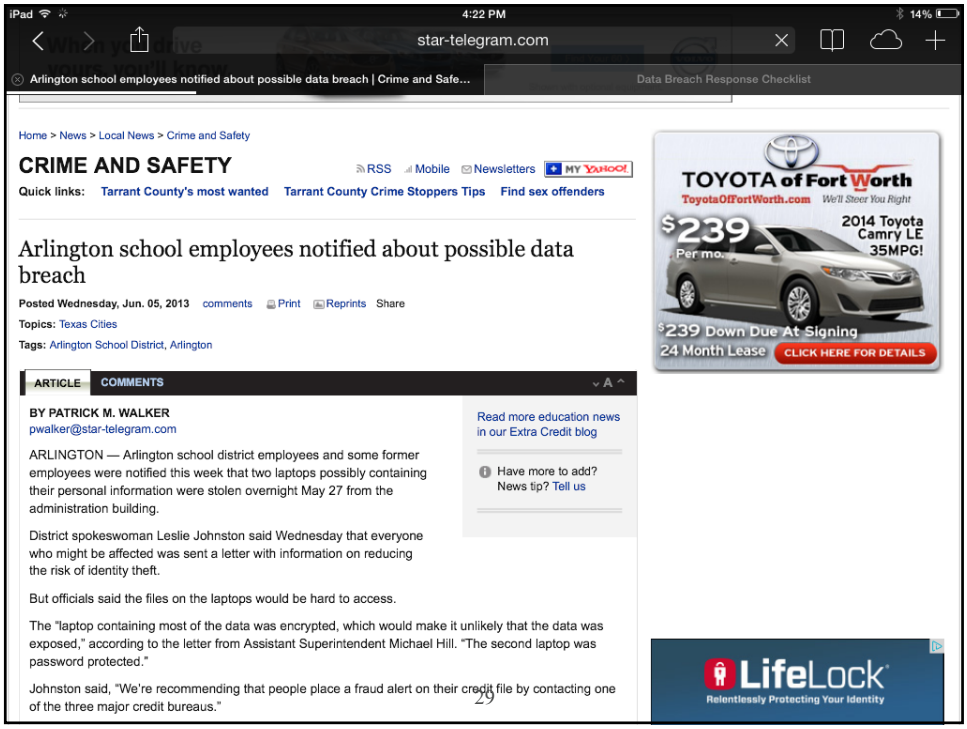
- Firewall failure
- Hacking (whether from internal or external sources)
- Rogue employee data dump

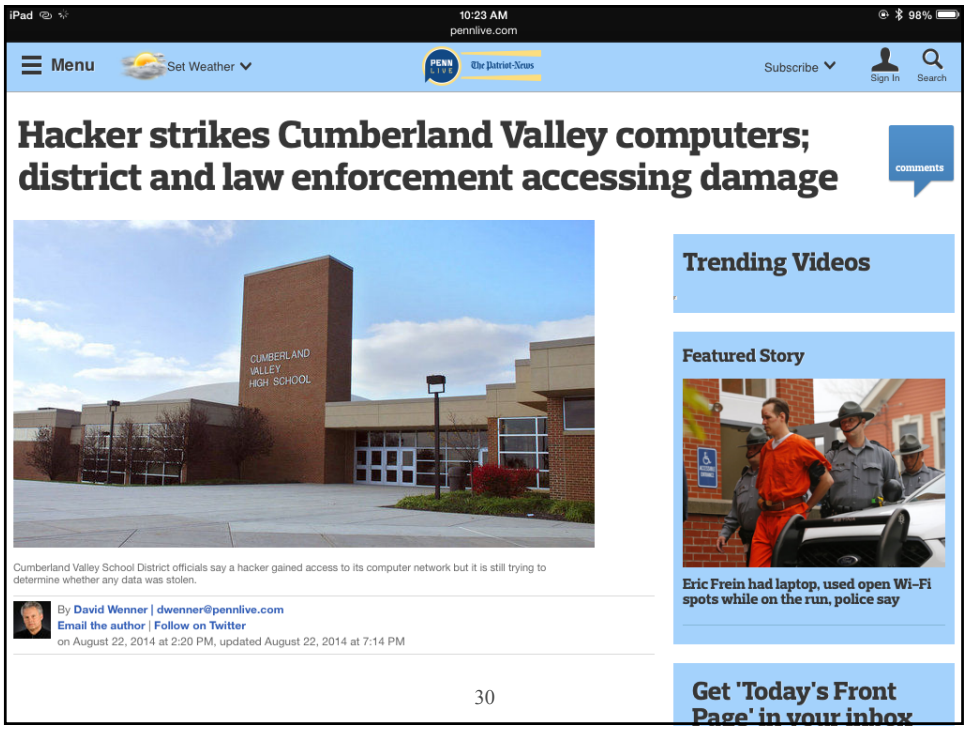
SWEET | STEVENS | KATZ | WILLIAMS

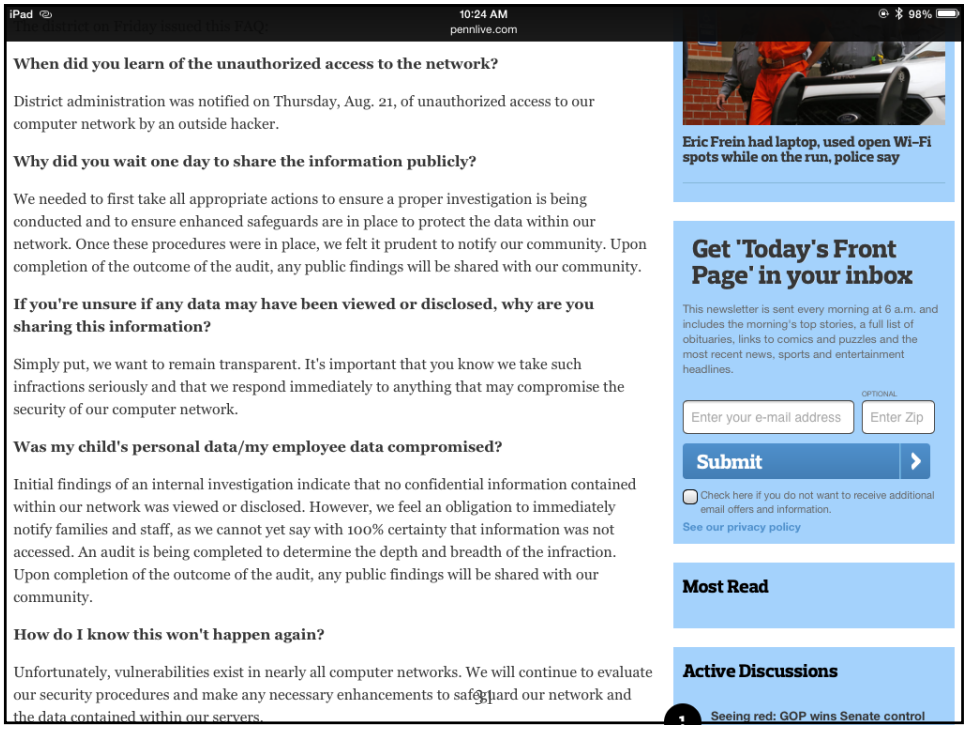
26


iPad
4:02 PM
19%
scmagazine.com
Data breach of Long Island school district affects thousands of students - SC Magazine
Adam Greenberg, Reporter
Follow @writingadam
November 21, 2013
Data breach of Long Island school district affects thousands of students
Share this article:
Roughly 15,000 students enrolled in 18 Long Island elementary, middle and high schools – comprising the Sachem School District – may have had personal data compromised by an unidentified individual who posted the information on an online forum.
How many victims? Roughly 15,000.
What type of personal information? Posted on the forum was a list of 15,000 names with student ID numbers and school lunch designations, student records on 360 students who graduated Sachem High School East in 2008, and a report relating to approximately 130 students who attended Sachem High School North who were receiving instructional services in an alternate setting in the 2010-2011 year, the district confirmed.
On a separate forum, a concerned user posted about having seen medical records, doctor's letters, report cards, district registration documents that include names, addresses, dates of birth and parent information, and disciplinary records.
What happened? On separate occasions, student documents were posted on an online forum by someone who claimed the Sachem School District database had been hacked.
What was the response? Sachem School District audited its firewalls and intrusion detection systems. The website that hosted the forum has been contacted and has removed any posts containing school data. The school district is mailing letters to affected families. An investigation is ongoing with local and federal law
SIGN UP TO OUR NEWSLETTERS
SC Magazine Canada
SC Magazine Featured White Paper of the Day
SC Magazine Newswire
SC Magazine Product Reviews
SC Magazine Product/Industry Buzz
Enter your email address
Sign up
POLL
Do you believe the NSA knew about and exploited the 'Heartbleed bug' before it became public knowledge?

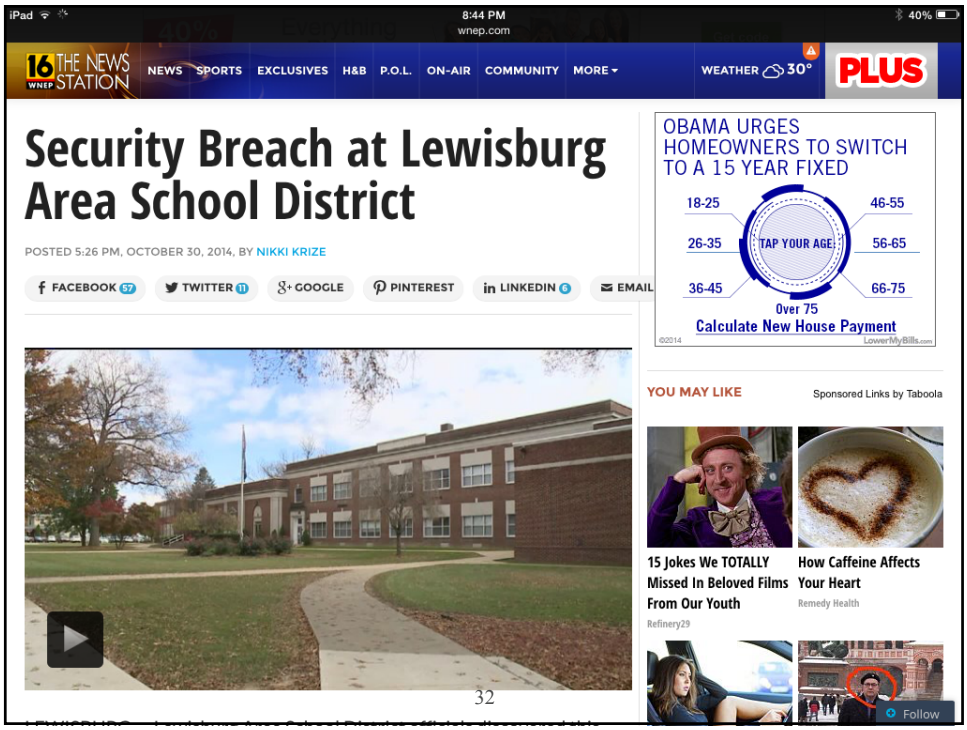

iPad
4:03 PM
18%
esecurityplanet.com
Virginia School District Admits Data Breach - eSecurity Planet
Virginia School District Admits Data Breach
Student names, addresses, phone numbers, dates and places of birth, dates of attendance, and school schedules were exposed.
By Jeff Goldman | Posted January 10, 2014
Share
Virginia's Loudoun County Public Schools (LCPS) recently acknowledged that an error made by third-party provider Risk Solutions International (RSI) made student and staff information accessible online (h/t Washington Post).
RSI, which had been maintaining an emergency management plan Web site for LCPS, conducted technical testing on November 4, 2013, December 19, 2013, and December 24, 2013. "Security protocols were not followed and the data was exposed," according to an LCPS statement. "The exact date of the incident has not been determined nor has the length of time the information was exposed."
"Risk Solutions International acknowledged that human error, on their part, was the cause of the data breach," LCPS superintendent Edgar B. Hatrick stated in a separate announcement. "I have insisted that they take all necessary steps to ensure the complete privacy of our data."
8 Ways to Better Monitor Network Security Threats in the Age of BYOD
Download Now
When LCPS was notified on January 2, 2014 that the information was accessible through a Web search, it contacted RSI requesting a shutdown. It took until January 8, 2014 to remove caches of the documents to ensure the information was no longer accessible.
Information exposed includes student names, addresses, phone numbers, dates and places of birth, dates of attendance, and school schedules. According to the Washington Post, one school's locker combinations were also exposed.
Photo courtesy of Shutterstock.
28
Silver Peak
A LEADER IN THE
GARTNER
MAGIC QUADRANT
FOR WAN OPTIMIZATION
View The Report
White Papers
eBooks
Top White Papers and Webcasts
Magic Quadrant for Endpoint Protection Platforms
Symantec.
By 2017, more than 50% of end-user devices will be restricted to running only apps that have been pre-inspected for security and privacy risks, up from 20% today. In today's market, the endpoint protection platform provides a collection of security utilities to protect PCs and tablets. Vendors in this market compete on the quality of their protection capabilities, the depth and breadth of features, and the ease of administration. Read this Gartner Magic Quadrant analyst report for an in-depth comparison of 17 ...


iPad
4:22 PM
14%
star-telegram.com
Arlington school employees notified about possible data breach | Crime and Safe...
Data Breach Response Checklist
Home > News > Local News > Crime and Safety
CRIME AND SAFETY
RSS Mobile Newsletters MY YAHOO!
Quick links: Tarrant County's most wanted Tarrant County Crime Stoppers Tips Find sex offenders
Arlington school employees notified about possible data breach
Posted Wednesday, Jun. 05, 2013 comments Print Reprints Share
Topics: Texas Cities
Tags: Arlington School District, Arlington
ARTICLE COMMENTS
BY PATRICK M. WALKER
pwalker@star-telegram.com
ARLINGTON — Arlington school district employees and some former employees were notified this week that two laptops possibly containing their personal information were stolen overnight May 27 from the administration building.
District spokeswoman Leslie Johnston said Wednesday that everyone who might be affected was sent a letter with information on reducing the risk of identity theft.
But officials said the files on the laptops would be hard to access.
The "laptop containing most of the data was encrypted, which would make it unlikely that the data was exposed," according to the letter from Assistant Superintendent Michael Hill. "The second laptop was password protected."
Johnston said, "We're recommending that people place a fraud alert on their credit file by contacting one of the three major credit bureaus."
Read more education news in our Extra Credit blog
Have more to add? News tip? Tell us
TOYOTA of Fort Worth
ToyotaOfFortWorth.com We'll Steer You Right
$239 Per mo.
2014 Toyota Camry LE 35MPG!
$239 Down Due At Signing
24 Month Lease
CLICK HERE FOR DETAILS
LifeLock
Relentlessly Protecting Your Identity

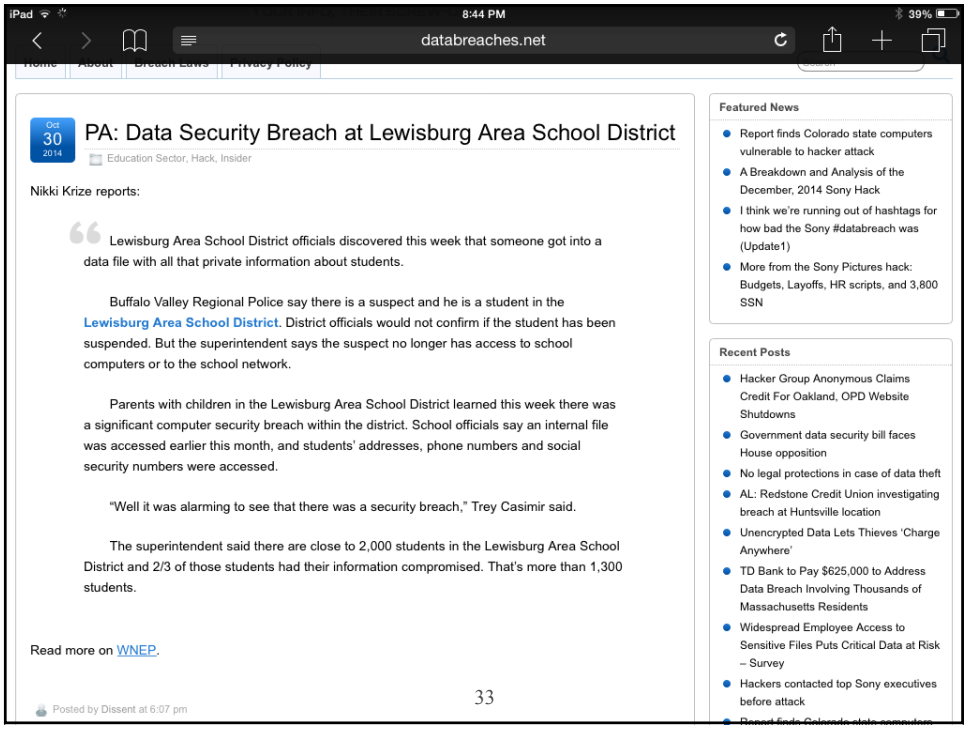

iPad
10:23 AM
pennlive.com
98%
Menu
Set Weather
The Patriot-News
Subscribe
Sign In
Search
Hacker strikes Cumberland Valley computers; district and law enforcement accessing damage
comments
CUMBERLAND VALLEY HIGH SCHOOL
Cumberland Valley School District officials say a hacker gained access to its computer network but it is still trying to determine whether any data was stolen.
By David Wenner | dwenner@pennlive.com
Email the author | Follow on Twitter
on August 22, 2014 at 2:20 PM, updated August 22, 2014 at 7:14 PM
Trending Videos
Featured Story
Eric Frein had laptop, used open Wi-Fi spots while on the run, police say
Get 'Today's Front Page' in your inbox


iPad
10:24 AM
pennlive.com
98%
When did you learn of the unauthorized access to the network?
District administration was notified on Thursday, Aug. 21, of unauthorized access to our computer network by an outside hacker.
Why did you wait one day to share the information publicly?
We needed to first take all appropriate actions to ensure a proper investigation is being conducted and to ensure enhanced safeguards are in place to protect the data within our network. Once these procedures were in place, we felt it prudent to notify our community. Upon completion of the outcome of the audit, any public findings will be shared with our community.
If you're unsure if any data may have been viewed or disclosed, why are you sharing this information?
Simply put, we want to remain transparent. It's important that you know we take such infractions seriously and that we respond immediately to anything that may compromise the security of our computer network.
Was my child's personal data/my employee data compromised?
Initial findings of an internal investigation indicate that no confidential information contained within our network was viewed or disclosed. However, we feel an obligation to immediately notify families and staff, as we cannot yet say with 100% certainty that information was not accessed. An audit is being completed to determine the depth and breadth of the infraction. Upon completion of the outcome of the audit, any public findings will be shared with our community.
How do I know this won't happen again?
Unfortunately, vulnerabilities exist in nearly all computer networks. We will continue to evaluate our security procedures and make any necessary enhancements to safeguard our network and the data contained within our servers.
Eric Frein had laptop, used open Wi-Fi spots while on the run, police say
Get 'Today's Front Page' in your inbox
This newsletter is sent every morning at 6 a.m. and includes the morning's top stories, a full list of obituaries, links to comics and puzzles and the most recent news, sports and entertainment headlines.
OPTIONAL
Enter your e-mail address
Enter Zip
Submit
Check here if you do not want to receive additional email offers and information.
See our privacy policy
Most Read
Active Discussions
Seeing red: GOP wins Senate control

31


iPad
8:44 PM
wnep.com
40%
16 THE NEWS STATION WNEP
NEWS SPORTS EXCLUSIVES H&B P.O.L. ON-AIR COMMUNITY MORE
WEATHER 30°
PLUS
Security Breach at Lewisburg Area School District
POSTED 5:26 PM, OCTOBER 30, 2014, BY NIKKI KRIZE
FACEBOOK 57
TWITTER 11
GOOGLE
PINTEREST
LINKEDIN 6
EMAIL
OBAMA URGES HOMEOWNERS TO SWITCH TO A 15 YEAR FIXED
18-25
26-35
36-45
46-55
56-65
66-75
Over 75
TAP YOUR AGE
Calculate New House Payment
©2014
LowerMyBills.com
YOU MAY LIKE
Sponsored Links by Taboola
15 Jokes We TOTALLY Missed In Beloved Films From Our Youth
Refinery29
How Caffeine Affects Your Heart
Remedy Health
Follow

32


iPad
8:44 PM
39%
databreaches.net
Oct
30
2014
PA: Data Security Breach at Lewisburg Area School District
Education Sector, Hack, Insider
Nikki Krize reports:
Lewisburg Area School District officials discovered this week that someone got into a data file with all that private information about students.
Buffalo Valley Regional Police say there is a suspect and he is a student in the Lewisburg Area School District. District officials would not confirm if the student has been suspended. But the superintendent says the suspect no longer has access to school computers or to the school network.
Parents with children in the Lewisburg Area School District learned this week there was a significant computer security breach within the district. School officials say an internal file was accessed earlier this month, and students' addresses, phone numbers and social security numbers were accessed.
"Well it was alarming to see that there was a security breach," Trey Casimir said.
The superintendent said there are close to 2,000 students in the Lewisburg Area School District and 2/3 of those students had their information compromised. That's more than 1,300 students.
Read more on WNEP.
Posted by Dissent at 6:07 pm
33
Featured News
Report finds Colorado state computers vulnerable to hacker attack
A Breakdown and Analysis of the December, 2014 Sony Hack
I think we're running out of hashtags for how bad the Sony #databreach was (Update1)
More from the Sony Pictures hack: Budgets, Layoffs, HR scripts, and 3,800 SSN
Recent Posts
Hacker Group Anonymous Claims Credit For Oakland, OPD Website Shutdowns
Government data security bill faces House opposition
No legal protections in case of data theft
AL: Redstone Credit Union investigating breach at Huntsville location
Unencrypted Data Lets Thieves 'Charge Anywhere'
TD Bank to Pay $625,000 to Address Data Breach Involving Thousands of Massachusetts Residents
Widespread Employee Access to Sensitive Files Puts Critical Data at Risk – Survey
Hackers contacted top Sony executives before attack


What are you required to do in light of a data breach?
SWEET | STEVENS | KATZ | WILLIAMS
34

PA Data Breach Law

- Breach of Personal Information Notification Act (73 P.S. § 2301)
- "Entity." A State agency, a political subdivision of the Commonwealth or an individual or a business doing business in this Commonwealth.

SWEET | STEVENS | KATZ | WILLIAMS

35

Notification of Breach

- (a) General rule.--An entity that maintains, stores or manages computerized data that includes personal information shall provide notice of any breach of the security of the system following discovery of the breach of the security of the system to any resident of this Commonwealth whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person.
- The notice shall be made without unreasonable delay.*

SWEET | STEVENS | KATZ | WILLIAMS

36

- "Breach of the security of the system." The unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information maintained by the entity as part of a database of personal information regarding multiple individuals and that causes or the entity reasonably believes has caused or will cause loss or injury to any resident of this Commonwealth.

SWEET | STEVENS | KATZ | WILLIAMS

37

- maintained by the entity as part of a database of personal information regarding multiple individuals and that causes or the entity reasonably believes has caused or will cause loss or injury
- Personal Information:
  - (1) An individual's first name or first initial and last name in combination with and linked to any one or more of the following data elements when the data elements are not encrypted or redacted:
    - (i) Social Security number.
    - (ii) Driver's license number or a State identification card number issued in lieu of a driver's license.
    - (iii) Financial account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account.

SWEET | STEVENS | KATZ | WILLIAMS

38

Other details

- Must provide notice of the breach if encrypted information is accessed and acquired in an unencrypted form OR if the security breach is linked to a breach of the security of the encryption, OR if the security breach involves a person with access to the encryption key.
- Contractor/Vendor - required to notify the entity. It is then the duty of the entity to make the notification required by the law.
- If more than 1000 notified, must also notify credit reporting agencies.

SWEET | STEVENS | KATZ | WILLIAMS

39

Exception

- (a) Information privacy or security policy.--An entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of personal information and is consistent with the notice requirements of this act shall be deemed to be in compliance with the notification requirements of this act if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

SWEET | STEVENS | KATZ | WILLIAMS

40

Summary of PA Data Breach Law

- Applies in a narrow instance to very specific and highly sensitive information.
- Definitely does not apply to many school district data breaches.
- Requires timely and specific response.
- May be costly response for large-scale breach, of breach whose scale is unknown.

SWEET | STEVENS | KATZ | WILLIAMS

41

If not required, then what are best practices?

SWEET | STEVENS | KATZ | WILLIAMS

42

Planning Ahead

- Set backup frequency to better plan data breach response.
- Plan for remote tracking or lost devices and securing authority to remotely wipe the contents of lost devices without other approval.
- Train staff to utilize approved cloud based storage instead of thumb drives for transferring files.
- Plan clean-up of downloaded files and other cached data at regular intervals.
- Password protect and/or encrypt data on school owned devices.
- Adopt policies and procedures for safeguarding data on employee owned devices.

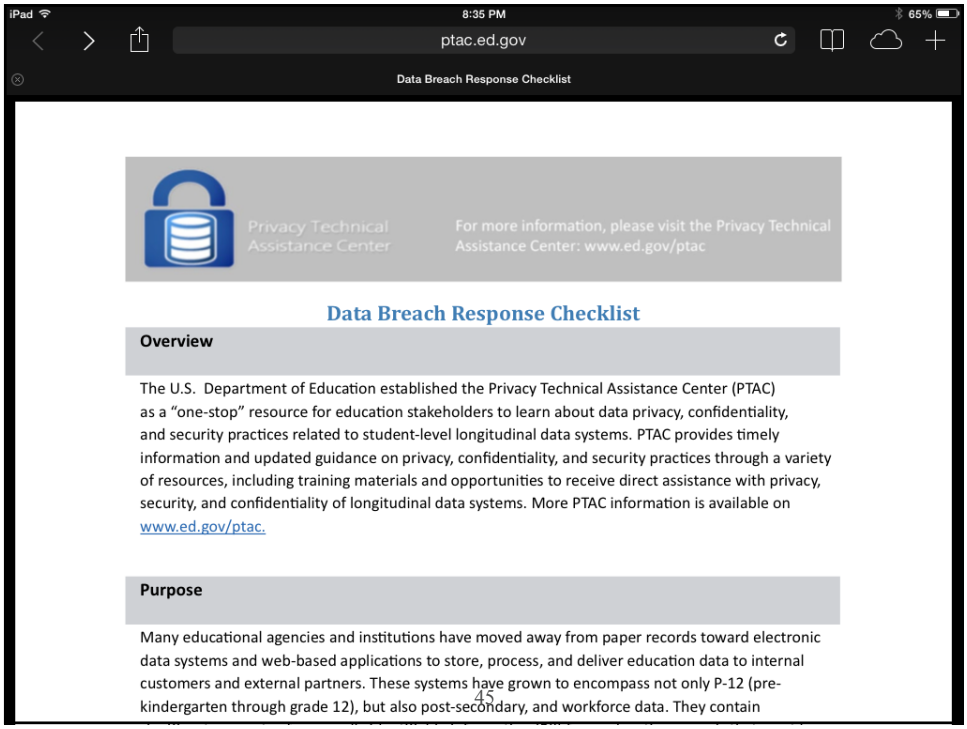
SWEET | STEVENS | KATZ | WILLIAMS

43

Data Breach Response Plan

SWEET | STEVENS | KATZ | WILLIAMS

44



45

Commandment 6 - Destroy Irrelevant and Outdated Records

- Student record do not need to be kept for 99 years, that "guideline" was repealed years ago.
- Should have a records retention and destruction policy and all employees should be trained to follow it.
- Work together within the administration to establish parameters for each department that everyone is capable of following.
- This ensures that data that is not longer relevant is destroyed, freeing up space and resources, but importantly removing any risk associated with data security.

SWEET | STEVENS | KATZ | WILLIAMS

46

tinyurl.com/pasborecords

47

Related: Destroy Temporary Data

- Examples: Chat logs, video surveillance, voicemails, text messages, fax cover sheets, post-it notes, etc.
- Define "records" to exclude these temporary data sources in record retention policy.

48

Commandment 7 - Mind The Metadata

- The internal data on files can tell who created the file, when it was edited, what changes were made, who sent a document, etc.
- It is relevant not only in litigation, but also to Parents and Staff who may submit a RTK request.
- Under RTK, must provide document in the form requested if it exists in the form requested. (e.g. Can't turn MS Word file into PDF prior to sending if request is for the MS Word file).
- When sending files outside the organization, use metadata tools to clean metadata from the file prior to sending.

SWEET | STEVENS | KATZ | WILLIAMS

49

Commandment 8 - Adopt and Enforce a Mobile Device Policy

- Require all employees to utilize data security standards on their personal devices.
- These include passwords on devices, and ensuring that sensitive data is never stored locally on a personal device.
- Also includes provisions for the termination of access upon retirement or separation to ensure data integrity.

SWEET | STEVENS | KATZ | WILLIAMS

50

More on Mobile Devices

- Data belonging to the organization that is stored on a personal mobile device is still subject to RTK, and would likely still be subject to a FERPA request.
- Need to utilize approved resources only to ensure that the data needed can be quickly recovered, preserved, and produced.

SWEET | STEVENS | KATZ | WILLIAMS

51

Commandment 9 - Emails Are a Record of Government

- Always use school account, not personal account, to conduct business (including board members).
- Utilize an email archiver to retain a searchable record of all messages into and out of the organization.
- Emails are subject to FERPA and RTK requests, and staff MUST be trained on the level of professionalism needed over email. Don't write anything you wouldn't want a parent or employee to see.
- Work with staff on when to speak on the phone, or in person, instead of utilizing email.

SWEET | STEVENS | KATZ | WILLIAMS

52

Commandment 10 - Establish a Culture of Data Security

- Establish a culture where security matters - from passwords, to encryption, to data back-ups.
- Don't just turn the other way when you find out that an employee is storing data in an unapproved resource.
- The only way data stays secure in large organizations is with team buy-in, where all employees are aware of expectations and policies.

SWEET | STEVENS | KATZ | WILLIAMS

53

Time for Questions

- Send text questions using the "Chat" function at the left side of your screen.
- Type message in box and click "Enter" to send.

PASBO

54

Smart Business + Informed Decisions = Great Schools

REMINDER:
Webcast sites are asked to have every participant sign-in on the Attendance Form and return to the PASBO Office for attendance and credit purposes.

Forms must be received by March 29.

Thank you for your participation!

PASBO

55

Smart Business + Informed Decisions = Great Schools

Join us for these upcoming programs:

- ELEMENTS OF LEADERSHIP & MANAGEMENT – April 5/Harrisburg
- ELEMENTS OF FOOD SERVICE – April 6/Mars; April 8/Kulpsville
- TECHNOLOGY SECURITY- April 7/Webcast
- ELEMENTS OF FACILITIES MANAGEMENT – April 13/Kulpsville; April 14/Mars
- STAYING OUT OF TROUBLE WITH YOUR TRANSPORTATION AUDIT – April 15/Webcast

For info, visit www.pasbo.org/workshops

PASBO

56

Smart Business + Informed Decisions = Great Schools

Join us for these upcoming programs:

- APPLICATIONS IN REVENUES – April 19/Harrisburg
- UNIFORM GRANT GUIDANCE – April 19/Webcast
- ELEMENTS OF SCHOOL LAW & ORGANIZATION – April 26/Kulpsville; April 28/Mars
- HOW TO NAVIGATE EMPLOYEE LEAVES – April 29/Mars; May 4/Kulpsville; May 5/Grantville

For info, visit www.pasbo.org/workshops

PASBO

57

Smart Business + Informed Decisions = Great Schools

PASBO
P.O. Box 6993
Harrisburg, PA 17112
(717) 540-9551
Fax (717) 540-1796
www.pasbo.org

SCHOOL RECORD RETENTION
Webcast Recording Order Form

Records management, retention, and destruction is an urgent security concern for many school districts. From data breach concerns, to compliance with Right To Know requests, to migrating from paper files to cloud-based databases – records management has been changing dramatically over the past ten years. This webcast will walk participants through the current legal landscape addressing the following essential questions:

- What constitutes a "record"?
- How long must records (Student, HR, Finance) be maintained? Which records?
- When must records be produced pursuant to a Right-To-Know request, or because of litigation?
- Is e-mail treated as an educational record? How long should e-mails be retained?
- What must a school district do in the event of a data breach?
- What should school officials look for in contracts where sensitive data is stored by a contractor?
- How should school districts protect sensitive data on personal cell phones and computers?

A recording of the webcast program will be available for download approximately one week after the program date. Whether you use it as a review or share it with fellow employees unable to attend the live webcast, the information is at your fingertips!

Fill out and send your order form to PASBO today!

Name:_____ Title:_____

School Entity/Employer:_____

Address:_____

City:_____ State:_____ Zip: _____

Phone:_____ Ext._____ Fax:_____

Email:_____

If you are tax exempt, enter your tax ID here:_____

Attendee Early Bird Discount Offer – April 5 deadline!

Webcast Attendee by April 5* *(*Available to paid webcast attendees only)*	**Non-Attendee or after April 5**
Online Access @ $10	PASBO Member Online Access @ $40 Non-member Online Access @ $65
Total Amount Due $_____	**Total Amount Due $_____**

METHOD OF PAYMENT (Select one – *Payment required with order*)

❒ Check Made Payable to PASBO ❒ Credit Card

Account Number:_____ Expiration:_____

Cardholder's Name:_____

Signature:_____

Check out other available webcast recordings at http://www.pasbo.org/store_home.asp

PASBO Webcast Attendance Form

ALL ATTENDEES SIGN IN ON THIS SHEET

Use this form to submit the names of <u>all attendees</u> viewing the webcast at your location.
All participating LEAs will be charged one webcast registration fee. (There is NOT a fee for additional attendees from the same LEA.)

Webcast Date: 3/22/16 Webcast Title: School Record Retention

Paid Registrant: _____ Registrant's LEA/organization: _____

You must sign-in on the form below (including the paid registrant if watching the program) to be counted as attending.
If you are requesting PASBO CEU or Accountant CPE Credit, you must check the appropriate column and provide your email address.

By completing below, I certify that I participated in the entire live webcast presentation.

PRINT NAME CLEARLY	*JOB TITLE*	*SCHOOL/ORGANIZATION*	*EMAIL (Required for Credit)*	*CEU Credit*	*CPE Credit*

Please return this form <u>no later than 7 days following the program date</u> by ONE of the following methods.
Scan and email to kpierich@pasbo.org ♦ Fax to 717-540-1796 *(Cover sheet is not required)* ♦ Mail to PASBO, 2608 Market Place, Harrisburg, PA 17110
CPE Certificates will be mailed. Credit is available for the live program only, not the recording.