SLRMA SM
School Leaders Risk Management Association
UPDATE
September 2017


The invention of cloud computing services - those services that allow users to store, access, and process data over the Internet or other networks – significantly altered how organizations retain and access collected data. Cloud computing services are widely used because they provide cost-effective, readily-scalable access to state-of-the-art information technology for data retention.

Like many organizations, school districts can put cloud computing services to powerful use. School districts engaging the services of cloud computing providers, can get out of the data storage business and devote more resources to their primary mission: providing students with a quality education.

All computerized data storage systems run the risk of data breach. Organizations employing cloud services face different risks by entrusting the security of their data to third parties. Data security experts often talk in terms of *when* – not *if* – a data breach will occur. Considering the myriad ways that data thieves can get access to information, such as malware, ransomware, phishing attacks, and old-fashioned physical removal of laptops or servers, data breaches seem inevitable.

The statistics on data breaches are formidable. As noted in the 2017 Cost of Data Breach Study: United States, issued by the Ponemon Institute, the average cost of a U.S. data breach per lost or stolen record increased 2% from 2016 to $225 per record.[1] Moreover, the frequency of breaches in the U.S. is on the rise, reaching an all-time high in 2016 of 1,091 reported breaches.[2] Although the vast majority of breaches were in the business sector, the educational sector accounted for 9% of reported breaches. Educational organizations are literally a hacker's treasure trove of information, and are therefore prime targets for attack. In early 2017, a notorious email phishing scam involving W2 forms exposed the vulnerability of school districts to such cyber threats. Despite an Internal

1 "IBM & Ponemon Institute: Cost of a Data Breach Dropped 10 Percent Globally in 2017 Study." PR Newswire, June 20, 2017. The full Ponemon Institute's 2017 Cost of Data Breach Study: United States can be downloaded at https://www-01.ibm.com/marketing/iwm/dre/signup?source=urx-15764&S_PKG=ov58458.

2 "Data Breaches Increase 40 Percent in 2016, Finds New Report from Identity Theft Resource Center and CyberScout." January 19, 2017. Identity Theft Resource Center website, available at http://www.idtheftcenter.org/2016databreaches.html.

*continued on page 3*

# Checklist Excerpt

## Cybersecurity & Privacy Risk Management for Cloud Computing – Self-Audit Checklist and Best Practices for School Districts

### II. Cybersecurity Best Practices, Generally

Does the district have information security policies in place that address the collection, handling, use, and storage of personal information (in any format) and meet applicable legal and regulatory requirements? Do such policies address:

The retention and secure destruction of personal information? ☐ Yes ☐ No

Restrictions on the access to personal information to those personnel with a legitimate business purpose? ☐ Yes ☐ No

Secure passwords and authentication requirements (e.g., password complexity and secure storage requirements, account lockout procedures, authentication bypass protections)? ☐ Yes ☐ No

Secure storage and transmission of personal information (e.g., through encryption)? ☐ Yes ☐ No

Secure access to the network (e.g., network segmentation, use of network monitoring tools, endpoint security implementation, user access limitations)? ☐ Yes ☐ No

Acceptable use of network resources? ☐ Yes ☐ No

Personal information stored on mobile devices? ☐ Yes ☐ No

Protection of multiple layers of network architecture (i.e., hosts, applications, networks, perimeters)? ☐ Yes ☐ No

Change management procedures applicable when new technology or business processes are introduced? ☐ Yes ☐ No

Does the district regularly review policies, procedures, and contracts (especially contracts with cloud providers) to ensure that they meet applicable legal requirements, appropriately address security concerns, and evolve to meet changing technologies and expectations? ☐ Yes ☐ No

Has the district implemented appropriate technical measures to protect personal information stored on its network (e.g., antimalware software, firewalls, intrusion detection and prevention tools, vulnerability scanning, etc.)? ☐ Yes ☐ No

# Recent Dispatches in the Newsroom

## NEW Federal Cases

### April 2017

**Endrew F. v. Douglas County School District**

In the first major decision on special education in 30 years, the U.S. Supreme Court has weighed in on school districts' obligations under the IDEA. The Endrew F. opinion now sets the standard for IEPs as higher than "just above trivial" education. Read the summary of this case on SLRMA.org now to prepare your school district for the upcoming school year.

**Hively v. Ivy Tech Community College of Indiana**

The United States Court of Appeals for the Seventh Circuit became the first federal appellate court in the country to hold that Title VII of the Civil Rights Act of 1964 prohibits employers from discriminating against employees and job applicants based on their sexual orientation. Learn the implications for school districts' policies and procedures today by downloading this discussion.

*continued from page 1*

Revenue Service warning[3] about this particular phishing incident, it is believed that this attack was the single most widespread threat ever to school district data systems in the U.S., impacting tens of thousands of school employees.[4]

With the next cyberattack lurking around the corner, what can be done to protect school districts' data from vulnerabilities, while still using the most current cloud computing technologies? SLRMA's latest offering, the Cybersecurity and Privacy Risk Management for Cloud Computing Self-Audit Checklist and Best Practices, aims to steer members clear of air turbulence when soaring into cloud computing. Member districts already in the cloud and districts considering using the cloud will benefit from this comprehensive, practical approach to the issues involved in cloud computing, including cybersecurity best practices, personal data gathering policies, security incident breach response, and vetting cloud computing providers.

No one can predict when or where the next cyber threat will come. But by using SLRMA's latest Self-Audit Checklist now, your district will be well-prepared to meet that threat head-on.

3 The Internal Revenue Service communiqúe regarding the W2 form email scam can be viewed at *https://www.irs.gov/uac/dangerous-w-2-phishing-scam-evolving-targeting-schools-restaurants-hospitals-tribal-groups-and-others*

4 Levin, Doug. "IRS Official to Schools: "One of the Most Dangerous Email Phishing Scams We've Seen." March 22, 2017. *https://www.edtechstrategies.com/blog/irs-phishing/*

## SLRMA Board of Directors

**Roger Eddy**
Chair
Executive Director
Illinois Association of School Boards

**Lance Melton**
Vice Chair
Executive Director
Montana School Boards Association

**Dr. John Heim**
Treasurer
Executive Director
Kansas Association of School Boards

**John Spatz**
Secretary
Executive Director
Nebraska Association of School Boards

**Shawn Hime**
Treasurer
Executive Director
Oklahoma State School Boards Association

### NSBA Liaison

**Heather Dean**
Chief Operating Officer
National School Boards Association

Content provided by:

FLIC Federal Legislation Insurance Committee


**Maree F. Sneed**
Partner
Hogan Lovells US, LLP
(Washington, D.C.)

**Dr. Gillian Chapman**
Superintendent
Teton County School District
(Jackson, WY)

**Dr. Jerry D. Weast**
CEO
Partnership for Deliberate Excellence, LLC
(Potomac, MD)

**Dr. Troy Loeffelholz**
Superintendent
Columbus Public Schools
(Columbus, NE)

**Cheryl L. Sandner**
President
Brokers' Risk
(Chicago, IL)

**Tracy L. Olsen**
SLRMA Chief Content Editor
Senior Managing Counsel, Brokers' Risk
(Chicago, IL)


## Top 4 Downloads

1) **Questions and Answers on Title IX and Sexual Violence**
2) **Rights of Transgender Students (Hogan Lovells Memo)**
3) **English Language Learner Services and Education: Self-Audit Checklist and Best Practices for School Districts Part 1**
4) **School Districts Cloud Computing Services Self-Audit Checklist**





New York Times - June 16, 2017

The Department of Education is scaling back investigations into civil rights violations at the nation's public schools and universities, easing off mandates imposed by the Obama administration that the new leadership says have bogged down the agency.

According to an internal memo issued by Candice E. Jackson, the acting head of the department's office for civil rights, requirements that investigators broaden their inquiries to identify systemic issues and whole classes of victims will be scaled back.

## SLRMA Members

The Department of Education's new directive represents a significant departure from past OCR investigation practices. Head to the SLRMA.org Newsroom to download a discussion of how these changes may impact your school district going forward.

**Log onto slrma.org for more information.**