NHSBA
NEW HAMPSHIRE
SCHOOL BOARDS
ASSOCIATION
Incorporated 1946

New Hampshire
School Boards Association

Excellence in Public Education Through School Board Leadership

Data Security & Privacy for School Districts: Policy Guide and Legal Requirements

2018 Bradley F. Kidder
Education Law Conference

October 3, 2018

Data Breaches – Real Risks & Real Costs

RISKS – HACKERS & ERRORS

According to the Privacy Rights Clearinghouse, nearly half of all reported data breaches in 2016 involved school districts. EdTech reports 355 cybersecurity-related incidents in 2018 as of August 20. A few older examples include:

- April 2016 – The Olympia (WA) School District fell victim to a phishing attack on employee data. The district offered credit monitoring/identity theft prevention to 2,164 affected employees.
- April 2016 – The Concord (NH) School District suffered a breach in which the perpetrator obtained employee names, Social Security numbers, and other information using a phishing email. The breach may have resulted in the filing of fake income tax returns.
- November 2016 --Chicago Public Schools announced that confidential information belonging to 30,000 students had been improperly distributed to a charter school operator for marketing purposes (followed a May 2016 incident where CPS sent PII of 4,000 Students to vendors).

Data Breaches – Real Risks & Real Costs

RANSOMWARE - NETWORKS & DATA HELD HOSTAGE

- Over the past few years, several school systems throughout the United States (Leominster, MA.; Bigfork, MT; Roseburg, OR; Chester, SC, among others) have suffered more debilitating attacks wherein hackers have used ransomware (e.g., "WannaCry") to seize control of the entire networks and servers of school districts.
- In most instances, hackers have infiltrated systems with the malicious programs – by way of attachments to emails – sometimes legitimate. Once opened, the files spread, often through out-of-date hardware or software (e.g., Windows XP), and eventually embed enough to begin encrypting system data, rendering it inaccessible by the school system. The hackers then hold the data hostage, demanding ransom (payable through Bitcoin or other cryptocurrency) before providing decryption keys.
- Although some districts have been successful without making the demanded payments, most capitulate if only to cut short the time the data is inaccessible.
- As with other types of data breaches, school systems are particularly vulnerable lack of employed or retained IT personnel with proper cyber security training.

Data Breaches – Real Risks & Real Costs

COSTS -

- The Ponemon Institute determined that in 2016-2017, the average cost in for all organizations (commercial, non-profits, and public) to address a data breach is $200 per record, but for educational institutions, the cost was $245 per record.

  650 students X $245 = $159,250.00

- Several factors led to both the increased per record cost, as well as the fact that the costs are higher for schools: first is the extensive use of mobile platforms by districts, and second was systemic compliance failure.

- These costs can be avoided or at least minimized through employment of best practices, trained personnel, and strong policies / procedures (data governance plan).

General Areas of Risk

- Intentional – Hacking, Phishing, Ransomware Attack - Deliberate attacks on systems and individuals who have access to sensitive data. Such attacks can cause more harm than inadvertent exposure. Examples: Hacking of district human resource records to obtain employee information; false emails seeking personally identifiable information ("PII") or other confidential/critical information.

- Neglect & Physical Loss – Insufficiently protected data, or the physical. Examples: Outdated district computers or hard drives are sold or recycled without properly erasing district data; Carelessness regarding physical storage/transmission – e.g., loss of flash drives or laptops.

- Insecure Practices – insufficiently cautious collecting, storing, sending, encrypting, finding, and removing data. Example: Individual student achievement data is transmitted via unsecured email or public wireless networks.

Data Privacy and Security Questions

Questions for boards and administrators regarding data and privacy and security of the district's confidential and/or critical data and information:

- What confidential information/data does the district "have"? Need?
- What data security risks do school districts face?
- What is data governance? Does the school district need a data governance plan?
- What should my school district do to safeguard the privacy and security of data?
- What kinds of data security policies and procedures should a district have in place?
- What should a school district do to notify its community in the event of a data breach?
- What does the law require?

Data Security vs. Data Privacy

Data security: the protections in place to prevent unauthorized access to or acquisition of personal data and information critical to the operations of the district.

Data privacy: the relationship between the collection, use and retention of personal, confidential data and information.

Confidential Data & Information

Confidential Data/Information: Personal information that the district is prohibited by law, policy or contract from disclosing or that the district may disclose only in limited circumstances.

- Examples of statutorily protected confidential data:
  - Personally identifiable information ("PII") regarding students under FERPA;
  - "Student personally-identifiable data" under RSA 189:65, VII;
  - Teacher personally-identifiable data" or "teacher data" under RSA 189:65, VII-a.
- Each example includes information directly identifying individual students or staff – such as name, family names, addresses, social security numbers, and indirect identifiers, such as date of birth, or "other information … that would allow … a person … to identify" the student/staff member.

Critical Data & Information

Critical Data/Information: Information that is determined to be essential to district operations and that must be accurately and securely maintained to avoid disruption to district operations. Critical data is not necessarily confidential, but confidential data is almost always critical.

- Examples of non-confidential, critical data:
  - Safety plans and procedures;
  - District login information for district accounts;
  - Payroll procedures;
  - Policy and SOP databases.

Data Security Examples

<u>Data security</u>: the protections in place to prevent unauthorized access to or acquisition of personal data and information critical to the operations of the district – applies to both digital and other forms of storage.

- Examples:
  - keeping student and staff personal data in locked filing cabinets;
  - limiting access to those filing cabinets to people within the school district who need that data in order to do their jobs;
  - using encryption when transmitting personal data electronically;
  - requiring passwords to access files containing personal data;
  - installing software to help prevent intruders (hackers) into the multitude of network portals, or detecting them when prevention fails;
  - multiple layer backups – in system/out-of-system.

Data Governance ,
Data Governance Plans
&
HB 1612

NHSBA
NEW HAMPSHIRE SCHOOL BOARDS ASSOCIATION

Data Governance & Data Governance Plans

What is data governance?

- Data governance is the overall management of the availability, usability, integrity, quality, and security of data.
- A data governance plan includes a defined set of procedures and a plan and personnel to execute those procedures. Some states use the term written information security plan ("WISP").

What is a data governance plan?

- Data governance plans help ensure that appropriate policies and procedures are in place to facilitate accumulation of, access to, and use of confidential and critical data while protecting privacy.
- Passage of HB 1612 (codified at RSA 189:66, V) now requires all districts (LEAs) to develop a "data and privacy governance plan" by June 30, 2019.

Creating a Data Governance Plan

Initial Step: Audit - Network Map & Data Inventory/Map *(RSA 189:66, V (a-b))*:

- Perform a comprehensive information technology audit, either in-house, or through a consultant. At a minimum, the audit will include review and recommendations concerning the districts network map, applications and programs assessment, data map and review of existing policies and procedures.

  - What information does the district collect?
  - What information is personally identifiable, confidential or otherwise subject to protection by what specific federal or state law ("PII")?
  - Where is the data stored within the district's systems?
  - Who has access to it and who can share it?
  - How is district data protected as it moves through the district's system?
  - What programs, applications, and other digital tools/extensions are being uses on or through the district's servers, hardware and networks? *RSA 189:66, V(b) requires that the software inventory include "the provider, purpose, publisher, privacy statement, and terms of use" for each program.*

Components of a Data Governance Plan

Comprehensive data governance plans will include policies and operating procedures which provide for:

- Layered digital and physical security of confidential and critical data / information – access, storage, use, backups, and destruction (189:66, V (c));
- Data and program inventories along with network mapping (189:66, V (a)-(b));
- Implementation of data storage destruction standards (schedule and methods);
- Standards for use of software, programs and apps (189:66, V (b));
- Response plans for any breach of information or cyber-attack (189:66, V (d));
- Establishment of firewalls & user authentication standards; use of encryption;
- Appropriate training for all levels of users/managers/administrators;
- Vendor compliance with applicable privacy & security standards (189:66, V (e);
- Identification of necessary resources, e.g., budget and personnel needs;
- MOST IMPORTANTLY - Ongoing review and updating data governance plan, including the pertinent policies, and procedures.

Miscellaneous

Role of Senior Administrators and Legal Counsel

- Recognizing the tension between transparency laws, privacy requirements and security safeguards;
- Familiarity with the district’s data security governance plan;
- General understanding of the network and data inventories and network map;
- Understanding of likely security risks at each point on the map (e.g., old printers, and other networked hardware);
- Knowledge of the Federal and State laws implicated by the district’s technology and its data governance plan; and
- Identification of needed policies, procedures, contract requirements are necessary or useful for data security purposes.

Board members should familiarize themselves with the same issues, but need not have the same level of detail.

Acceptable Use Policies

- Apply Staff, Students, Parents, Volunteers and Visitors
- How Is It Communicated?
  - Policy in Manual or Handbook
  - Separate Sign off
  - Part of Contract
  - Click-Through Agreement
- Coordination with bring-your-own-device ("BYOD") policies, practices or procedures JICM/EDCA
- Enforcement

Information Security Officer – “ISO”*

Sample Job Description

- Understanding the technology of the school district
- Knowing the software (programs and applications) in use within the District
- Knowing how teachers and students are using technology and software
- Developing, maintaining and updating annually the district’s Data Governance Plan
- Developing acceptable use and other technology policies, procedures, inventories and contracts

**Some resources designate as “Chief Privacy Officer”*

Key State and Federal

Laws Impacting Digital Data &

Student/Teacher Privacy

NHSBA
NEW HAMPSHIRE
SCHOOL BOARDS
ASSOCIATION

New Hampshire Laws

- RSA 189:65 * Definitions
- RSA 186:66 * Student Information Protection and Privacy
- RSA 189:67 * Limits on Disclosure of Information
- RSA 189:68 * Student Privacy
- RSA 189:68-a * Student Online Personal Information
- RSA 359-C:19-21 * Right to Privacy/Notice of Security Breach

Federal Statutes

- FERPA - Family Educational Rights and Privacy Act
  - 20 U.S.C. § 1232g; 34 CFR Part 99
- COPPA - Children's Online Privacy Protection Act
  - 15 U.S.C. §6501-6505
- CIPA - Children's Internet Protection Act
  - 47 U.S.C. §254
- PPRA - Protection of Pupil Rights Amendment IDEA - Individuals with Disabilities in Education Act
  - 20 U.S.C. § 1232h; 34 CFR Part 98

Attachments

and

Additional Resources

Attachments & Additional Resources

ATTACHMENTS:

- HB 1612
- NHSBA sample policy EHAB – Data Governance & Security
- Sample Inventory of Software, Programs & Applications

ADDITIONAL RESOURCES:

- National Center for Education Statistics – *Privacy Technical Assistance Center Toolkit* (information and best practices in privacy protection and data security)

  https://nces.ed.gov/programs/ptac/Toolkit.aspx

- National School Boards Association – *Data Security for Schools: A Legal and Policy Guide for School Boards*

  https://www.nsba.org/data-security-schools-legal-and-policy-guide-school-boards

William Phillips
Staff Attorney & Director of Policy Services

NHSBA
25 Triangle Park Drive, Suite 101
Concord, NH 03301
(603) 228-2061
wphillips@nhsba.org

DISCLAIMER: The above information is copyrighted to the New Hampshire School Boards Association. The information is provided for general information only. School board members and administrators should consult with legal counsel to address local facts and circumstances.

w/training/tech/bk2018/BK 2018 Data Security (F)