K-12 Information Security Breaches

It is easy to think of information security breaches only happening to huge companies. We assume that these hackers are looking for profitable information. Think again. Hackers vary in their experiences, motivation, and targets. According to Shields (2003), there are three type of hackers—"Script Kiddies" novice wannabe hacker who merely use a program found on the internet to gain access, criminals who utilize stolen information such as credit cards and social security numbers, and cyberterrorists looking to disrupt government functions (2003). The motivation of hackers can stem from a political, criminal, or vandalism drive (Brown & Rycham, 2010). Whereas, the targets of attacks have been reported from businesses (retail/merchant, financial, insurance, etc.), educational institutions, government and military, healthcare (medical providers) and nonprofit organizations.

The recent news attention devoted to cybersecurity have people wondering how secure is their personal information? Attacks at such popular retail chains such as Target, Home Depot, and have spark the general public to understanding that thieves may steal their credit card information. However, the recent attacks at Sony and OPM have sparked new concern to how personal information is being secured.

In 2014, PWC, CSO magazine, the CERT Division of the Software Engineering Institute at Carnegie Mellon University, and the United States Secret Service cosponsored a survey study to reveal US State of Cybercrime. It was found that

- 69% of US executives are worried that cyber threats will impact growth.
- 82% of companies with high performing security practices collaborate with others to deepen their knowledge of security and threat trends.
- 59% of respondents said that they were more concerned about cybersecurity threats this year than in the past.
- 49% of all respondents have a plan for responding to insider threats.
- 38% have a methodology to prioritize cybersecurity investments based on risk to the business.

The Privacy Rights Clearing House's Chronology of Data Breaches website https://www.privacyrights.org/data-breach contains reports of data breaches since 2005 in which compromised information such as Social Security numbers, account numbers, and driver's license numbers have been access by identity thieves. The breaches posted include only those reported in the United States. The website is usually updated every two days.

Since 2005, approximately, 853,478,057 records have been compromised due to security breaches. This number only represent record and not represents individuals due to the fact that some may have more than one breach. Total number of 4,567 data breaches have been made public since 2005.

On a smaller scale, some attention have been devoted to information security breaches at educational institutions. The general public may not be shocked to learn that breaches may occurred at larger universities or colleges such as Harvard University, Penn State College, University of California Berkeley, California State University, University of Illinois, Butler University, Arkansas State University, San Diego State University, Iowa State University, North Dakota University, Indiana University, and University of Maryland. Here are two examples:

- In May 2015, Penn State's College of Engineering (University Park, Pennsylvania) reported that their servers were hacked in two different incidents. Allegedly, hackers are based in China and may have gained access to 18,000 individuals' sensitive data. Everyone (faculty, staff and students) connected to College of Engineering were affected. More information can be founded at: http://arstechnica.com/security/2015/05/penn-state-severs-engineering-network-after-incredibly-serious-intrusion/
- In 2014, Butler University (Indianapolis, Indiana) experience a data breach exposing Over 160,000 individuals (students, staff and alumni) personal information. The theft suspect was identified and arrested. The suspect had downloaded the information to a flash drive. Information exposed included birthdates, Social Security numbers and bank account information.

The general public may be shocked to learn that breaches are occurring at K-12 schools/districts. Schools/District rely heavily on computer-based systems, especially online systems, for almost everything from grading to professional development. Since 2005, approximately, 14,725,924 educational records have been compromised and 755 educational institutions data breaches have been made public (The Privacy Rights Clearing House's Chronology of Data Breaches website, 2015). A breakdown of the last five years include the following 2010: 74, 2011: 61, 2012: 86, 2013: 48, 2014: 28, and 2015: 8.

The degree to which student personal information has been compromised significantly varies among schools/districts. Breaches have taken the form of student hacker, stolen laptops or flash drive, phishing via emails, vendors (3rd party billing) and inadvertently sending or posting to the Internet. Here are six examples:

- In July, 2015, The Bonita Unified School District (San Dimas, California) discover a breach of unauthorized access on a San Dimas High School server. The district believed that the individual(s) had gained access to the server, changed several students grades, and downloaded personal information of students. Information compromised included names, Social Security numbers, birthdates, medical information, the school's systems usernames and passwords, addresses, email addresses, and phone numbers. More information about the breach can be found at http://oag.ca.gov/ecrime/databreach/reports/sb24-56705
- In February, 2015, The Escondido Union School District (Escondido, California) notified some students and employees of the district of potential security breach of a limited amount data. A district employee's iPad and a backup hard drive was stolen from a backpack during a board of education meeting. Information saved on the district issued device included student contact information, assessment results, and self-reported income by parents. More information about the breach can be found at http://www.sandiegouniontribune.com/news/2015/feb/17/tp-school-district-warns-of-potential-security/
- In October, 2014, The Provo City School District (Provo, Utah) notified employees of a phishing attack which allowed access to employees email accounts. In this incident, student records were not compromised. However, the employee's email account contained sensitive, personal identification information. A total of 1,400 employees' personal information could be compromised. More information about the breach can be found at http://fox13now.com/2014/10/01/provo-city-school-district-warning-employees-students-of-data-breach/

- In July, 2014, The Park Hill School District (Kansas City, Missouri) informed both current and former students and employees about a data breach involving a former employee. Seems that the employee had downloaded files onto a hard drive without authorization. While at home, the employee connected to the Internet and the files were posted. The files included personal identifying information such as social security numbers.
- In July 2015, Milford Schools (Milford, Massachusetts) reported that a third party billing service, Multi-State Billing Services, had experienced a breach. The information was on an employee's laptop in a locked vehicle. The laptop was stolen and the personal information (names, addresses, Medicaid id numbers and social security numbers) of up to 25 students was compromised. The laptop was password protected but not encrypted. It contained records on nearly 3,000 students from 19 school districts.
- Unencrypted medical data of 100 Denver Public School students were exposed by a school nurse negligence (Goldman, 2013). The data was downloaded and stored on a thumb dive and placed in a briefcase. However, the briefcase was stolen from the nurse's car. At the time, there were no polices in place prohibiting the actions of nurse. However, this has prompted the school system to review and revise their policies in regards to student records (Goldman, 2013)

Additionally, the general public may be shocked to learn that "keeping student data safe" is the overarching theme of chief technology officers (CTOs) staying up at night. Recently at the TCEA Convention and Exposition Conference in Texas, a panel discussed the state of education and technology from their perspective. The panel shared their key challenges and offered some solutions for handling these hurdles. The main hurdle with keeping student data safe is finding a balance between the increasing number of tech-based learning tools available and the need for solid personal and data security. Districts using more cloud-based service versus hard drive-based system were experiencing the most impact. Plus, CTOs struggle to decide whether to give teachers and administrators access to some or all these tools. The other five key challenges were data sharing, social media, budgets, Wi-Fi and device diversity.

There is a hard cost of information security breaches.

The cost of security breaches may result in significant downtime and time consuming efforts by the IT department. In 2011, Panda Security, a cloud security company conducted a Kindergarten-12 Education IT Security study which can be located at http://www.pandasecurity.com/mediacenter/src/uploads/2011/03/Panda-K12-Education-IT-Security-Study_03.23.11.pdf Surprising results how that 63% of schools experience malware outbreaks or unauthorized user access at least twice a year. Plus, 64% of schools have experienced significant downtime during these incidents. This case study surveyed 104 individuals (employees or consultant) who manage IT security at K-12 school districts in the United States. The purpose of the study was to examine security practices and concerns of the school districts. Major results of the report consisted of the following:

- Security issues consume staff time which diverts attention away from educating children.
- Social media sites is a top concern but school policies varied significantly.
- The schools recognized that BYOD introduce external risks yet they struggle to fully integrate security policies for the devices.

- Schools were more likely to look to the cloud to improve their IT infrastructure.

Also, the report made recommendation to improving school IT Security.

- Invest in cloud-based security.
- Protect against external threats by having Require registration BYOD.
- Monitor social media access.
- Implement regular security awareness education programs.

The Need to Protect Data

The Family Educational Rights and Privacy Act of 1974 (FERPA) is a United States federal law that protects the privacy of student education records. All schools receiving funds from U.S. Department of Education must comply with this law. FERPA provide parent certain rights such as right to inspect and review their child's records maintained by the school and request that a school amend items on records which they believe maybe inaccurate or misleading. Once a child reaches the age of 18 (eligible student) or attends a school beyond the high school level these rights are transferred to the student. Additional regulations under this act, starting January 3, 2012, which allowed for greater disclosures of personal and directory student identifying information. Parents or eligible students must provide written permission in order for education record to be release. However, FERPA allows schools to disclose records, without consent, to the following parties or under the following conditions (34 CFR § 99.31):

- School officials with legitimate educational interest;
- Other schools to which a student is transferring;
- Specified officials for audit or evaluation purposes;
- Appropriate parties in connection with financial aid to a student;
- Organizations conducting certain studies for or on behalf of the school;
- Accrediting organizations;
- To comply with a judicial order or lawfully issued subpoena;
- Appropriate officials in cases of health and safety emergencies; and
- State and local authorities, within a juvenile justice system, pursuant to specific State law.
  http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

Student Digital Privacy Act

Update to the FERPA, in which data collected in the educational context is used only for educational purposes.

Best Practices to Protecting Data

In a presentation titled, The CERT Top 10 List for Winning the Battle Against Insider Threats, Dawn Cappelli (2012) provided real-case examples to reinforce best practices in mitigating insider threat. The presentation was delivered at the RSA Conference 2012, held in San Francisco, CA from February 27 to March 2, 2012. The presentation can be found at

http://resources.sei.cmu.edu/asset_files/Presentation/2012_017_001_52427.pdf In summary, Cappelli suggest the following practices:

- Create formal teams to examine the incidents and develop new controls.
- Protect the crown jewels such as your IP by adding extra controls.
- Create and train threat team about insider threat. Implement systems such as intrusion detection systems and Security Information and Event Management systems (SIEMs). Customized tools reduce information overload (Data Leakage Protection, host based controls, change controls).
- Mitigate threats from trusted business partners
- Recognize concerning behaviors as a potential indicator
- Educate employees regarding potential recruitment
- Pay close attention at resignation / termination!
- Address employee privacy issues with General Counsel
- Work together across the organization
- Create an insider threat program NOW!

Conducting a Cybersecurity Audit

Chip Shield (2003) suggest conducting a cybersecurity audit. Hire an outside expert to determine the vulnerabilities of the schools information system. After which, the audit results should be compare to best practices of safeguarding the computer system (2003). For example, Wyoming legislators has raised concerns after receiving a statewide technology audit from their Department of Education ("Data in Danger", 2015). 12 of the 38 schools districts have failed to use encryption software to protect student data. This is contrary to the state legislators' approaches to data security and privacy issues. The legislators' believed that smaller districts may not have the resource to implement such security measures. However, the Department of Education has both formalized and formerly unwritten security procedures and expectations of implementing mandatory training for all staff referencing data security protocols (2015).

Data Sharing

The Privacy Technical Assistance Center encourages schools to become transparent about data sharing. Answering the following 5 questions have been determine as the best practices for schools and districts alleviating student concerns:

- What information are you collecting about students?
    - Create and publish a data inventory listing of information collected about the students
- Why are you collecting this information?
    - Explain you reasons for collecting the data.
- How is the information protected?
    - Explain the school/district Infosec data protection and retention policies.

- Do you share any personal information with third parties?
    - State whether you share data with a third party and for what purposes such as research.
- Who should students contact if they have questions about your data practices?
    - Display contact information and ask for feedback to how student privacy policies and practices can become more transparent.

Developed a Risk Management Plan

Simonson (2012) Proactive and reactive measure to consider when developing a Risk Management Plan:

- Determine gaps completing a comprehensive assessment of the in place computer system and safeguards.
- Protect the organization by installing new hardware/software and network measures.
- Create a response plan and assembly a team for handling a negative incident.
- Consider purchasing cyber insurance cover the data breach and other unexpected exposures not covered by traditional insurances (Simonson, 2012).

References

*Bathon, J. (2013). How Little Data Breaches Cause Big Problems. *T H E Journal*, *40*(10), 26-29.

*Data Breaches Shake Consumer Confidence. (2014). *Information Management Journal*, *48*(6), 6.

*DATA IN DANGER. (2015). *American School & University*, *87*(5), 34.

*Hackers Attend Summer Camp. (2013). *Information Management Journal*, *47*(5), 12.

Herold, B., & Davis, M. R. (2014). Personal Danger Of Data Breaches Prompts Action. (Cover story). *Education Week*, *33*(18), 1-11.

Negrea, S. (2015). Hard costs of a data breach. *University Business*, *18*(6), 61-63.

Panda security. (2011). *M2 Presswire* Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/858127405?accountid=10639

Privacy Rights Clearing House's Chronology of Data Breaches website https://www.privacyrights.org/data-breach

*SHELHART, M. (2015). THE FIRST 24 HOURS. *Public Management (00333611)*, *97*(2), 28.

*Simonson, K. (2012). DEFENDING AGAINST TECHNOLOGY'S DARK SIDE'S. *Public Management (00333611)*,*95*(11), 16-19.

Student Digital Privacy Act https://www.whitehouse.gov/the-press-office/2015/01/12/fact-sheet-safeguarding-american-consumers-families

*THOMPSON, G. (2015). THE POWER OF SMALL DATA. *T H E Journal*, *42*(3), 12-16.

*VIJAYAN, J. (2015). 5 THINGS YOU SHOULD KNOW ABOUT CYBER INSURANCE. *Computerworld Digital Magazine*, *1*(11), 27-32.