Good afternoon Mr. Chairman and members of the House Education Committee.

My name is Brian Huesers. I want to thank you for asking me to speak this afternoon regarding data security. In today's world data privacy and security is the single most frightening thing regarding technology.

A few credentials; I've been in the I/T world for almost 30 years, the first fifteen years at H&R Block, and the last 15 years I have been lucky enough to lead the I/T divisions of two private organizations (La Petite Academy and Westlake Hardware) and two public organizations (Kansas City Mo School District and Kansas Department of Health and Environment).

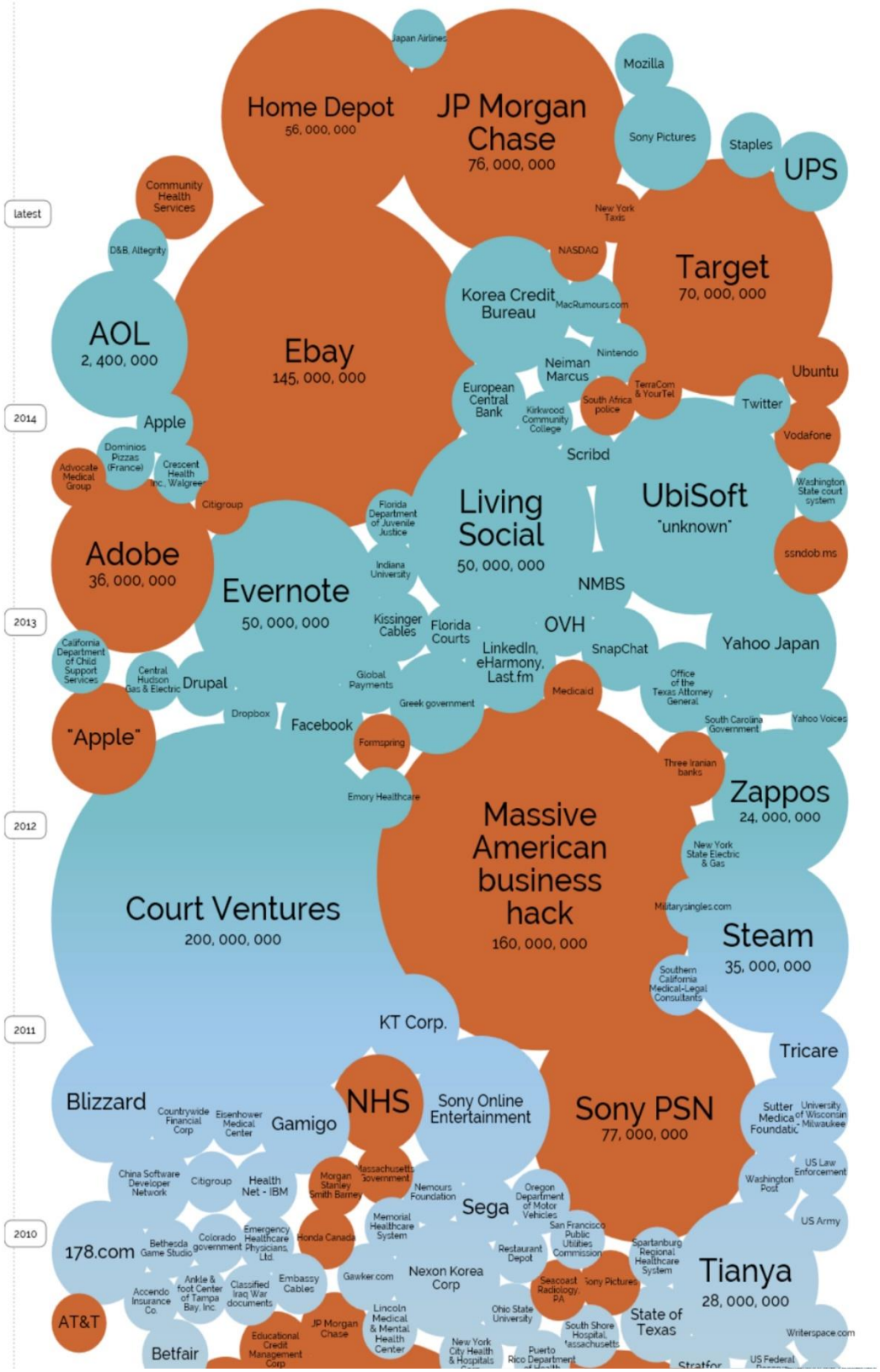
Needless to say, a great deal of my time is spent worried about data security. In various capacities, I've been concerned with protecting tax information, information regarding children and students, various databases involving diseases, birth and death certificates, and currently credit card information.

Most federal regulations regarding security are very general in nature. They try to avoid controversy by not making hard and fast requirements. For example, regarding HIPAA regulations which safeguard our medical records, www.hhs.gov says that "medical providers must implement reasonable safeguards to limit incidental, and avoid prohibited, uses and disclosures. The Privacy Rule does not require that all risk of protected health information disclosure be eliminated. Covered entities must review their own practices and determine what steps are reasonable to safeguard their patient information." Interestingly enough, the HIPAA regulations themselves are over 100 pages long but most of that deal with definitions and disclosure statements.

Compare that to PCI standards. PCI stands for the Payment Card Industry and it is an industry group that creates security standards for the credit card industry. Retailers are required to have an external audit performed annually or a certified PCI auditor on-staff. The audit document is over 80 pages long with well over 350 specific requirements. If a company is not compliant then they will be fined, and if not corrected, unable to use credit cards.

Are any of these regulations /standards effective? Let's look at some of the data breaches that have occurred the last few years.

World's Biggest Data Breaches



Provided by Information is Beautiful. www.informationisbeautiful.net

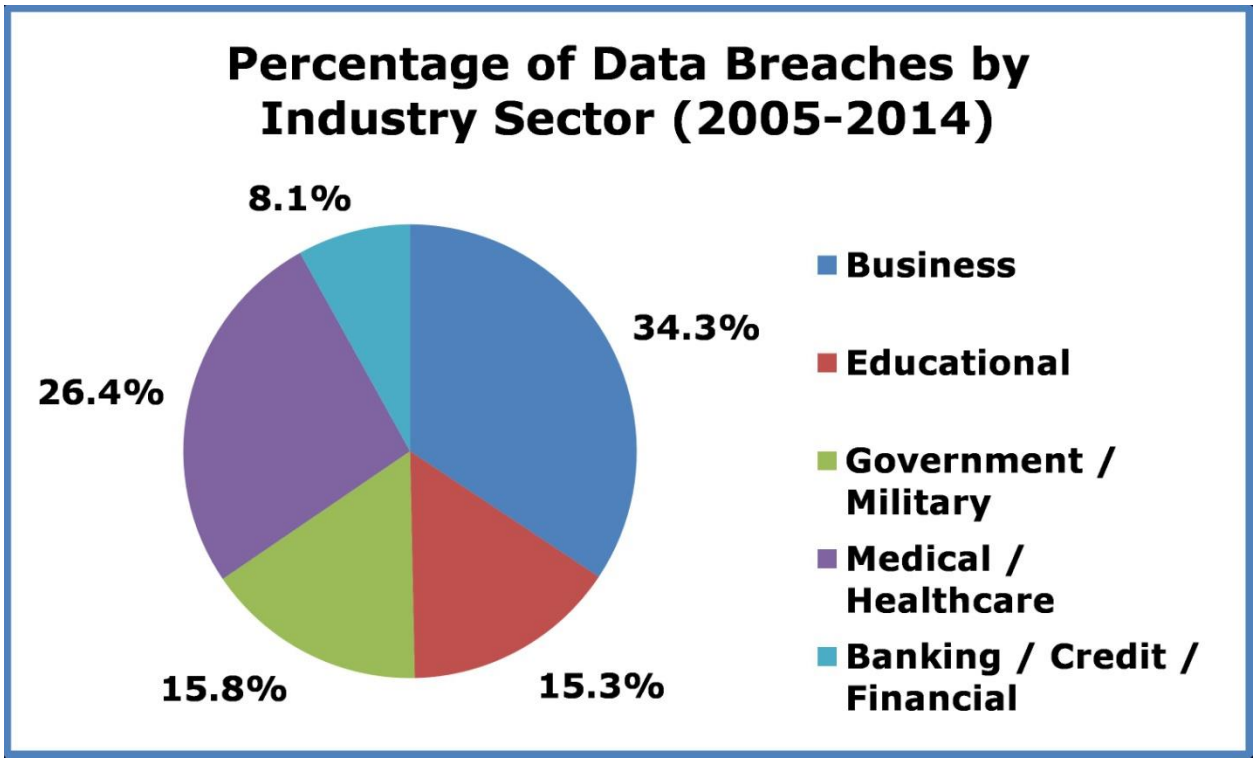
What are three things Target, Home Depot and Ebay, for example, have in common?

- Spent millions on I/T security
- Passed the PCI audit
- Were hacked anyway

Scary, isn't it?

Data Breaches by Industry Sector

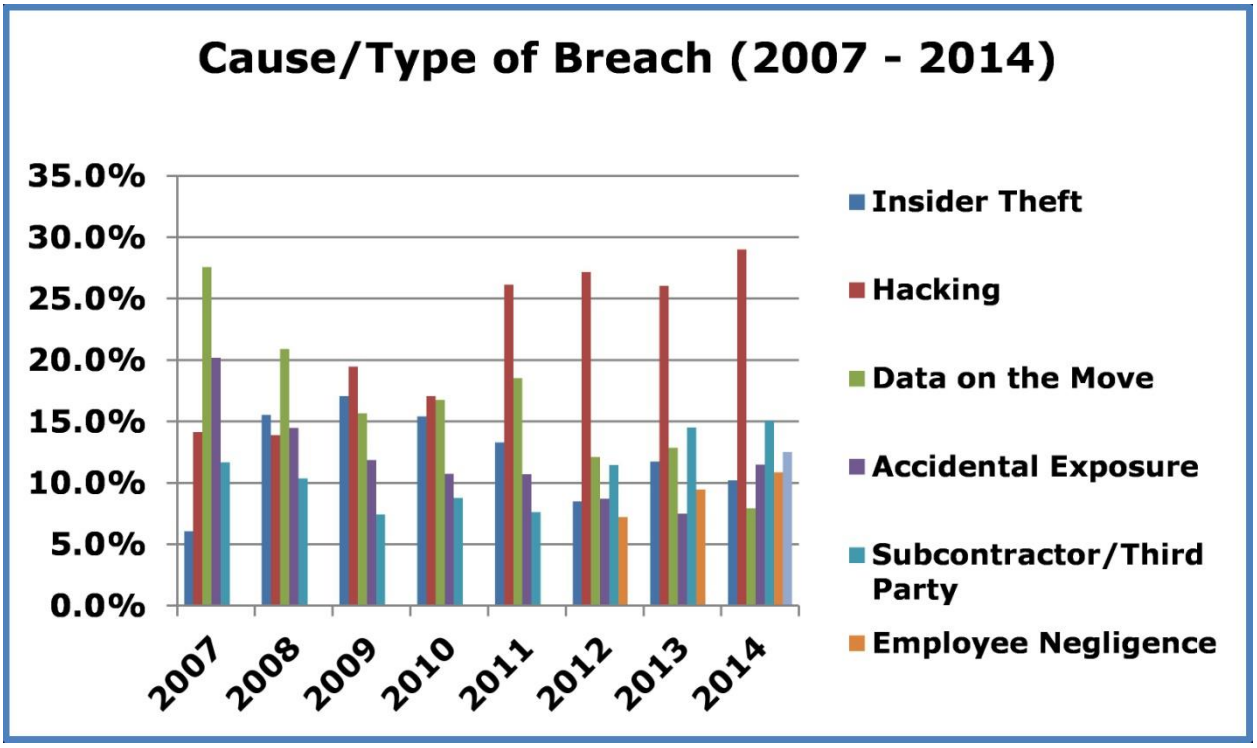
In looking at the Industry Sectors of data breaches, not suprisingly, Business leads the way as hackers tend to follow the money, but Healthcare is fairly close behind. Education data breaches account for 15.3% of all data breaches. Total data breaches for 2014 is 783.



Produced by ITRC - www.idtheftcenter.org

Cause/Types of Breaches

It's important to look at how the breaches occur. Hacking is the most frequent cause – and growing, the others are all around 10%. "Data on the move" means laptops being lost, etc... Total number of breaches has risen from 157 in 2005 to 783 in 2014.



Produced by ITRC - www.idtheftcenter.org

FERPA

Obviously, we all know about FERPA, but in a nutshell the law provides:

Access to Education Records - Under FERPA, a school must provide a parent with an opportunity to inspect and review his or her child's education records within 45 days following its receipt of a request.

Amendment of Education Records - Under FERPA, a parent has the right to request that inaccurate or misleading information in his or her child's education records be amended.

Disclosure of Education Records - Under FERPA, a school may not generally disclose personally identifiable information from a minor student's education records to a third party unless the student's parent has provided written consent. However, there are a number of exceptions to FERPA's prohibition against non-consensual disclosure of personally identifiable information from education records. Under these exceptions, **schools are permitted to disclose personally identifiable information from education records without consent**.

As with HIPAA, the regulations are deliberately vague with very little guidance on how personally identifiable information should be protected.

We could have a long discussion about FERPA and its limitations particularly the “exclusions” part of the bill that was modified by regulations recently, but that is probably a discussion best held at another time.

Things that should be done.

To try to give you some idea of some of the things that should be required, here are the minimum things that should be done to help protect and secure data:

Make someone Responsible – Make one person or group in your organization responsible for data security. They should monitor and analyze security alerts, distribute security policies and procedures, monitor and control all access to data and create and follow an incident response plan if needed.

Two Factor Authentication – all remote access into systems should require two things. Something you know – like a password, and something you have – like a token, or a fingerprint. Implementing two factor authentication would have prevented the Target data breach from occurring.

External/Internal Vulnerability Scans - All outward facing systems (Internet) should be scanned monthly to ensure that vulnerabilities are found and eliminated. Internal scans of servers, printers and firewalls are also very useful in identifying possible security concerns. There are many 3rd party companies that do this at a pretty reasonable fee.

Classifying business data - One of the most important things to do is to classify the databases in your organization basing the level of security on the nature of information contained within those databases.

Use encryption on Sensitive data – All major databases have the ability to encrypt data at a field level, so encrypting sensitive data should be a no-brainer that in the case the data is ever accessed illegally or stolen, the sensitive data is protected.

Security Awareness Training – All employees should be required annually to attend security awareness training. The training should be used to review your organization's security policy, its data classification and how to handle sensitive data, workspace and desktop security, password security, phishing, hoaxes, malware and file sharing.

Anti-Virus software - Deploy anti-virus mechanisms on all systems commonly affected by viruses (e.g., PC's and servers) that might contain sensitive data.

Automatically update Desktop software - All the software we use every day is riddled with security issues. Software companies (like Adobe, Windows, MS Office, Google) regularly release security patches for such software. It's important to install such software updates as soon as possible after they're available through their automatic update process.

External Vendors – Data that goes outside your organization doesn't mean you've abdicated responsibility for that data. Whomever that data goes to must be contractually obligated to maintain privacy and security standards to protect data.

Laptop Security – If a laptop contains sensitive data, encrypt the data and configure the laptop so users can't download software or change security settings. Basic handling practices of laptops on the road should be defined.

Firewalls – Proper deployment of firewalls is critical to the safety of your organization's network and data. Perimeter firewalls (between Internet and your Network) are a requirement. An additional layer of protection for your data is to add a DMZ firewall so that the organization's data resides behind a firewall and data requests must transverse through the DMZ.

Disposal Policies - Implement information disposal practices that are reasonable and appropriate to prevent unauthorized access to—or use of—personally identifying information. This could include disposal of paper records, recycling of old computers, or archiving of old data or emails.

Data Security Issues Unique to Education

Each industry sector has data security challenges unique to its industry, whether it is tax returns, credit cards, or children. The education industry has its own unique challenges because it deals with our most precious asset.

When I was the CIO for the KC Missouri School District, things seemed pretty easy. My Student Information System was a local database and tracked things like attendance and grades. The curriculum was hard copy books and was not available on-line. The tests were taken via pencil and graded by teachers. My primary concern was trying to keep high schoolers from getting to inappropriate web sites.

Now, things are totally different. Most student information systems are contracted out and are available through the Internet and based in the "Cloud". Curriculum is also cloud based. Tests are taken on-line and a lot are adaptive in nature.

While on the surface all of that sounds fine, there are significant concerns about the data that makes up the curriculum, student systems, and testing. With the recent change to FERPA allowing access to data to those companies with "educational interest" our children's data is now available to private companies to market to, provide analysis for, and possibly exploit.

Here are some things we all should be concerned with:

Student Information Systems that have data points that track things like attitudes, values or beliefs.

Curriculum that requires individual log-ins to access text books and complete work. By requiring individual log-ins they can monitor activities and learn things that are not pertinent to education including a behavioral profile at the individual student level.

Adaptive Testing – that is the latest "craze" in the education field that produces tests where nobody (including the teacher) sees the test questions. They are different for every child and the reliance on the person/party that makes up the test is total and complete.

The sheer volume of personally identifiable data generated is enormous. Identifying the amount and number of points at which it is collected, and by whom, would be a large undertaking. The resources to do so competently would have to be extensive. Add, the "places it can go", and you now have an environment where it is nearly impossible to say that personally identifiable student data is private, much less secure.

How to maintain control of our data

There must be laws that mandate full disclosure and communication to parents and the public of when and what data is being collected. Parental consent for the data generation/collection and dissemination of their children's data must be emphasized. School districts and state agencies must demand contracts that have specific and limiting data use and privacy language. Audits must be perform to any outside entity that data is shared with to ensure student data privacy and security.

Thank you for your time, and please let me know if you have any questions.