CYBER SECURITY TRAINING

FOR EDUCATORS AND ADMINISTRATORS ©

Shared Knowledge, LLC

http://ishareknowledge.com

Hello!

Tonya J. Mead CFE, PI, MBA, MA
and School Psychologist

Shared Knowledge, LLC

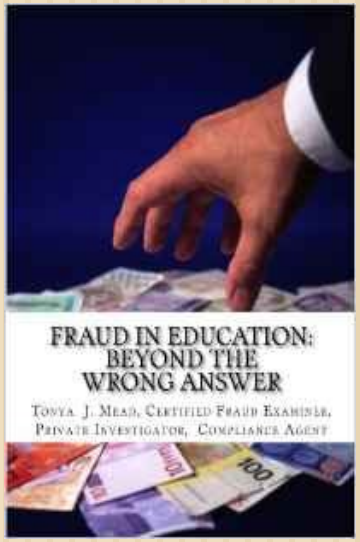
http://ishareknowledge.com
tonya@ishareknowledge.com

Licensed Private Investigations and Security Agency

Author: Fraud in Education: Beyond the Wrong Answer

ISBN-13: 978-1539301844
ISBN-10: 1539301842

PROFESSION OF INTEGRITY



Educators *are* Esteemed

	Gallup 2013		Gallup 2014
1	Nurses	1	Nu
2	Pharmacists	2	Me
2	Teachers *Tied	2	Pha
3	Medical Doctors	3	Pol
4	Military Officers	4	Clergy
4	Police Officers *Tied	5	Bankers

?

FACT

- Schools and universities spend almost $12 billion on information technology each year

Source: Center for Digital Education, Folsom, CA, May 22, 2015. Available: http://www.centerdigitaled.com/higher-ed/US-Education-Institutions-Spend-66-Billion-on-IT-in-2015.html

SITUATION

- upgrade antiquated data warehouses
- data driven instruction
- student interventions driven by data
- data used to guide management decisions

SITUATION

- policy and governance impacted by data
- parents and stakeholders demand more data
- real time data entry, storage, analysis, tracking, and visualization requirements

VULNERABILITIES

- The greatest security weakness of school districts is a lack of IT resources
- Compounded by pressures to provide greater access to the network
- School systems tend to spend less on sophisticated protections than large corporations, making targets for penetration

Source: Fraud in Education:: Beyond the Wrong Answer Available at: http://amazon.com/author/tonyajmead

FITARA SCORECARD

	Incremental Development	Risk Assessment Transparency	Information Technology Portfolio Review Savings	Data Center Consolidation	Average Grade
US Department of Education	F	D	F	B	D

Source: House Oversight and Government Reform Committee: FITARA Implementation Scorecard- May 2016

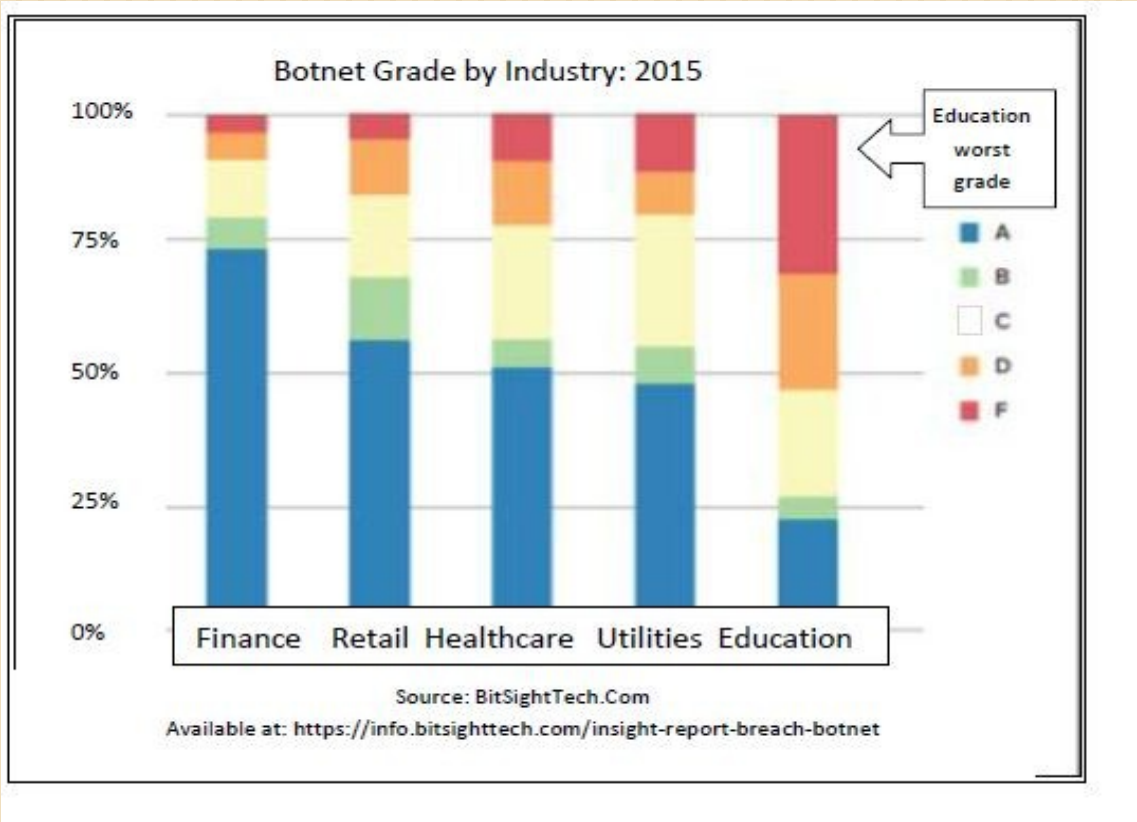
WHAT IS FITARA?

- **FITARA** "(Federal IT Acquisition Reform Act) is U.S. legislation passed in December 2014 that puts federal agency CIOs in control of Information Technology investments.

  It requires U.S. federal agencies to provide the Office of Management and Budget (OMB) with a comprehensive inventory of data centers."

Source: https://www.apptio.com/fitara-summary

BOTNET GRADE



WHAT IS A BOTNET?

- **Botnet** "is a collection of internet-connected devices, which may include PCs, servers, mobile devices and internet of things devices that are infected and controlled by a common type of malware.

  Users are often unaware of a botnet infecting their system."

Source: http://searchsecurity.techtarget.com

EXAMPLES OF BOTNETS

- Botnets are used for sending
  - spam,
  - phishing emails,
  - Ransomware, and
  - spyware

Source: http://searchsecurity.techtarget.com

WHAT IS AT RISK?

The Confidential Information of:

- 100,000 k-12 public schools
- 7,200 colleges and universities
- 75.2 million students
- 4.6 million faculty and 5.3 million public administrators
- 3.4 million faculty, staff and administrators at private institutions

Source: NCES 2016-014), Chapter 2, tinyurl.com/zort7df

SECURITY EXPERTS

- The education sector is the "second most sector—behind only healthcare—for businesses with lost or stolen records globally.

Source: Bitsight Insights, "Beware the Botnets: Botnets Correlated to a Higher Likelihood of a Significant Breach," April 2015.

2 (TWO) KEY FACTORS

- **Lost-**
  - implies insider/internal threat
- **Stolen-**
  - Implies outsider/external threat

Source: Bitsight Insights, “Beware the Botnets: Botnets Correlated to a Higher Likelihood of a Significant Breach,” April 2015.

UNINTENTIONAL HUMAN ERROR

SANS Institute

discovered “in more than 63% of security breaches identified by respondents, human error was the major cause. Only 8% were purely technical failures.”

Source: Bitsight Insights, “Beware the Botnets: Botnets Correlated to a Higher Likelihood of a Significant Breach,” April 2015.

FILE SHARING

- **Makes any information on a computer's hard drive accessible**
  - Online procurement, banking and financial information
  - Human resources information, salary, family members, social security numbers
  - Insurance, medical history

Source: First Commonwealth Bank Available at: https://www.myfcb.com/7-practices-safer-computing.htm

MALWARE

- **Access information from devices**
  - Phone and email contacts
  - Call logs
  - Data about the device's location
  - Internet data
  - Calendar data

Source: FTC Available at: https://www.consumer.ftc.gov/articles/0018-understanding-mobile-apps and Wikipedia Available at: https://en.wikipedia.org/wiki/Social_engineering_(security)

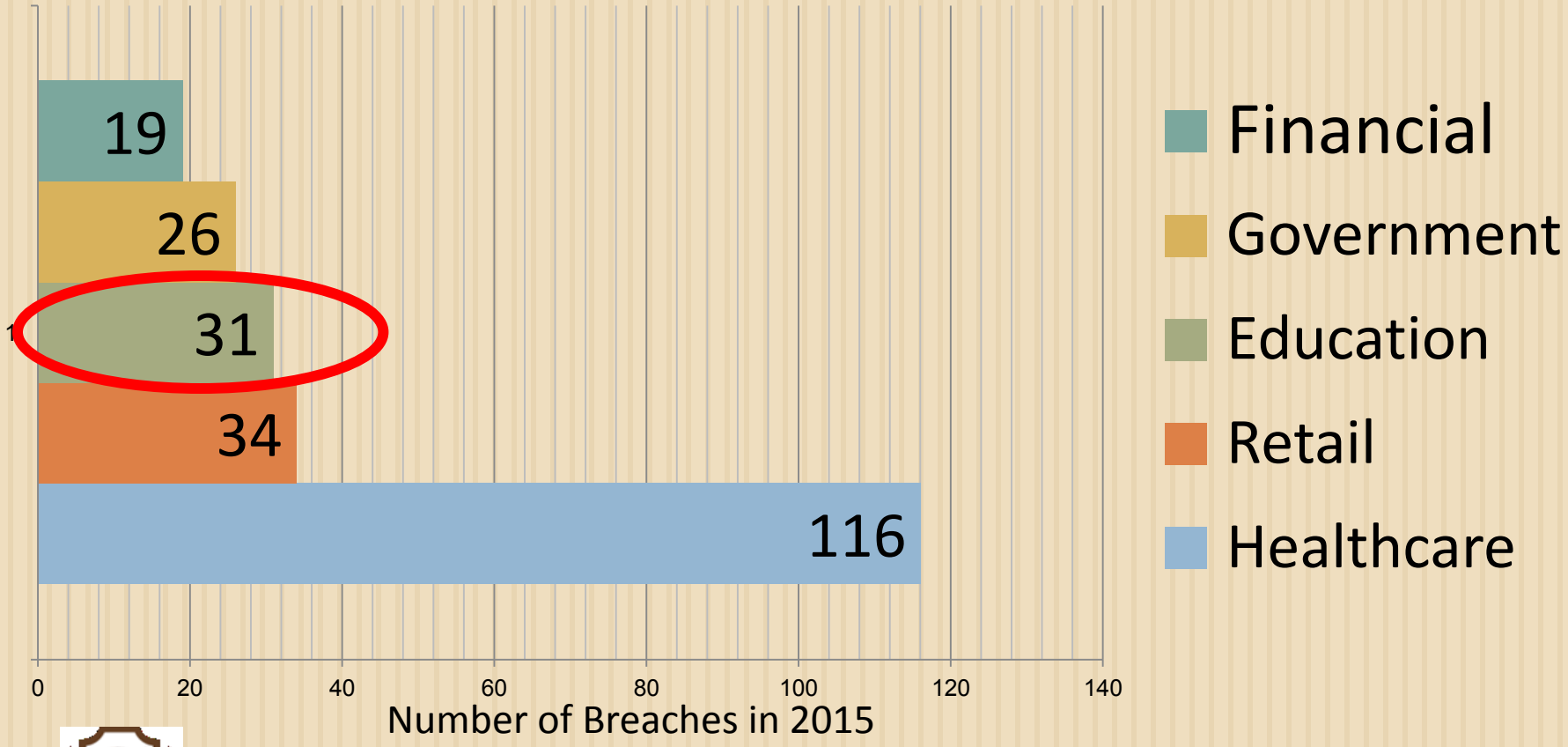
SOCIAL ENGINEERING

- Phishing
  - Games- Loss of points, status and credentials when gaming
- Pre-texting
  - Social media- verify contacts or click link appears to be from friend

SECURITY EXPERTS

- Michael Oppenheim of FireEye estimates that 550 universities had experienced some type of data breach from 2006 to 2013, exposing confidential student and staff information

DATA BREACHES BY SECTOR



Source: "Top Trending Education Targets in 2015," *Surfwatch Labs*. 2015. Available at: https://www.surfwatchlabs.com/?gclid=CKXqwZ_0xMUCFVKQHwodTAYAhQ

DATA BREACHES

- **Can yield <u>anything</u> that is stored**
  - Confidential data
  - Uploaded files and documents
  - Photos
  - Chat logs
  - Audio recordings

DATA BREACHES

- Free File Sharing
- Malware- Mobile Apps
- Hack internal computer data for ransom
- Store Audio & Video for Resale

Source: FTC Available at: https://www.consumer.ftc.gov/blog/gamers-avoid-phishing-hook Breitbart Available at: http://www.breitbart.com/tech/2017/03/01/report-hackers-held-voice-recordings-from-cloudpets-toys-for-ransom/ and Koando Available at: Source: http://www.komando.com/happening-now/337372/updated-major-data-breach-puts-hundreds-of-thousands-of-children-at-risk/

IDENTITIES EXPOSED

Education Sector 1,359,190

Source: K. McCarthy, "Five Colleges with Data Breaches Larger Than Sony's in 2014," *Huffington Post*. Available: http://www.huffingtonpost.com/kyle-mccarthy/five-colleges-with-data-b_b_6474800.html

IDENTITIES EXPOSED

2014 Data Breaches	Date of Breach	Records Breached	Type of Breach
University of Maryland	3/2014	309,079	Hacking or malware
North Dakota University	2/2014	290,000	Hacking or malware
Butler University	6/30/2014	163,000	Hacking or malware
Indiana University	7/17/2014	146,000	Hacking or malware
Arkansas State University	6/10/2014	50,000	Unintended disclosure
Riverside Community College	n. d	35,212	Not indicated
Iowa State University	n. d	29,780	Not indicated
Orangeburg-Calhoun Technical College	7/14/2014	20,000	Portable device
University of Wisconsin-Parkside	n. d	15,000	Not indicated
Seattle Public Schools	11/14/2014	8,000	Unintended disclosure
Provo City School District	1/10/2014	1,400	Hacking or malware
Alumni Relations, Penn State College of Medicine	10/7/2014	1,176	Hacking or malware
Fort Hays State University	1/10/2014	138	Unintended disclosure
Milford Schools	2/7/2014	25	Portable device

CONFIDENTIAL INFORMATION

- Student, parent and staff full name (first, middle, last)
- Maiden name
- Date of birth
- Social Security numbers
- Current and previous physical addresses
- Phone number
- Employer and Employment History
- Income
- Disciplinary records, 12 year academic history
- Disability status
- Extended relatives and emergency contacts
- Utility receipts

Source: NCES 2016-014), Chapter 2, tinyurl.com/zort7df

CRIMINAL INTENT

Identity

Theft

Resource

Center

Criminals may

"purposely target children because of the often lengthy time between the fraudulent use of the child's information and the discovery of a crime."

Source: ITRC Fact Sheet 120, 2015, p.1).

CRIMINAL INTENT

The Federal Trade Commission

"a child's social security number can be used by identity thieves to apply for government benefits, open bank and credit card accounts, apply for a loan or utility service, or rent a place to live…"

Source: "Consumer Information: Child Identity Theft." The Federal Trade Commission Washington, DC. Available: http://www.consumer.ftc.gov/articles/0040-child-identity-theft

THEFT

- When a school or state education agency's computer system becomes infected with botnets, private records and data are at risk for theft.

Source: http://searchsecurity.techtarget.com

BLACK MARKET

Hacker service	Price
Social security number	$30
Date of birth	$11
Health insurance credentials	$20
Visa/MasterCard credentials	$4
Discover credit credentials	$8
American Express credentials	$7

Source: Dell SecureWorks 2013-2014

BLACK MARKET

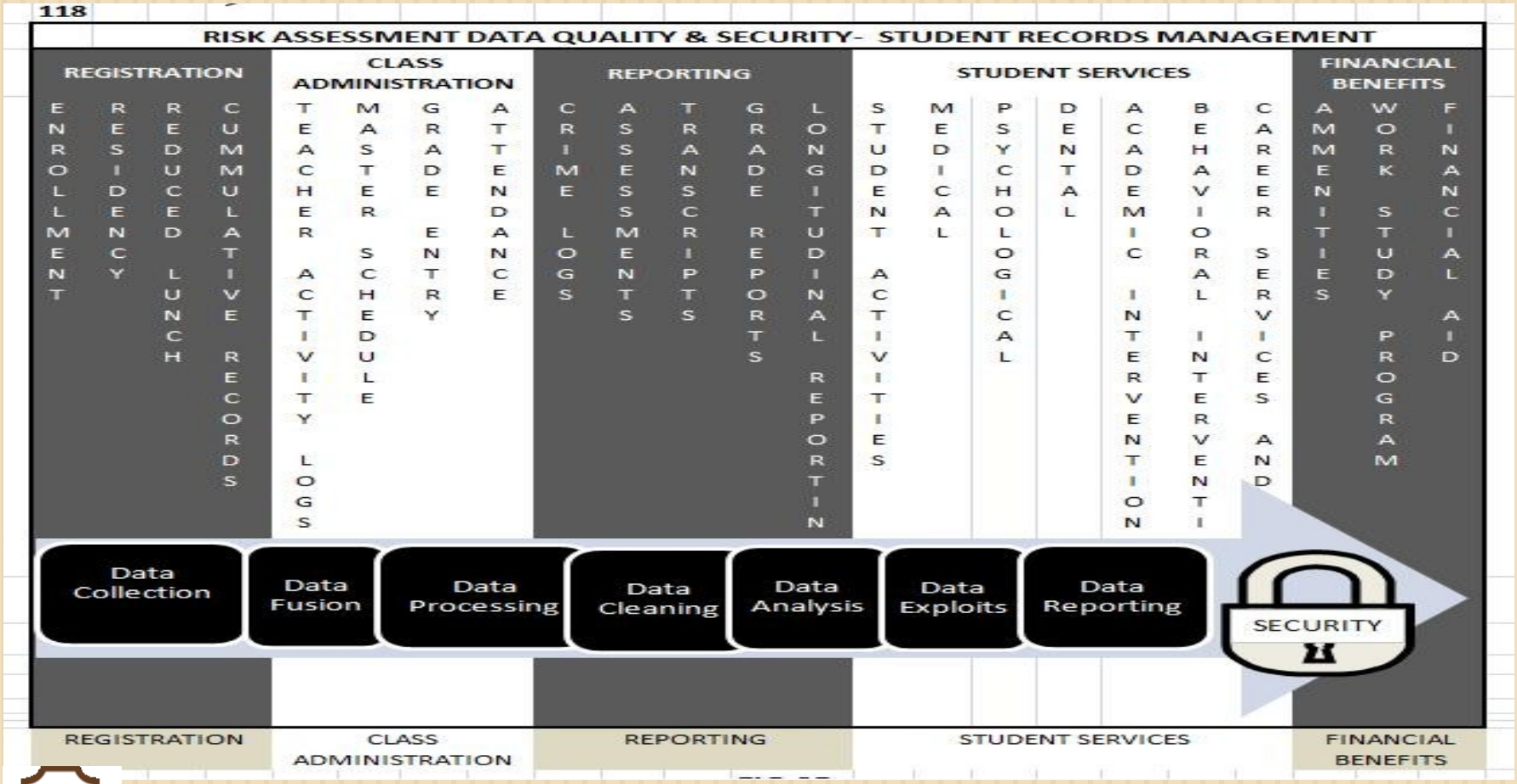
Hacker service	Price
Credit card with magnetic stripe/chip data	$12
Bank account number $70,000 -$150,000 balance	$300 or less
Full identity	$1,200 to $1,300

Source: Dell SecureWorks 2013-2014

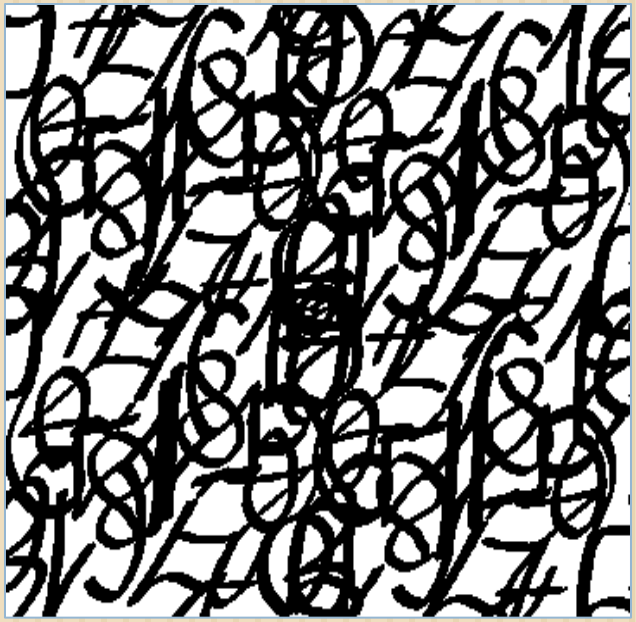
INFORMATION SOURCES

- **Front Office**
  - pre-admissions, registration, master scheduling, grant and grade reporting , and student matriculation
- **Back Office**
  - payroll, data management and storage, info technology finance, human resources procurement, and operations

ENTRY POINTS



WHY DOES IT MATTER?

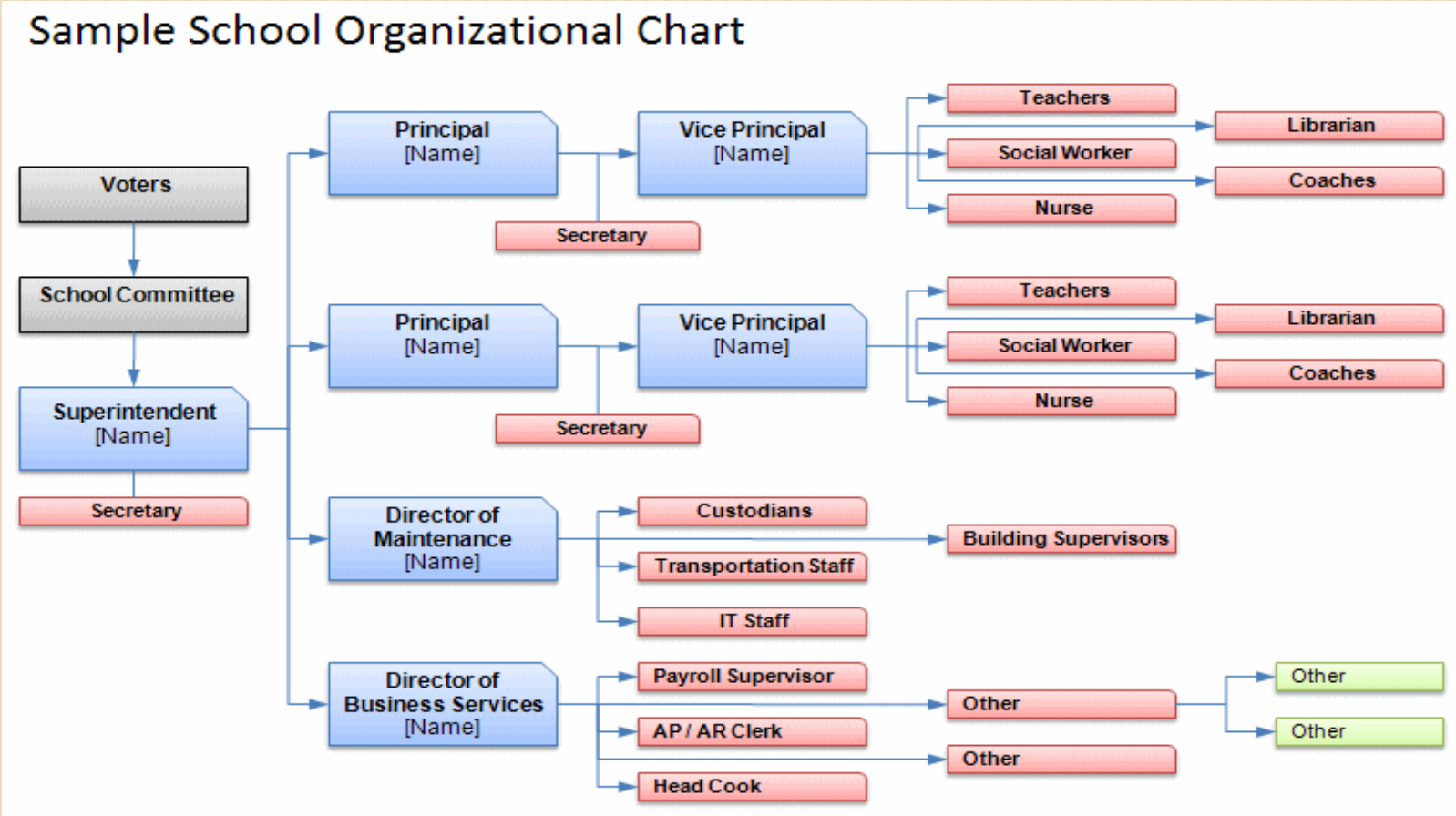


AGENCY'S OWN ASSESSMENT

- "Department of Education reported that it maintained 184 separate information systems with more than 65% of those systems maintained by outside contractors."

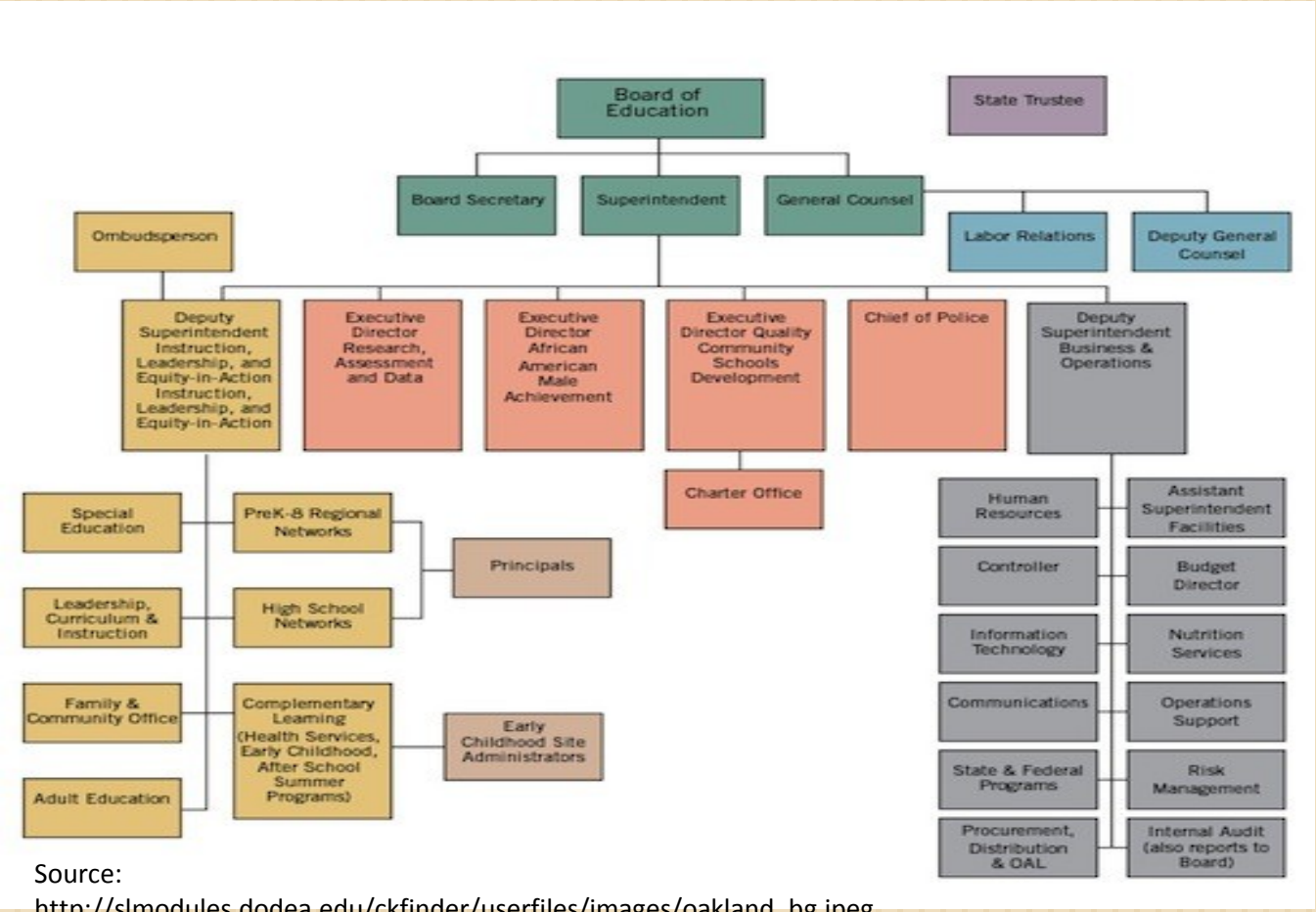
Source: https://www.washingtonpost.com/news/answer-sheet/wp/2015/11/19/congress-blasts-u-s-education-department-for-vulnerabilities-in-data-bases/?utm_term=.cc64f33ef444

SCHOOL STRUCTURE



Source: https://www.vertex42.com/ExcelTemplates/organizational-chart.html

DISTRICT SYSTEM STRUCTURE



Source:
http://slmodules.dodea.edu/ckfinder/userfiles/images/oakland_bg.jpeg

ENTRY POINTS

- Inadequate educator training
- Inadequate security systems for information technology and data
- Poor oversight of third party vendors

PARENT ADVISEMENT

- "Asking schools and other organizations to safeguard your child's information can help minimize your child's risk of identity theft."

Source: https://www.consumer.ftc.gov/articles/0040-child-identity-theft

WAYS TO BE PROACTIVE

- Seek up-graded technology supports for technicians
- Request cyber security and ethics training
- Demand data security training
- Demand info tech and data audits

WAYS TO BE PROACTIVE

- Educator Certification Programs
- Educator in-service Training
- Info Technology Infrastructure Support
- Technology, Internal Controls and Data Audits

WAYS TO BE PROACTIVE

- The National Council for the Accreditation of Teacher Education Programs adopted technology standards in 1998 The Association of School Administrators, in 2001.

Source: https://www.consumer.ftc.gov/articles/0040-child-identity-theft

WAYS TO BE PROACTIVE

- Yet, Data Quality Campaign, American Association of Teacher Education Programs, the CCSSO, NASDTEC, the National Council on Teacher Quality, the National Education Association and WestEd determined these measures have not been applied consistently.

WAYS TO BE PROACTIVE

- The coalition has advocated for “teacher data literacy through state policy” while promoting and incentivizing ongoing technical training [34, p.1].

WAYS TO HELP ME

- Invite me to do an information technology and/or data audit
- Invite me to give a presentation
- Invite me to serve on your advisory board as you consider cyber-training for k-12 (and educators)

WAYS TO HELP ME

- Presenting at the Women and Minorities in Technology Conference in the Spring 2018 on Free resources to jump start your cyber career. If anyone knows of free resources please send an email to me tonya@*i*shareknowledge.com

WAYS TO HELP ME

- Read my book, Fraud in Education Beyond the Wrong Answer
- Purchase RFID 'animal guardian' credit card protectors
- Follow me on Linkedin or Twitter

REASONS FOR VULNERABILITY

↓ Discovery risk	↑ Threat of Exploits
↓ Enforcement risk	↑ Threat of Exploits
↓ Prosecution risk	↑ Threat of Exploits
↑ Undisciplined data use	↑ Threat of Exploits

Source: Fraud in Education: Beyond the Wrong Answer Available at: http://amazon.com/author/tonyajmead

THANKS FOR YOUR TIME

Shared Knowledge, LLC

http://ishareknowledge.com