Managing Cybersecurity Risks in the Digital Campus

Recent Developments in the Threat Landscape, Law, and Risk Mitigation

WIGGIN AND DANA

Overview

- Data security threat environment
- Costs
- Regulatory and legal environment
- Best practices
- Is the education sector prepared?
- Case discussion

© 2015 Wiggin and Dana LLP

WIGGIN AND DANA

Threat environment: Universities at Risk

- Over 50 universities have suffered major breaches in last year
- Approximately 1 breach every week between 2005 and 2013
- In December 2014, UC Berkeley hacked
  - Real Estate Division servers hacked
  - PI of 1,600 individuals accessed, including SSNs and credit card information
- Other breaches in 2014
  - University of Maryland: 309,079 records
  - Indiana University: 146,000 records
  - University of Delaware: 74,000 records

© 2015 Wiggin and Dana LLP

WIGGIN AND DANA

Threat Environment: Sources

Threat	Description
Bot-network operators	Bot-network operators are hackers; however, instead of breaking into systems for the challenge or bragging rights, they take over multiple systems in order to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. The services of these networks are sometimes made available in underground markets (e.g., purchasing a denial-of-service attack, servers to relay spam, or phishing attacks, etc.).
Criminal groups	Criminal groups seek to attack systems for monetary gain.
Foreign intelligence services	Foreign intelligence services use cyber tools as part of their information-gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities.
Hackers	Hackers break into networks for the thrill of the challenge or for bragging rights. Hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use.

Source: DHS-ICS-CERT

© 2015 Wiggin and Dana LLP

WIGGIN AND DANA

Threat Environment: Sources

Threat	Description
Insiders	A principal source of computer crime. Often have unrestricted access to the system and to steal system data. The insider threat also includes outsourcing vendors as well as employees who accidentally introduce malware into systems.
Phishers	Individuals, or small groups, who execute phishing schemes in an attempt to steal identities or information for monetary gain. Phishers may also use spam and spyware/malware to accomplish their objectives.
Spammers	Individuals or organizations who distribute unsolicited e-mail with hidden or false information in order to sell products, conduct phishing schemes, distribute spyware/malware, or attack organizations (i.e., DDOS).
Spyware/malware authors	Individuals or organizations with malicious intent carry out attacks against users by producing and distributing spyware and malware.
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the U.S. economy, and damage public morale and confidence.

Source: DHS-ICS-CERT

© 2015 Wiggin and Dana LLP

WIGGIN AND DANA

Failure to Address the Threat is Costly

- Cost per breached record (Education): $294
- Cost drivers include:
  - Response
  - Notification
  - Hurting current/future alumni donations
  - Ticket/apparel purchases
  - Lost IP

© 2015 Wiggin and Dana LLP

WIGGIN AND DANA

Regulatory Environment

- Payment Card Industry Data Security Standards (PCI-DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- Gramm-Leach Bliley Act (GLBA)
- Family Education Rights and Privacy Act (FERPA)
- Red Flags Rule
- Federal Information Security Management Act (FISMA)

© 2015 Wiggin and Dana LLP

WIGGIN AND DANA

Regulatory Environment: FTC Example

- The Federal Trade Commission (FTC) seeks to protect consumers when businesses fail to protect their information through enforcement and policy initiatives
- Standard injunctive terms of FTC consent decrees:
  - Written program for reasonable security (a/k/a WISP)
  - Accountability and governance, including a point person
  - Periodic risk assessments and adjustment of practices

© 2015 Wiggin and Dana LLP

WIGGIN AND DANA

Regulatory Environment: FTC Example

- Standard injunctive terms of FTC consent decrees (continued):
  - Senior management and/or board involvement
  - Ability to detect, close, and respond to a breach (IRP)
  - Security and privacy by design
  - Security and privacy awareness training
  - Oversight of vendors and other 3rd parties

© 2015 Wiggin and Dana LLP

WIGGIN AND DANA

Notification Laws: A Complex Web

- There is no national data breach notification standard . . . Yet
- You have data on thousands of current and former students
  - Do you know in which states they live?
  - Are you familiar with the data breach notification requirements of each of those states?
  - Certain states, such as Massachusetts, have pre-breach data handling requirements

© 2015 Wiggin and Dana LLP

WIGGIN AND DANA

Growing Liability

- Class action update
  - Only the Connecticut AG may bring an action for violation of the CT data breach notification statute
  - Historically, plaintiffs have failed to convince courts they have suffered "actual harm," but this may be changing
- Individuals in Connecticut now can bring suit for HIPAA violations
  - *Byrne v. Avery Center for Obstetrics and Gynecology* (CT 2014)
  - HIPAA for a breach of confidential health information as HIPAA provides no private cause of action.

© 2015 Wiggin and Dana LLP

WIGGIN AND DANA

Best Practices

- CISOs make a difference
- Documents: WISP, IRP
- Regular network testing
- Training
- Cyber liability insurance
- Encryption
- Understanding security vs. IT
- Data disposal

© 2015 Wiggin and Dana LLP

WIGGIN AND DANA

Best Practices: Vendor contracts

- Access, use, and disclosure restrictions consistent with applicable laws, regulations, and institutional policies
- Detailed data security requirements, including
  - Encryption
  - Network and systems security tools and monitoring
  - Incident response plans

© 2015 Wiggin and Dana LLP

WIGGIN AND DANA

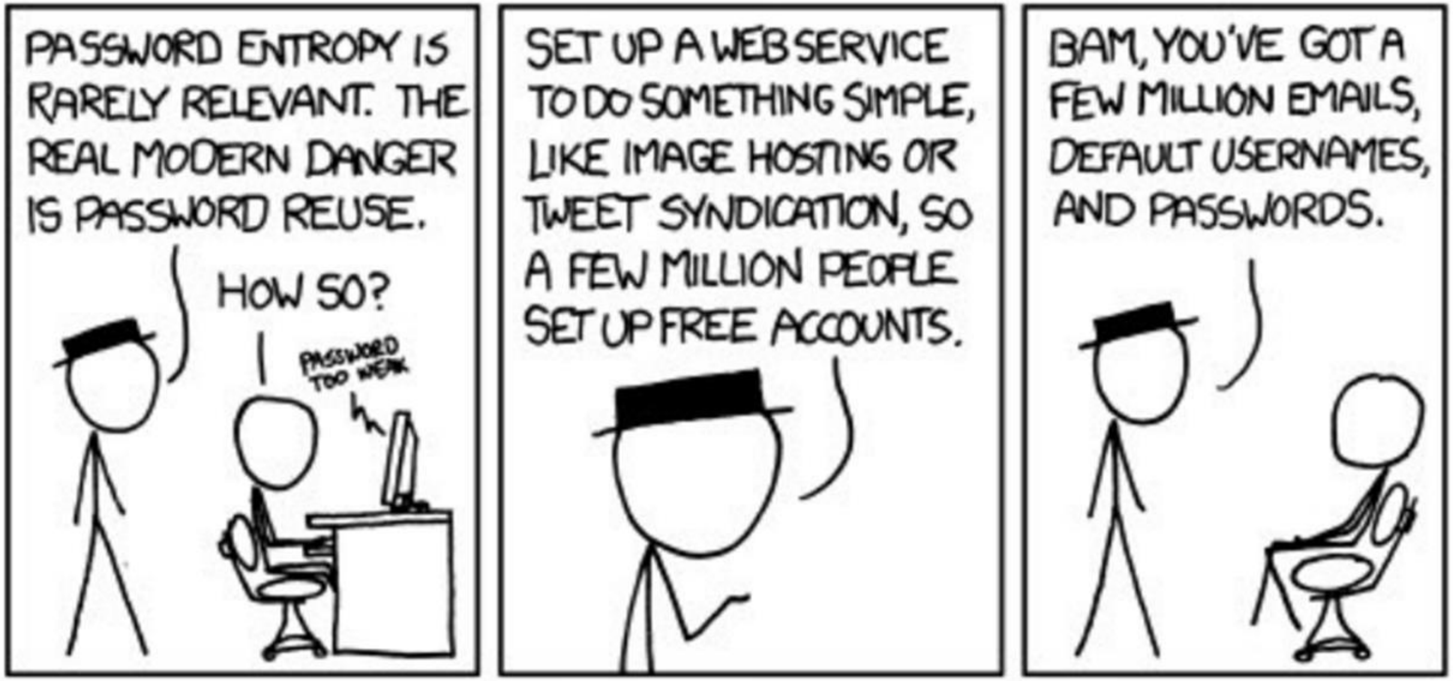
Best Practices: Vendor contracts

- Audit rights and reports
- Periodic risk assessments and reports
- Terms allocating financial liability for data security breaches
- Ownership of data

© 2015 Wiggin and Dana LLP

WIGGIN AND DANA

Best Practices: Passwords

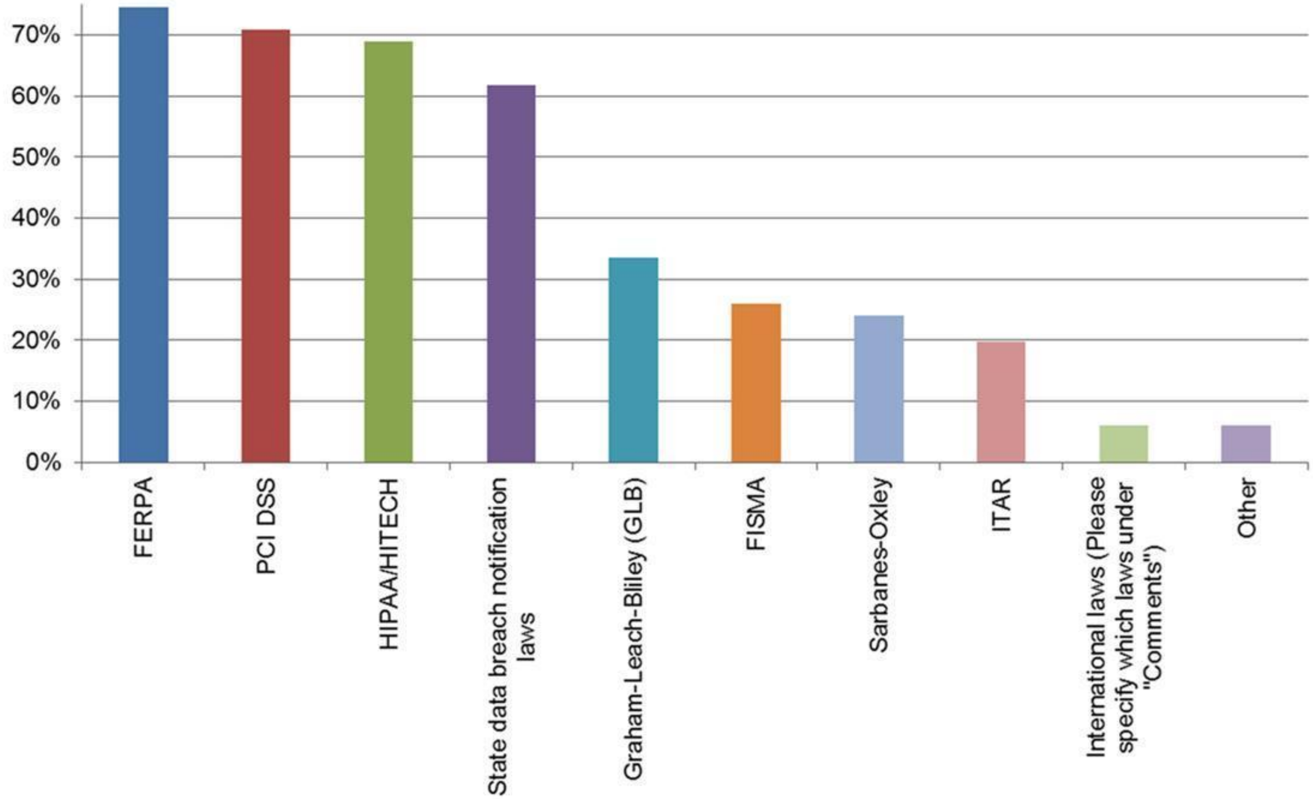

PASSWORD ENTROPY IS RARELY RELEVANT. THE REAL MODERN DANGER IS PASSWORD REUSE.
HOW SO?
PASSWORD TOO WEAK
SET UP A WEB SERVICE TO DO SOMETHING SIMPLE, LIKE IMAGE HOSTING OR TWEET SYNDICATION, SO A FEW MILLION PEOPLE SET UP FREE ACCOUNTS.
BAM, YOU'VE GOT A FEW MILLION EMAILS, DEFAULT USERNAMES, AND PASSWORDS.

Source: xkcd

© 2015 Wiggin and Dana LLP

WIGGIN AND DANA

Is the Education Sector Ready?

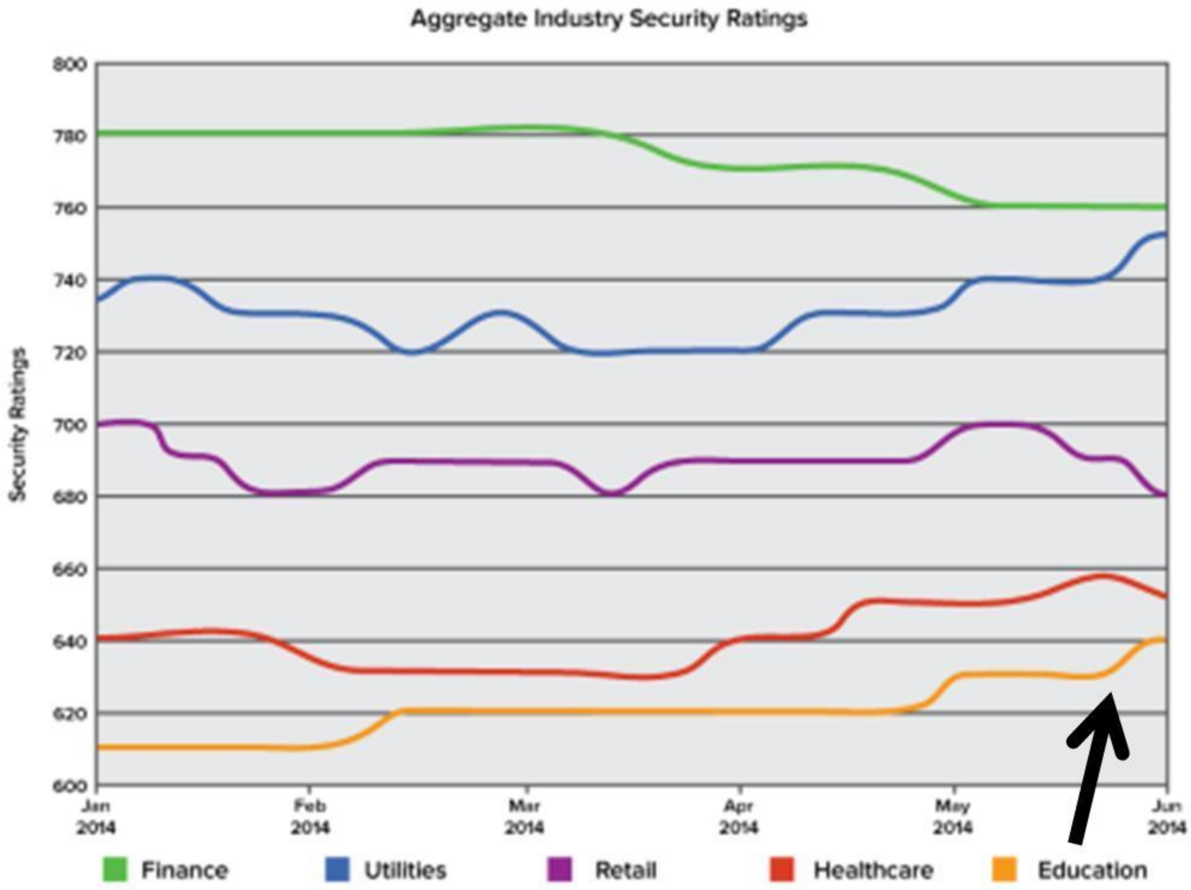


Source: SANS 2014 Higher Education Survey

© 2015 Wiggin and Dana LLP

WIGGIN AND DANA

Is the Education Sector Ready?



Source: BitSight, August 2014

© 2015 Wiggin and Dana LLP

WIGGIN AND DANA

Case Discussion: Point Loma

- In October 2014, Point Loma Nazarene University (CA) hacked
- School has 3,500 students
- Hackers accessed SSNs, birthdates, credit card information, user names, passwords, DL numbers
- Result of a phishing attack
- Attack occurred over two-week period
- Unauthorized access of 5 staff email accounts

© 2015 Wiggin and Dana LLP

WIGGIN AND DANA

Contact Information

John B. Kennedy
203.363.7640
jkennedy@wiggin.com

Michael T. McGinley
203.363.7638
mmcginley@wiggin.com

© 2015 Wiggin and Dana LLP

WIGGIN AND DANA

This presentation is a summary of legal principles.

Nothing in this presentation constitutes legal advice, which can only be obtained as a result of a personal consultation with an attorney.

The information published here is believed accurate at the time of publication, but is subject to change and does not purport to be a complete statement of all relevant issues.

© 2015 Wiggin and Dana LLP

WIGGIN AND DANA