PRESENTATION

Privacy and Data Security: Hot Topics for Higher Education Institutions

Dan Cohen

Eric Setterlund, CIPP/US

Fundamentals: What is Privacy?

- Generally, “privacy” is a concept centered on access, uses and disclosures of personal information

- No general Constitutional “Right to Privacy” in the U.S.
  - Privacy inferred from “liberties” protected by the Due Process Clause of the 14th Amendment
  - Extensions of “right to privacy” through the 1st, 4th and 5th Amendments

- “Right to Privacy” is a fundamental human right in the EU but not in the U.S.

U.S. Privacy Protection is a Patchwork

- For example:
  - Online Privacy / Consumer Protection Laws
    - FTC Act
    - COPPA – Children's Online Privacy Protection Act
  - Communication, Marketing and Surveillance Laws
    - ECPA – Electronic Communications Privacy Act
    - TCPA – Telephone Consumer Protection Act
    - CAN-SPAM – Controlling the Assault of Non-Solicited Pornography and Marketing Act
    - VPPA – Video Privacy Protections Act
  - Financial Privacy Laws
    - FCRA / FACTA – Fair Credit Reporting Act / Fair and Accurate Credit Transactions Act
    - GLBA – Gramm-Leach-Bliley Act
  - Health Privacy Laws
    - HIPAA / HITECH – Health Insurance Portability and Accountability Act / Health Information Technology for Economic and Clinical Health Act
  - Education laws
    - FERPA
  - State laws
    - Federal law equivalents
    - Social Security Number Protection laws

Fundamentals: What is Security?

- Generally, “security” relates to the measures undertaken to protect personal information against impermissible access, uses and disclosures
  - Technical, physical and administrative *safeguards* to ensure *confidentiality*, *integrity* and *availability* of protected data
    - *Don’t forget about hard copy documents!*
- Foundation of any security program is ongoing risk analysis and risk management

Security Risk Analysis & Management

"[a] flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy."

Vulnerabilities can be technical or non-technical.

"[t]he potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability."

Threats can be natural, human or environmental.

"the net mission impact considering (1) the probability that a particular [threat] will exercise (accidentally trigger or intentionally exploit) a particular [vulnerability] and (2) the resulting impact if this should occur."

A Vulnerability potentially triggered or exploited by a Threat equals a Risk.

Source: NIST SP 800-30, Risk Management Guide for Information Technology Systems

Fundamentals: What is a Breach?

- Generally, an *impermissible disclosure* of *protected data*
  - Depends on definitions, standards, safe harbors set forth in applicable law
  - Don’t forget about the tort of negligence
    - What was the expectation of privacy and what duty did you have to protect it?

Breach Notification Laws

- No federal breach notification law of general application (yet)
- State breach notification laws:
  - Generally apply to “breaches of the security of a system” involving “personally identifiable information” (PII):
    - Varying definitions of PII
    - Which law applies depends on state(s) of residence of the affected individual(s)
    - Many states have encryption safe harbors
    - Varying notification requirements (e.g., timeframe and notice recipients)
  - Except as noted below, all states, D.C., Puerto Rico, U.S. Virgin Islands and Guam have a breach notification law:
    - No data breach law: Alabama, New Mexico, South Dakota
  - Tennessee Data Breach Notification Law: Tenn. Code Ann. § 47-18-2107

FERPA and Confidentiality Concerns

FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT OF 1974 ("FERPA")
20 U.S.C. § 1232g
(Title 34 C.F.R. Part 99 – U.S. Department of Education)

- Gives college students the rights to:

  1. Control the disclosure of their "education records" to others
  2. Inspect and review their own "education records"
  3. Seek amendment of their "education records"

- The rights belong to the student, not his or her parents or legal guardians, once s/he enrolls in a college or university

- Rights can be waived by the student's express consent

FERPA and Confidentiality Concerns
(continued)

KEY FERPA DEFINITIONS	
"Education Records": 34 C.F.R. § 99.3 (emphasis added)	"Those records that are: (1) Directly related to a student; and (2) Maintained by an educational agency or institution or by a party acting for the agency or institution
"Educational institution": 34 C.F.R. §§ 99.1 and 99.3	"[A]ny public or private…institution" that receives funds "under any program administered by the Secretary [of Education]."
"Record": 34 C.F.R. § 99.3	"[A]ny information recorded in any way, including, but not limited to, handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche."

FERPA and Confidentiality Concerns
(continued)

What Can You Disclose?

- "The parent or eligible student shall provide a signed and dated written consent before an educational agency or institution discloses personally identifiable information from the student's education records, except as provided in § 99.31."

SOURCE: See 34 C.F.R. § § 99.30

FERPA and Confidentiality Concerns
(continued)

FERPA ***does*** permit a school to inform the alleged victim of its final determination and any disciplinary sanctions imposed on the accused in sexual violence cases (as opposed to all harassment and misconduct covered by Title IX)

SOURCE: See 34 C.F.R. § § 99.31(a)(13) and (14); Questions and Answers on Title IX and Sexual Violence, Press Release, April 29, 2014, Office for Civil Rights of the Department of Education.

FERPA and Confidentiality Concerns
(continued)

What can you disclose?
(continued)

- **… unless joint records are "inextricably intertwined" …**
  - "Under [20 U.S.C. 1232g(a)(4)(A) and 34 C.F.R. § 99.3] … [an] eligible student … has a right to inspect and review any witness statement that is directly related to the student, even if that statement contains information that is also directly related to another student, if the information cannot be segregated and redacted without destroying its meaning."
    - "For example, … both John and Michael would have a right to inspect and review the following information in a witness statement maintained by their school district because it is directly related to both students: ''John grabbed Michael's backpack and hit him over the head with it.'' …
    - "[B]efore allowing Michael [] to inspect and review [other statements, the school] must also redact any information about John (or any other student) that is not directly related to Michael, such as: ''John also punched Steven in the stomach and took his gloves.'' Since Michael[] likely know[s] … about other students involved in the altercation, under paragraph (g) the district could not release any part of this sentence to Michael[]."
- **SOURCE**: 73 Fed. Reg. at 74832 (Dec. 9, 2008) (DOE's comments to the FERPA regulatory amendments)

FERPA and Confidentiality Concerns
(continued)

What Can You Disclose?
(continued)

- **… or unless the joint records will be "used" in such a way that requires "equal access" under VAWA**
  - "The VAWA regulations (34 C.F.R. § 668.46(k)) state that disciplinary proceedings "***in cases of alleged dating violence, domestic violence, sexual assault, or stalking*** … [will include] (3)(i) A prompt, fair, and impartial proceeding … that is … (B) [c]onducted in a manner that (3) ***[p]rovides timely and equal access to the accuser, the accused, and appropriate officials to any information that will be used during informal and formal disciplinary meetings and hearings***…"

- While the regulation doesn't specifically address redaction, Section 668.46(*l*) states that "compliance with paragraph (k) of this section does not constitute a violation of FERPA."

FERPA and Confidentiality Concerns
(continued)

What Can You Disclose?
(continued)

- The VAWA exception is narrow, as it:
  - Does not apply in cases involving sexual harassment or retaliation
  - Does not permit disclosure to witnesses

FERPA and Confidentiality Concerns
(continued)

Requests for Confidentiality
(continued)

- For Title IX purposes, if a student **still** requests that his or her name not be revealed to the alleged perpetrator ***or*** asks that the school not investigate or seek action against the alleged perpetrator, **the school will need to determine whether or not it can honor such a request while still providing a safe and nondiscriminatory environment for all students**, including the student who reported the sexual violence

- The report still has to be investigated

SOURCE: Questions and Answers on Title IX and Sexual Violence, Press Release, April 29, 2014, Office for Civil Rights of the Department of Education.

Emerging Threats
&
Challenges

W-2 Phishing Scams

- It is a Business Email Compromise (BEC) attack
- Plays on trust relationships by spoofing email address of persons with authority
- More than 41 large companies were hit in 1Q 2016

- SOLUTION:
  - Training and Awareness
    - Empower employees
      - Permit them to question information requests, no matter the source
    - Train them to alert key members of your University

Ransomware

- Ransomware is a specialized form of malware that blocks access to information or systems until a sum of money is paid
  - Drive-by-download, malicious links and phishing scams

Preparing for Ransomware

- Have external back-ups
- Train your employees in:
  - Recognizing the threat
  - Responding to the threat
- Keep your system, software and applications updated
- Segment your network, if possible

Cloud Security

- Require meaningful due diligence before outsourcing to third party vendors
- Address risk contractually
  - Beware start-up vendors

Data Retention

- When you don't need information anymore DESTROY IT
- Hoarding unnecessary data just leads to greater risk
- Make sure assets are appropriately wiped before decommissioning an asset
  - *Don't forget mobile devices!*

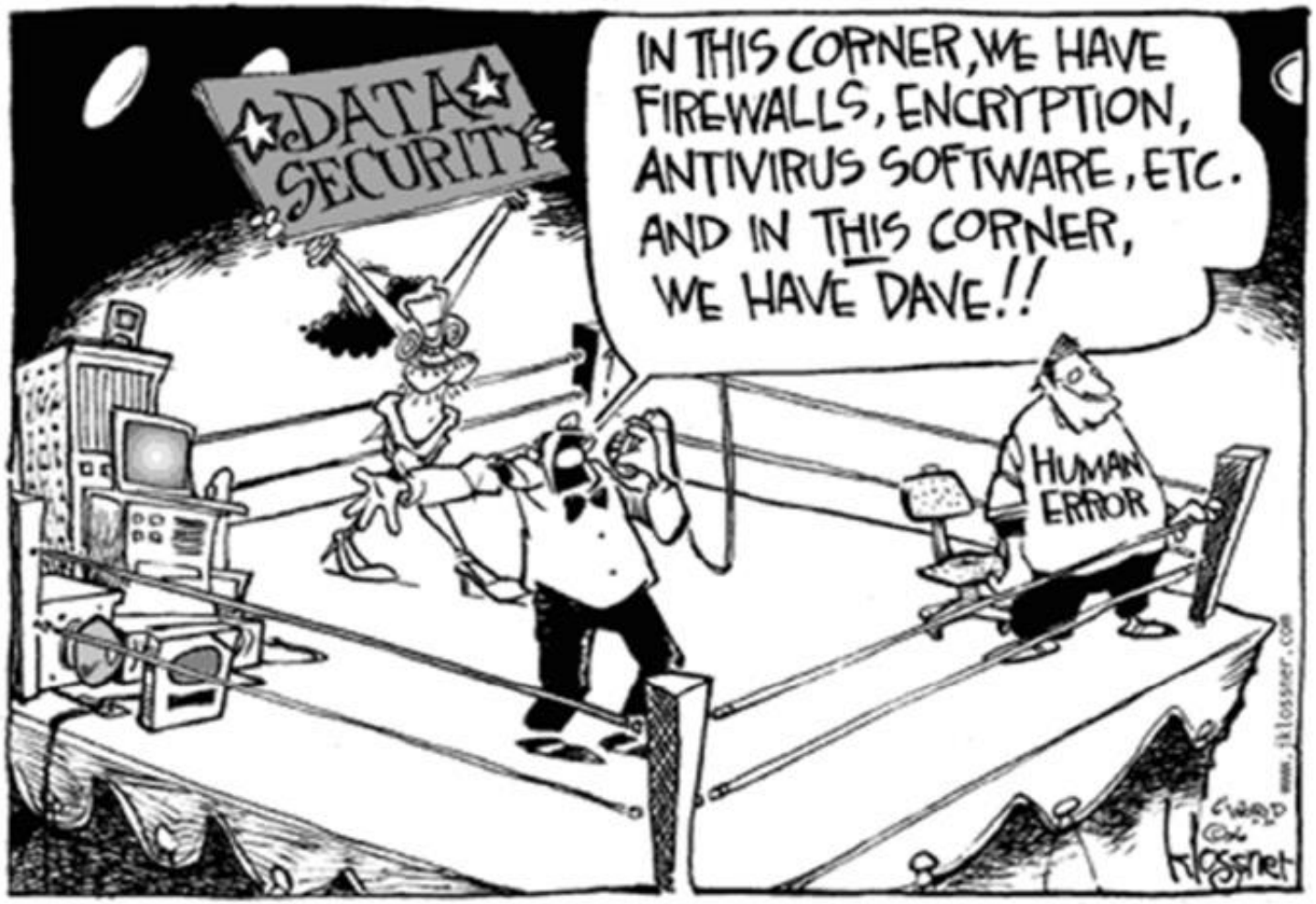
Protections and Strategies Play Book: Key Tips

- Minimize data collection and retention:
  - Think (e.g., rewards programs, payment data) – what do you really need and for how long? DELETE, DESTROY, DELETE, DESTROY
- Implement role-based access rights and prompt termination of rights:
  - Exercise due care with “Keys to the Kingdom” (local and global admin rights)
- Encrypt data at rest and data in motion
- Evaluate cost / benefit of “Bring Your Own Device” (BYOD) programs:
  - Are the risks worth the convenience?
  - Can you get agreement to wipe the device?
- Provide secure access to Internet:
  - Think Internet of Things; general WiFi offering
- Implement meaningful firewalls within enterprise and franchised systems:
  - Robust back-up systems in offline environment

Key Tips (continued)

- Conduct penetration and vulnerability testing
- Evaluate cyber-liability insurance coverage (including for vendors)
- Training, training and more training
- Last, but not least, Privacy and Information Security Program should be:
  - Dynamic
  - Adaptable
  - Defensive / Reactive
  - Offensive / Proactive
  - Endorsed and promoted by Administration

A Challenging Reality



Questions?