

It's Not Just FERPA

Privacy and Security Issues in Higher Education

Alisa Chestler – Washington, D.C.

Eric Setterlund, CIPP/US – Chattanooga, Tennessee

Today's Topics

- Our world
- What kind of information are we concerned about?
- What is “privacy and information security?”
- What is a “data breach?”
- What laws impact higher education institutions?
- What should you do?

Our World



“Sensitive Information” is What We Are Concerned About

- Educational Records
- Employee health information (for group health plans)
- Employment files
- Accounting and financial reporting information
- Company trade secrets (products, customers, business strategies, etc.)
- Legal files: litigation, patent, M&A, etc.
- Network user IDs and passwords
- Student financial information
- Credit card information/account information

What is “Privacy and Information Security,” Anyway?

- Two sides of the same coin – ensuring confidentiality of information
- Privacy is the objective, security is means

Applicable Regulatory Regimes

- **Family Educational Rights and Privacy Act (FERPA)**
- **Health Insurance Portability and Accountability Act (HIPAA)**
- Payment Card Industry Data Security Standards (PCI-DSS)
- Family and Medical Leave Act
- Americans with Disabilities Act
- 42 C.F.R. Part 2
- Privacy Act
- FCRA/FACTA
- Genetic Information Nondiscrimination Act
- CAN-SPAM
- Library Patrons Acts?
- Applicable destruction laws?

Can't forget about state laws

- 47 states with laws.



A Case Study

- A student is a victim of sexual assault on campus.
- She is unsatisfied with the university's response and decides to sue the university.
- Should the university access the student's psychotherapy records from the student health center?

Legal Implications

- Title IX
- FERPA or HIPAA?
 - Treatment Records/Educational Records
 - <http://www2.ed.gov/policy/gen/guid/fpco/doc/ferpa-hipaa-guidance.pdf>
 - http://www.hhs.gov/ocr/privacy/hipaa/faq/ferpa_and_hipaa/518.html
- Any applicable state laws limiting disclosure of psychotherapy records?

Legal Implications (continued)

**What's in your notice of
privacy practices?**

Surveillance



What is a Data Breach?

A data breach is the unauthorized disclosure *or the unauthorized use of information.*

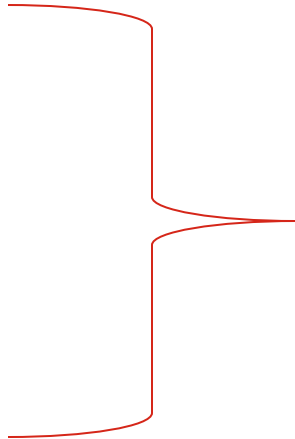
The Culprit?



EMPLOYEES!



Risk Management Considerations: Data Breach

- High cost of data breach response (potentially astronomical)
 - forensic consultant
 - breach notification
 - call center
 - credit monitoring
 - legal fees
 - PR costs
 - government investigation costs
 - civil monetary penalties and fines
 - regulatory fines
 - Reputational harm – public relations fiasco
- About \$200 per person per incident
- 

Off-Campus Information

Employees Removing Information from Campus

- Laptops, iPhones and iPads at home or sitting around in airports, hotels, bars and unoccupied cars
- Forgotten thumb drives in sock drawers
- Personal email and personal cloud storage accounts (e.g., DropBox)
- All of the above for former employees who didn't return or destroy the information

Third Parties Holding or Accessing Information under Contract

- Physical files stored offsite
- Service vendors
- Virtual data rooms
- IT consultants
- Software-as-a-service (SaaS) vendors

Other *

- Discarded computers
- Copiers returned after lease expired
 - * hopefully wiped of data

**How should you
address the issue?**

Essential Elements of Any Compliance Program

- Designated responsible person/committee (accountability)
- Policies and procedures (documented expectations)
- Training and awareness (understanding of expectations)
- Open communication (channels to report compliance concerns)
- Monitoring (mechanisms to discover non-compliance)
- Enforcement (sanctions for non-compliance)
- Response plan (procedures to address effects of non-compliance)

Some of the Required Policies and Procedures

- Privacy
 - Documented policies and procedures
 - Formal training and security awareness program
 - Sanctions for non-compliance
 - Permitted and prohibited uses and disclosures
 - Minimum necessary use
- Security
 - Security management program
 - Periodic security risk analyses
 - Role-based access
 - Physical security protocols
 - Technical security protocols

Fundamentals of Security Risk Management

ASSESSMENT

and

CONTROL

Options for Dealing with Security Risks

- Three options for addressing any given risk:
 - **Mitigate it** – implement controls to reduce likelihood and/or impact of the threat (i.e., abate the vulnerability)
 - **Transfer it** – put the risk off to an insurer or contract party
 - **Accept it** – if likelihood and impact of threat are limited, or if cost to mitigate or transfer is too high

- **Can only address risks that have been**

IDENTIFIED and
ASSESSED

The Risk Assessment

- Cannot control a risk that is not identified
- We can always lock down information so tightly that no one can use it, but we cannot implement appropriate controls without understanding the risk to be controlled
- Security risk analysis:
 - Focus attention and resources (i.e., controls) on threats representing the

GREATEST TOTAL RISK

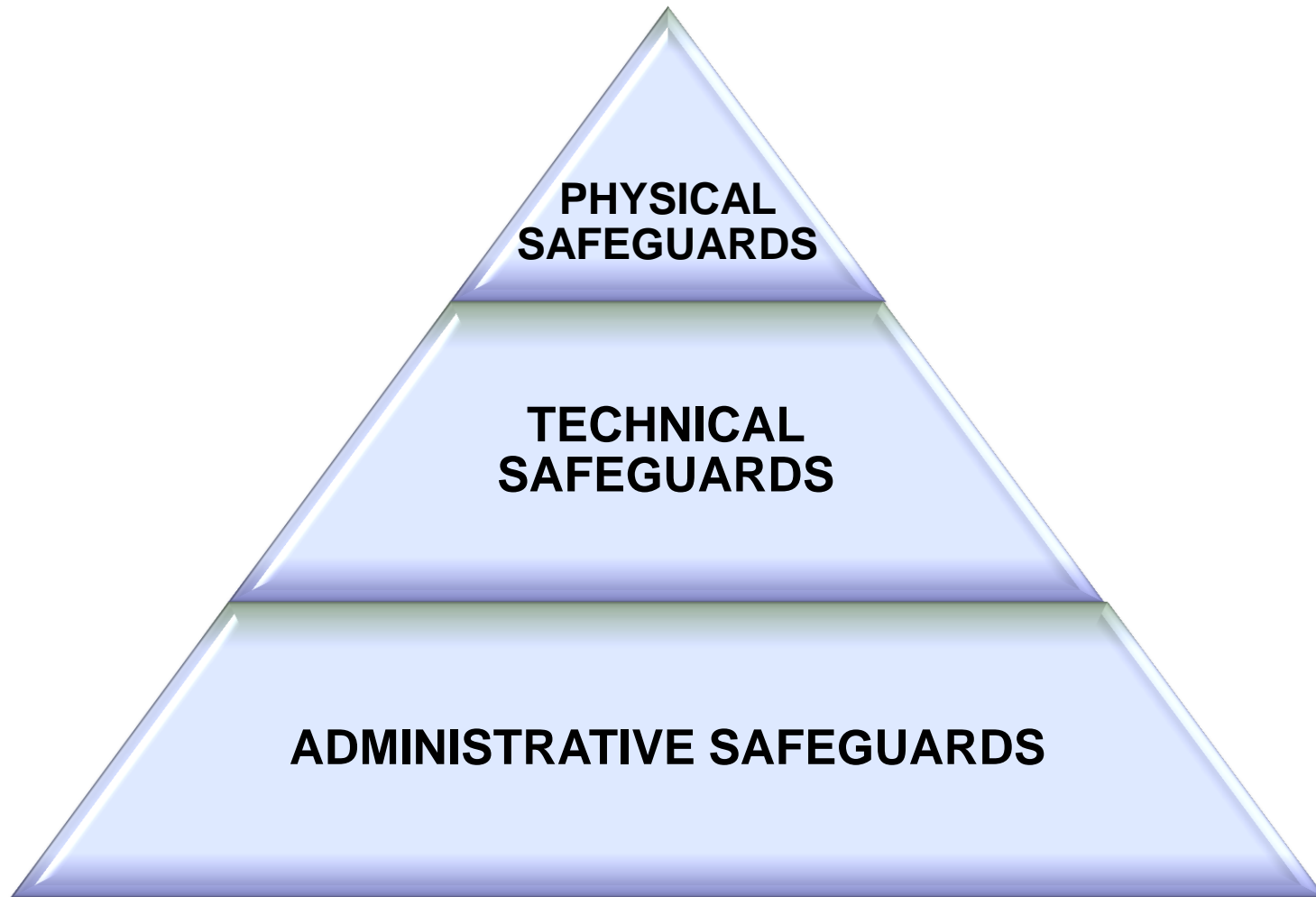
The Risk Assessment Process

Set Your Boundary



Implement Appropriate Controls

Risk Mitigation Strategies – Internal Controls



Risk Mitigation Strategies – Internal Controls

- Physical safeguards
 - Examples of threats:
 - external environment (lightning, tornado, flood, riots, power outage)
 - internal environment (water leaks, fire, excessive heat or humidity)
 - human threats
 - intentional (theft, vandalism, espionage)
 - inadvertent (loss, accidental erasure, unintended change)
 - Examples of controls:
 - locks on doors, file cabinets, etc.
 - ID badges and visitor escorts
 - physical intrusion detection systems
 - redundant power and HVAC systems
 - fire suppression systems
 - back-ups

Risk Mitigation Strategies – Internal Controls

- Technical safeguards
 - Examples of threats:
 - access by unauthorized persons
 - inability to discern improper access or transmission
 - unauthorized or unintended changes to or deletion of information
 - data corruption
 - Examples of controls:
 - strong passwords
 - firewalls
 - access and activity logs
 - anti-virus software
 - network intrusion detection systems
 - *encryption, encryption, encryption*
 - **Encryption (for data at rest and in transit) cures many ills**

Risk Mitigation Strategies – Internal Controls

- Administrative safeguards
 - Examples of threats:
 - inadvertent disclosure or loss of information
 - improper use of information
 - unknown unknowns
 - Examples of controls:
 - **appropriate policies and procedures are the foundation**
 - key principles of least privilege, minimum necessary, and fail securely
 - security awareness program (*training, re-training and reminders*)
 - monitoring for violations and **sanctioning violators**
 - regularly performed security risk analyses
 - Largely the domain of the legal/compliance function rather than IT

Risk Mitigation Strategies for Service Providers

- Due diligence – what institutions should do before handing over client info
 - Questions to ask:
 - Designated privacy and security officer(s)? When designated?
 - Formal, written privacy and security policies and procedures?
 - Security risk assessment? Performed by qualified third party? When?
 - Any use of downstream hosting vendors or data centers?
 - Any security-related audits or certifications? Same question for any downstream service provider.
 - Ever experienced a data breach involving personal information of individuals?
 - Maintain cyber-liability insurance? What coverage(s)?
 - Examine privacy and security policies and procedures
 - Talk with privacy and security officer(s)