Higher Ed
Data Security

Mike Hayes
mhayes@mmwr.com
215.772.7504

Priya Roy
Proy@mmwr.com
215.772.7430

Here's Your HYPO

9 a.m.:
Unauthorized intrusion into U servers discovered; CIO still determining scope/source, systems affected, duration of intrusion, potential damage, and whether PII has been compromised

Noon:
Posts appear on YIK YAK and other anonymous sites alleging possession of students' PII and demand for BitCoin payment to avoid public release

Legal / Regulatory Framework

FERPA

FTC
Red Flag
Gramm Leach Bliley

HIPAA

HITECH Act

State Notification and
Privacy Laws

FTC

GLBA

Compliance with other laws
Privacy Safeguards

Red Flag Rules

Risk Assessment
Detection
Appropriate Response Protocols
Periodic re-evaluation

State Laws

What State law matters?
Depends on school location and affected students' states of residence

Examples of State Laws:
Pennsylvania Breach of Personal Information Notification Act
73 P.S. §§ 2301, *et seq.*
and
California General Breach Notification Statute
CAL. CIV. CODE § 1798.81.5

DOE 7.29.15
"Dear Colleague" Letter

Warning that HEIs need to …

Assess risks of data breach and identity theft

Classify documents and information set appropriate levels of security

Develop and implement policies to cost-effectively reduce risks

Monitor, test and improve

Before the Crisis

Establish Information Security Working Group

Chair needs clear authority to direct others across the U

Working Group will:

Develop risk assessments, protocols for security, response plan, notifications, etc.

Evaluate systems and 3d party vendor relationships

Look at cyber insurance

Demonstrate U's awareness and commitment

Back to the HYPO

9 a.m.:
Unauthorized intrusion into U servers -
CIO still determining scope/source, what systems, duration of intrusion, damage, and whether PII actually has been compromised

Noon:
Postings appear on YIK YAK and other anonymous sites alleging possession of PII and demand for BitCoin payment to avoid public release

What now?

Diagnose/identify
Fix
Preserve evidence
Prevent recurrence
Notify Law Enforcement [situation-dependent]
Report [as required]
Develop notifications [as required]

And then ….

Get ready for the next one.

Appendix of Relevant Statutes and Materials

FERPA
GLB Act
Red Flag Rules
HIPAA
HITECH Act
Pennsylvania Breach of Personal Information Notification Act
California General Breach Notification Statute