



APRU 2010

IT Security Issues in Higher Education

Robert Lau
Director, Information Security
Information Technology Services
University of Southern California



The Higher Ed Security Model

The Real World™ – deny all / allow few
Higher education – allow all / deny few

Is this still true?

Is it a valid model?

Is it scalable and sustainable?



Threats & Issues

Worms, viruses, malware

Phish / spear phishing

Keyloggers / information stealers

Single sign-on

Network access control

Data loss

Regulatory compliance

Trust

Education

Privacy

Censorship



Keyloggers / information stealers

Vectors

- Email – spam, phish, spear phish
- Web – malicious sites, social networking
- Human – social engineering

Consequences

- Compromised accounts
- Loss of academic integrity
- Regulatory violations
- Data loss
- Financial loss

Recent case

Duanesburg Central School District

On Friday, Dec. 18, thieves tried to electronically transfer \$1.86 million from the district's account at NBT Bank to an overseas account. The following Monday, the attackers attempted to move another \$1.19 million to multiple overseas location. It wasn't until the next day, when transfers totaling \$758,758.70 were flagged by a bank representative as suspicious, that the two previous unauthorized transactions were discovered, school officials said.

[FBI Investigating Theft of \\$500,000 from NY School District](#)

Brian Krebs, 2010-01-05



Solutions

User education

Anti virus/spyware/malware (zero-day)

Two-factor authentication (MITMA)

Firewalls (fast-flux)

URL filtering

Compartmentalization