

## Brave New World of Cyber Risks: Don't Take This Trail Without a Map



### Rodney Petersen

Senior Government Relations  
Officer and Managing Director  
EDUCAUSE

### Shannan Fort

Broker  
Aon Risk Solutions

### Holly Towle

Partner  
K&L Gates LLP

### Steve Pacheco

Assistant Vice President  
ACE Professional Services



UNIVERSITY RISK MANAGEMENT AND INSURANCE ASSOCIATION

## Introduction of Panel

- Rodney Petersen, EDUCAUSE
- Holly Towle, K&L Gates LLP
- Shannan Fort, Aon Risk Solutions
- Steve Pacheco, ACE Professional Risk

**Expedition Risk!**  
URMIA + Portland + 2011



## Learning Objectives

- Recommendations on how to evaluate and manage cyber risk
- Transfer risk through insurance coverage, with specific examples of policy language
- Claim scenarios
- Cyber liability coverage availability



***Expedition Risk!***  
URMIA ☉ Portland ☉ 2011

## Flow of Panel

- Practitioner's Perspective...what are practical "best practices"
- Legal Scene...where higher education sits on the map
- Broker's View...getting client from concerned to covered
- Carrier's Corner...available coverages & claim scenarios



***Expedition Risk!***  
URMIA ☉ Portland ☉ 2011

## Practitioner's Perspective

- All-Hazards Approach to Asset Protection

- People
- Physical
- Cyber



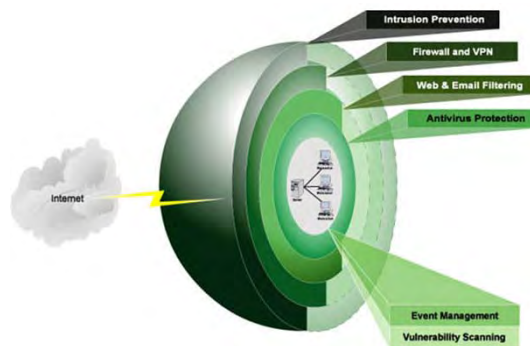
**Expedition Risk!**

URMIA ⊕ Portland ⊕ 2011

## Practitioner's Perspective

- Safeguarding Cyber Assets

- People
- Process
- Technology

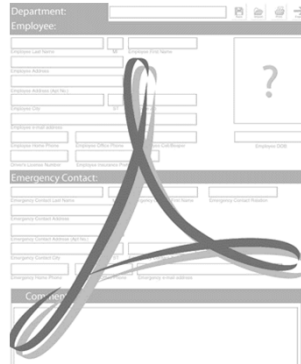


**Expedition Risk!**

URMIA ⊕ Portland ⊕ 2011

## Practitioner's Perspective

- Standards-Based Approach to Information Security
  - ISO 27002
  - NIST 800-53
  - PCIDSS
  - COBIT
  - State Requirements



**Expedition Risk!**

URMIA ⊕ Portland ⊕ 2011

## HE Information Security Guide

- Risk Management
- Security Policy
- Organization of Information Security
- Asset Management
- Human Resources Security
- Physical and Environmental Security
- Communications and Operations Management



**Expedition Risk!**

URMIA ⊕ Portland ⊕ 2011

## HE Information Security Guide

- Access Control
- Information Systems Acquisition, Development, and Maintenance
- Incident Management
- Business Continuity
- Compliance



***Expedition Risk!***

URMIA  Portland  2011

## Legal Scene

Where is higher education on the *legal* map of cyberspace?



***Expedition Risk!***

URMIA  Portland  2011



## Higher Education Is at a Complex Traffic Circle of Numerous Legal Rules...



### ...e.g., Roads to Major Federal Statutes

- **FERPA** (for education records)
  - read *introduction* in 73 F.R.74806 (12/9/08)
  - non-coverage coverage!
  - willful failure to comply = federal funding risk
- **GLBA**
  - covered if “**financial institution**”
  - “**Safeguards**” rule *applies*
  - “**Privacy**” rule doesn’t (*if* FERPA compliant)
- **FTC?** (e.g., UDAP)

**Expedition Risk!**  
URMIA ☉ Portland ☉ 2011

### Roads to OTHER Data Protection Laws:

- **PCI** (Payment Card Industry Standard) & ACH (fundraisers; tuition etc.)
- **Authentication** (e.g., Illinois biometrics, CA credit card "ID"; swiping & copying laws)
- **Access Controls** (e.g., employee records + FERPA)
- **Data security breaches** (46 states + ?)
- **Disposal** (of data and hardware), e.g., FCRA (cons. reports on employees or background checks)
- **Transmission** (e.g., SSNs, PII) – *are you emailing?*
- **RFID**
- **Service Provider contracts** (+ "FERPA" school official concepts)

***Expedition Risk!***

URMIA ⊕ Portland ⊕ 2011

### Roads *Beyond* Privacy that Create Cyber Dangers for Universities with E-data

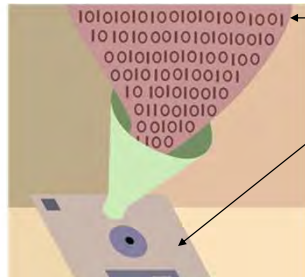
- **FRCP:** ESI discovery rules (can you *produce* your records in litigation?)
- **E-evidence rules** (can you *admit* your records?)
- **E-system risks** (e.g., free form entry fields – what *new* records are you creating?)

***Expedition Risk!***

URMIA ⊕ Portland ⊕ 2011



**Watch Out for Potholes re: NATURE of Information  
vs. Goods / Property – *Impacts Law and Insurance Coverage!***



← This intangible (thing in action) is  
the information / data

→ This (tangible item) is a red herring  
and confuses outcomes

→ This is the increasing reality



**Expedition Risk!**

URMIA ⊕ Portland ⊕ 2011

**Many Types of Data Security Breaches –  
What Laws and What Coverage Exist?**

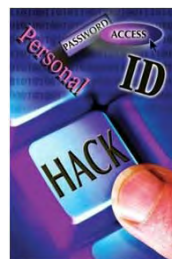


Physical theft



Complex systems

Employees &  
human error



Hackers – ??



Laptops

**Expedition Risk!**

URMIA ⊕ Portland ⊕ 2011



## Broker's View

- Many Challenges

- Decentralized structure
- Multiple IT environments with various controls
- Loss history difficult to obtain
- Content: Library and UGC

**Expedition Risk!**

URMIA ⊕ Portland ⊕ 2011

## Broker's View

- Carriers have Concerns:

- Top three underwriting concerns
- Top three issues
- Results of PRS Carrier Survey

**Expedition Risk!**

URMIA ⊕ Portland ⊕ 2011

### Broker's View

- Frequency versus severity
- Litigation very infrequent and so far unsuccessful
- Breach response expenses

***Expedition Risk!***

URMIA ⊕ Portland ⊕ 2011

### Broker's View

- However...a few actual claims to keep you up at night...
  - UH breach class action
  - Ohio State breach = \$\$\$
  - University of Connecticut vendor breach

***Expedition Risk!***

URMIA ⊕ Portland ⊕ 2011

## Broker's View

- Making it happen
- Carrier landscape and appetite
- Key underwriting information and challenges
- Scope of coverage – Setting priorities
- Budget expectations

**Expedition Risk!**

URMIA ⊕ Portland ⊕ 2011

## Carrier's Corner – Network and Privacy Insurance

- Key Elements of Coverage
  - Privacy coverage includes:
    - personal information in any format
    - breaches not restricted to a network event
    - customer and employee information
  - Policy covers wrongful acts of Insured and its service providers
  - Regulatory proceeding coverage extends to both privacy and network



**Expedition Risk!**

URMIA ⊕ Portland ⊕ 2011



### Carrier's Corner – Network and Privacy Insurance

- No retention, coinsurance, or prior written approval restrictions for identity theft response fund
- Crisis management and notification expenses are not subject to a post-discovery time restriction
- Broad form network security grant versus specified perils



**Expedition Risk!**

URMIA ⊕ Portland ⊕ 2011

### Carrier's Corner – Network and Privacy Insurance

- Definition of damages includes a consumer redress fund awarded from a regulatory proceeding and punitive and exemplary damages (most favorable jurisdiction language)
- Definition of insured includes leased employees, temporary employees, and independent contractors



**Expedition Risk!**

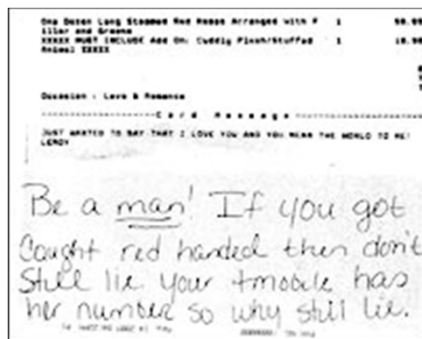
URMIA ⊕ Portland ⊕ 2011

### Carrier's Corner – Network and Privacy Insurance

- Bodily injury exclusion includes a carve back for mental injury, mental anguish, mental tension, emotional distress, pain and suffering, or shock resulting from privacy liability
- Fraud and profit exclusions are severable and triggered only if there is a final adjudication

**Expedition Risk!**  
URMIA ☉ Portland ☉ 2011

### Loss Example #1 – Privacy Breach 1-800-FLOWERS



“Just wanted to say that I love you and you mean the world to me!”

“Be a man!” it began. “If you got caught red handed then don't still lie. Your tmobile has her number so why still lie.”

**Expedition Risk!**  
URMIA ☉ Portland ☉ 2011

## Loss Example #2 – Privacy Breach Abortion Clinic

### The Issues:

- The center had no written plan
- While the opinion does not discuss the privacy and security regulations under HIPAA, it is likely that the center is covered under those regulations
- There was no written “no-cal” policy
- The nurse discussed plaintiff's medical issues with the plaintiff's mother
- Jury awarded \$300,000 in punitive damages and \$65,000 for emotional distress

### Key Takeaways:

- Absolute need for proper policies and procedures for both internal awareness and defensibility in the event of a breach
- Employee training is critical for any company handling sensitive patient or customer information

**Expedition Risk!**

URMIA ☉ Portland ☉ 2011

## Loss Example #3 – Network Security Breach

### The Issues:

- Large US technology company with best in class controls
- Overseas subsidiary contracted software vendor for work
- Software vendor left universal “admin” defaults installed on server
- Chinese “hacker-for-hire” paid only \$20,000 to exploit vulnerability
- Hackers accessed records of millions of registered users

- Hackers attempted to extort firm by posting records on a blog
- Forensic and crisis management costs expected to exceed \$2M
- Multiple class actions filed in local jurisdiction

### Key Takeaway:

- Proper review of all vendors and service providers is critical



**Expedition Risk!**

URMIA ☉ Portland ☉ 2011



A graphic with a blue background and a yellow torn-paper bottom. It lists several websites under the heading "Helpful Websites". A large "WWW." is in the top right. A barcode is on the right side. The text "Expedition Risk! URMIA Portland 2011" is at the bottom.

**Helpful Websites**

<http://www.privacyrights.org/ar/ChronDataBreaches.htm>  
<http://www.ftc.gov/privacy/>  
<http://www.fbi.gov/cyberinvest/cyberhome.htm>  
<http://www.cybercrime.gov/>  
<http://www.pogowasright.org/>  
<https://www.pcisecuritystandards.org/>  
[www.gigalaw.com/](http://www.gigalaw.com/)  
<http://www.techweb.com/>  
<http://www.aceusa.com/News/Pages/News.aspx>

**Expedition Risk!**  
URMIA Portland 2011

A graphic with a light gray background of puzzle pieces. One piece in the center is red and has a white question mark on it. The text "Questions?" is above the puzzle piece. The text "Expedition Risk! URMIA Portland 2011" is at the bottom.

**Questions?**

**Expedition Risk!**  
URMIA Portland 2011