Cyber Risk and Business Continuity

David Skica, Director IT – University of Bridgeport
Steven Helwig, Information Security Officer – SunGard Collegis

Connecticut Conference of Independent Colleges
July 14, 2005

Proprietary and Confidential
Agenda

- A Vision
- Organization: Who Owns Security?
- IT Security and Academic Values
- Higher Education Incidents
- Are you Prepared?
- Perceived Barriers
- Risk
- Business Continuity
- Who is Paying For This?
- Q & A
“We must all become much more vigilant in the provision of secure systems, in intrusion detection, in rapid response, and especially in education. We must practice, teach, and infuse all aspects of security into campus lives.”

Dr. Linwood H. Rose
President, James Madison University

“Information Security: A Difficult Balance”
EDUCAUSE Review, September/October 2004
A UNIVERSITY IS...

PEOPLE
(Students, Faculty, and Staff)

INFORMATION
Classes/ Admin. Functions

ACCESS
(Hardware/Software)
Organization

**Who Owns It? Who is the Leader / Driving Force?**
- Define the Infrastructure
  - Decentralized or Centralized
    - *People, Processes, Technology*
  - Size of the Institution
  - External Support

**Develop a Security Plan**
- Metrics and Validation
  - Make sure there is a feedback process to learn from mistakes.
- Skillset: Develop or Buy?
- Training: Technical Staff, User Community, Faculty
- Certifications
  - CISSP: 4 years plus 6 hour exam (www.isc2.org)
  - GIAC: Mastery of security areas (www.sans.org)
- Behavior Guidance: This is what a good plan will adjust.
There is a balancing process that needs to be evaluated between the desire for academic freedom and the need to secure the computer and network infrastructure of the institution.

Principles:
- **Community**: Supporting the core values of the institution.
- **Intellectual Freedom**: How secure is secure, and How open is Open?
- **Privacy and Confidentiality**: Develop practices to protect the collection and disclosure of personal information.
  - HIPPA, FERPA, GLB
- **Fairness and Process**
  - The community needs to agree on policy and in the event of abuse, do not over-react. Due process is to be observed in handling incidents.
- **Ethics and Integrity**
  - Education and communications is critical to having the community follow agreed to policies on access to resources.
Higher Ed Security Incidents

- **San Diego State University** - That hackers broke into a server in the Office of Financial Aid and Scholarships, gaining access to names and Social Security numbers for more than 178,000 former and current students, applicants and employees.

- **University of California** - Notified 2,156 applicants a few weeks ago that an overloaded server may have allowed Social Security numbers, test scores and other personal details to be shared over the Internet with competing applicants.

- **California State University at Monterey Bay** - Some 2,800 applicants were informed in February that their names, addresses and Social Security numbers were made available on the Internet by an employee who moved the data to a computer folder that was not secure. The data was accessed more than 100 times from around the world before the error was discovered.

- **Georgia Institute of Technology** - A hacker downloaded information that could have included names, addresses, phone numbers, e-mail addresses and credit card numbers for about 57,775 patrons from the campus arts center box office.

- **University of Texas at Austin** - 55,200 names and Social Security numbers were downloaded by hackers after a similar incident a few months earlier.

- **New York University** - It was discovered that several mailing lists with names, birth dates, addresses, phone numbers, e-mail addresses and some Social Security numbers for at least 2,100 students, alumni and professors were inadvertently posted on a campus Web site, according to the campus newspaper, the Washington Square News.
Higher Ed Security Incidents (cont)

- **Indiana State University** – School officials said a hacker breached a computer server containing personal information on about 35,000 current and former students and staff.

- **University of Georgia** – School officials found that hackers penetrated the school's Web site, gathering personal information including Social Security and credit card numbers of 31,000 students and applicants.

- **University of Texas** - The names and Social Security numbers of 55,000 current and former students, faculty, and staff were compromised by a hacker who was also a student at the university.

- **Central Washington University** – A philosophy professor was sentenced to six months in prison for a credit-card scam that stemmed from stealing students' Social Security numbers from campus computers.

- **Stanford University** – School officials released a security alert on stating that a number of systems running Sun Solaris and Linux operating systems on the Stanford campus were compromised. Attackers also took advantage of shared folders, which were loosely secured by the university to make it easier to manage systems and share data processing tasks between machines, the advisory said.
Are You Prepared?

Michigan legislature also recently passed the Social Security Number Privacy Act (MCL §445.81 et seq. 2005), which will become effective on January 1, 2006. This new law requires companies that obtain Social Security numbers to publish a privacy policy that:

- (1) limits who has access to the Social Security numbers;
- (2) prohibits unlawful disclosure;
- (3) establishes a document destruction protocol;

Employers in every jurisdiction should take steps to avoid liability related to sensitive employee information.

- Implement and maintain procedures for protecting sensitive information.
- Consider using ID numbers other than Social Security numbers. Substitute a different employee identification number instead.
- In the event that sensitive information is accessed by an unauthorized person, immediately disclose the security breach to the affected employee(s).
What will you do when it hits your campus?

Will you be prepared?
Perceived Barriers To IT Security

- Freedom of Speech
- Vendor Hardware/Software
- Individual Privacy
- Legal Lags Technology
- Technology
- Senior Management Support
- Enforcement of Policies
- Absence of Policies
- Culture of Decentralization
- Academic Freedom
- Awareness
- Resources

Information Technology Security Study
EDUCAUSE Center for Applied Research, Sept. 2003
What is Risk?
Risk Definition

Potential for exposure to loss.

Risks, either man-made or natural, are constant.
Determining Risk

**Should You Immediately Conduct a Risk Analysis? Why or Why Not?**
- Legal Ramifications – What are they?
- Develop a Risk Assessment Plan: How should an Institution Proceed
- Acquire Legal Assistance from a firm that has expertise in the area.

**Look at Models:**
- National Institute of Standards and Technology (NIST)
  - *Special Publications: Series 800*
- National Security Agency (NSA) Methodologies (IAM, IEM)
- National Association of College and University Business Officers (NACUBO)
  - *Developing a Strategy to Manage Enterprisewide Risk in Higher Education*
Types of Risk Evaluation

Criticality Matrix

Organizational Information vs. Impact Attributes

- Organizational Information – Information Critical to Institution: Determined by Institution.
- Impact Attributes – Confidentiality, Integrity, Availability, Accountability, etc..
  - Usually: High, Medium, Low – Definitions determined by Institution

Example:

<table>
<thead>
<tr>
<th>Organizational Information</th>
<th>Confidentiality</th>
<th>Integrity</th>
<th>Availability</th>
<th>Accountability</th>
<th>????</th>
</tr>
</thead>
<tbody>
<tr>
<td>Student Records</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>M</td>
<td>????</td>
</tr>
<tr>
<td>Staff / Faculty Payroll Records</td>
<td>H</td>
<td>H</td>
<td>M</td>
<td>H</td>
<td>????</td>
</tr>
<tr>
<td>Annual Budgets</td>
<td>H</td>
<td>H</td>
<td>M</td>
<td>M</td>
<td>????</td>
</tr>
<tr>
<td>Marketing Information</td>
<td>M</td>
<td>M</td>
<td>M</td>
<td>M</td>
<td>????</td>
</tr>
<tr>
<td>Alumni Information</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>????</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Information Criticality</th>
<th>Confidentiality</th>
<th>Integrity</th>
<th>Availability</th>
<th>Accountability</th>
<th>????</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>????</td>
</tr>
</tbody>
</table>
Risk Evaluation (con’t)

Types of Risk Evaluation (con’t)

Risk Assessment / Analysis
- Process of identifying the risks to an organization, assessing the critical functions necessary for an organization to continue business operations, defining the controls in place to reduce organization exposure and evaluating the cost for such controls. Risk analysis often involves an evaluation of the probabilities of a particular event.
- Can be Quantitive or Qualitative
  - Quantitative – Attempts to assign numeric values (i.e. monetary)
  - Qualitative – Does not assign numeric value, uses scenarios
  - These are more detailed than a Criticality Matrix
What is Business Continuity?
Disaster Definition - Industry

- A sudden, unplanned calamitous event causing great damage or loss as defined or determined by a Risk Assessment and Business Impact Analysis;
  - 1) Any event that creates an inability on an organization’s part to provide critical business functions for some predetermined period of time.
  - 2) In the business environment, any event that creates an inability on an organization’s part to provide the critical business functions for some predetermined period of time.
  - 3) The period when company management decides to divert from normal production responses and exercises its disaster recovery plan.
“ANY condition that prevents anyone from performing their critical functions in an acceptable period of time!”
Business Impact Analysis Definition

A process designed to identify critical business functions and workflow, determine the qualitative and quantitative impacts of a disruption, and to prioritize and establish recovery time objectives.
Disaster Recovery Definition

The process whereby an institution would restore any loss of data in the event of fire, vandalism, natural disaster, or system failure.
Business Continuity Definition

The ability of an institution to ensure continuity of service and support for its customers and to maintain its viability before after and during an event.
When Disaster Strikes...

You Need:

- Recovery Plan
- Compatible Equipment
- Alternate Site
- Data
- Recovery Teams
Provide Protection Through Business Recovery

- Preparation
- Documentation
- Organization
- Procedures
- Agreements
Recovery Won’t Happen Without…

- Planning
- Training
- Documentation
- Practicing
- Mock Testing
- Updating
Risk Reduction:
- Data Backups
- Off-Site Storage
- Security Audits
- Current Technology
- Policies & Procedures
- Training/Mock Testing
What’s Needed?

Business Continuity Plan (BCP)
- Brodest scope - Encompasses recovery of Critical University Functions, Information Technology, Communications, and associated Networks (Protects the business)

Disaster Recovery/Resumption Plan (DRP)
- Specific emphasis on recovery of Information Technology (Does not insure business can operate)
1. **Awareness:** Like safety and security, organizations must begin to think about recovery issues before they happen so they can be properly identified and addressed.

2. **Analysis/Education (BIA/BFA):** Identification and prioritization of business functions and information technology applications. Once identified, cost efficient recovery solutions can be developed. This process in itself is invaluable awareness training.

3. **Plan Development:** Upon addressing the issues & strategies, a workable plan can be developed. Training occurs throughout the Plan Development process.

4. **Plan Maintenance:** Continuous Improvement should be the goal of every Recovery Plan. The organization must continue to learn what the changing issues are and how they can be resolved.
Business Resumption Cycle

1. Increase Awareness

2. Provide Analysis (BIA/BFA) & Education

3. Develop Plan & Provide Training

4. Provide Plan Testing & Maintenance

DRP/BCP a Living Document
So! Who Pays for This?
Prioritizing Impact

-Priority 1- Critical*
0-48 hours...Major Financial Impact/Substantial impact on CORE Services

-Priority 2- Significant*
3-7 Days...Some Financial Impact/Substantial impact on CORE Services

-Priority 3- Important*
8-30 Days...Minimal Financial Impact/Long Range Support Functions

*Defined in Client Terms for a Particular Institution
Costs - versus - Recovery Time

- **DUPPLICATION**
- **TIME**
- **REBUILD**

- *Spend a lot, duplicate all systems… lowest risk/highest initial cost!*
- *Spend a little, don’t duplicate systems… highest risk/lowest initial cost!*
Balance Recovery Capability And Cost

- **Needless Cost**: Too Much Protection
- **High Recovery Cost**: Too Little Protection
- **Reasonable Cost**: Adequate Protection

Balance Recovery Capability And Cost
“No one plans to fail...!!!”

“They simply fail to plan.”
Is Your Institution Protected?
Thanks for Attending!
References

- NIST – www.nist.gov
- Disaster Recovery Journal – www.drj.com
- NSA – www.iatrp.com
- SunGard – www.availability.sungard.com
- SunGard Collegis – www.collegis.com
- Contingency Planning World - www.business-continuity-world.com
- International Standards Organization (ISO) – www.iso.org
- NACUBO - www.nacubo.org