Welcome

IT Exchange

January 15, 2015
Announcements
Security Framework

Thomas Porter
Information Technology Security Framework and Standard

January 15, 2015
Students alerted after data breach at San
Indiana University reports potential data exposure

Feb. 25, 2014
FOR IMMEDIATE RELEASE

BLOOMINGTON, Ind. -- Indiana University notified the Indiana attorney general's office today of the potential exposure of personal data for some students and recent graduates.

The data potential approxi from 20

Marcos Colón, Online Editor

Back to

May 20, 2014

Maricopa County data breach costs reaching the $20 million mark

By Patrick Syrek and Nick Anderson, Published: February 19

North Dakota University System hacked, roughly 300K impacted

By Vanessa Miller, The Gazette
Published: April 22 2014 | 12:21

The North Dakota University System (NDUS) is notifying more than 290,000 former and current students and roughly 780 faculty and staff that their personal information – including Social Security numbers – may be at risk after an unauthorized party gained access to one of its servers.
Just take care of it...

Security is an on-going risk management process

• It must be maintained

Who manages the RISK?

• Partnership between Management and IT
• Part of a Information Security Program
Vision Statement

Vision

- Diminish IT security risks to an acceptable level and become the most effective IT function; enable the University to make informed decisions based on risk.
Mission Statement

Mission

• **Design, implement and maintain** an information security program that protects the University’s resources against unauthorized use, modification and loss. Establish a **practical** information security program that enables MSU to be the best public research University in the world.
IT Services Action Plan

“...a multi-year journey that will stabilize and strengthen information technology...”

-Joanna C. Young, CIO
Characteristics of an Information Security Program

1. Always be aware of our “state of security”
2. Iteratively review existing Policies and Standards
3. Develop ANNUAL strategic security plans
4. Security Awareness Program
5. Integrate into Culture of the institution
IT Security Standard

• A list of security controls
  – Rules to meet future Policy goal.
  – Not based upon a specific technology.

• Tool to evaluate and improve our state of security.
  Gap analysis.
  Risk management.
  Remediation planning tool.

Project charter two-year implementation plan.
Risk Management Framework

Annual Security Life Cycle

- Categorize Information System
- Select Security Controls
- Implement Security Controls
- Assess Security Controls
- Authorize Information System
- Monitor Security State
IT Security Standard Risk-based Controls

130 controls, addressing 8 risk areas:

1. Business Risk
2. Facilities Risk
3. Human Resources Risk
4. Institutional Data Risk
5. Legal Risk
6. Management Risk
7. Purchasing Risk
8. Information Technology Risk
# Standard control example

## INFORMATION TECHNOLOGY RISK

<table>
<thead>
<tr>
<th>IT1</th>
<th>Disaster-related risk</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>To limit the negative impact of a disruptive event upon IT operations and to ensure the timely access to information assets.</td>
</tr>
</tbody>
</table>
|       | IT1.1: Backups must be made of all information systems periodically.  
NIST SP 800-53 CP-9 |
|       | IT1.2: A disaster recovery plan must be developed and maintained.  
NIST SP 800-53 CP-10 |
<table>
<thead>
<tr>
<th>Risk</th>
<th>Control</th>
<th>Example</th>
<th>Reference</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT1.1</td>
<td>Backups must be made of all information systems periodically.</td>
<td>RAID-6; Tape Backup; SAN; Backpack drive.</td>
<td>NIST 800-53 CP-9</td>
<td>P1</td>
</tr>
<tr>
<td>IT1.2</td>
<td>A business continuity plan must be developed and maintained.</td>
<td>Dust off Y2K plan; Coordinate with all stakeholders in advance of implementing plan.</td>
<td>NIST 800-53 CP-10</td>
<td>P1</td>
</tr>
</tbody>
</table>
Why are we doing this?

XKCD webcomic
Where do we start?

IT security Standards -> SecureIT web site
   - URL will be provided to IT Exchange list.
   - Best Practices, Checklists coming soon.

Implementation strategies (generalized):
1. Inventory (and document) your systems.
2. Review internal policies & procedures.
3. Vulnerability Assessment.
4. Malware defense.
5. Review Access Controls, and limit Admin account use.
Questions?

Thank you!