Bagels & Schmear

Planning and Statutory Compliance for Homeland Security Research Initiatives

Bradley R. Barnes (bradley.r.barnes@okstate.edu)
Sallie Fulsom Wright (sallie.wright@okstate.edu)

Educause Security Professionals Conference        April 11, 2006           Denver, Colorado
Institutional Profile

• Land Grant institution
• Stillwater, Oklahoma
• 30,500 System-wide students
• Comprehensive university system
  – Research
  – Undergraduate, Graduate and Professional Schools
  – Geographically dispersed campuses
• Center of Academic Excellence for Information Assurance Education
• **Bradley R. Barnes**
  – Technology Resources Manager for the Center for Veterinary Health Sciences. 20+ years at OSU. Specialty areas include hospital and accounting information systems. Strong separation from central campus IT infrastructure as a result of early adoption of networking and pc technologies as well as business process issues.

• **Sallie Fulsom Wright**
  – Information Security Officer for the Oklahoma State University System. 25+ years of IT management experience in arenas including higher education, manufacturing, consumer products, mining, petroleum, and retailing. Centralized collaborative approach to implementation of technologies and compliance.
Presentation Objectives

• Learn what Select Agents are
• Learn about the scope of Select Agent cybersecurity
• Develop and maintain successful partnerships
• Accelerate development of policies and procedures.
• Determine business requirements
• Conduct risk assessments
• Develop a security plan
• Develop a business continuity plan
• Exercise the plans
History
- **Statutory Compliance**: Those ridiculous policies, convoluted procedures, onerous processes and mountains of paperwork necessary to fulfill legal requirements of local, state or Federal regulations.

- **Select Agents**: The Centers for Disease Control and Prevention (CDC) regulates the possession, use, and transfer of select agents and toxins that have the potential to pose a severe threat to public health and safety. Examples of select agents are anthrax, ricin and botulism.

- **Cybersecurity**: involves the protection of information that is access and transmitted via the internet or more generally through any computer network. This term is frequently used in the context of Federal statutory compliance and was not very well defined at the time we began this process but has since become more generally used.
Criminal Penalties

- Imprisonment for up to 5 years, a fine, or both for:
  - transfer of a select agent to an unregistered person
  - possession of a select agent by an unregistered person
  - knowingly making a false statement
Civil Monetary Penalties

- up to $250,000 for an individual for each violation
- Up to $500,000 for an organization for each violation
- 10 violations could mean $5,000,000 in penalties
Strict Liability

- honest mistakes do not matter
- any violation is subject to a penalty
- few defenses exist (excuse or defense)
- entities are responsible for employee actions

Goldberg, J. (2005). Legal Aspects of the Select Agent Program
Presented at 2005 ABSA Conference.
Select Agent Final Rule

- Regulates the possession, use, & transfer of select agents & toxins

- Restricts access to agents & toxins
  - people deemed to have access must be DOJ approved
  - people who have a legitimate need to handle or use

- Requires withholding of public disclosure of information regarding select agents & toxins
  - security measures
  - location of agents
• Records have “controlled access”
  
  – Any records or IT systems that could allow a person to gain access must be safeguarded to prevent unauthorized access, theft, loss, or release of select agents or toxins.

  – You must immediately notify the RO/ARO of the theft, loss, or release of any select agent or toxin, as it must be reported by the RO to the CDC.
Select Agent Final Rule

- Requirements -

- Entity Security Plan
  - physical security of building & all labs
  - emergency response plans, bldg & labs
  - data & computer network security

- Personnel Security Policies
  - DOJ/FBI background checks
  - photo ID badges
  - annual training
Select Agent Final Rule

- Requirements -

- Security, Biosafety, & Incident Response Plans:
  - must be reviewed annually
  - must be revised as necessary

- Drills/Exercises:
  - must be conducted at least annually
  - object is to test & evaluate effectiveness
Why IT?

- Door Control Systems
- Building Control Systems
- Inventory Systems
- Email Systems
- Secured Data Storage
- Laboratory Instrumentation
- Workstation Security
Risk

- Life safety
- Criminal/Civil Penalties
- Public image of institution
- $40+ Million in sponsored research
- $10+ Million in facilities
Timeline

- First Contact - June 2003
- Delivery - No later than October 29, 2003 at 9:15 a.m.
Communications

- Research Compliance
- IT
- CVHS Technology Resources
<table>
<thead>
<tr>
<th></th>
<th>IT</th>
<th>CVHS</th>
</tr>
</thead>
<tbody>
<tr>
<td>People</td>
<td>Available, Knowledgeable resources</td>
<td>Limited availability, knowledgeable, torn between two lovers feeling like a fool</td>
</tr>
<tr>
<td>Deliverables</td>
<td>Suspected it would be ugly</td>
<td>Knew it was going to be ugly</td>
</tr>
<tr>
<td>Time to Deliver</td>
<td>Faster than a speeding bullet</td>
<td>Breathtakingly short</td>
</tr>
<tr>
<td>Compliance</td>
<td>Clueless</td>
<td>Didn’t know sic’im from come here.</td>
</tr>
<tr>
<td></td>
<td>IT</td>
<td>CVHS</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------</td>
<td>-----------------------------------------------------</td>
</tr>
<tr>
<td>Compliance</td>
<td>Not have to visit Brad in jail</td>
<td>Keep the get out of jail free card</td>
</tr>
<tr>
<td>Time to Deliver</td>
<td>Ahead of schedule</td>
<td>Just in time</td>
</tr>
<tr>
<td>Deliverables</td>
<td>Complete</td>
<td>Extra-ordinarily well done</td>
</tr>
<tr>
<td>People</td>
<td>We survived</td>
<td>No one died</td>
</tr>
</tbody>
</table>
Background Research

- Scope of cybersecurity was not well defined
- Reference documents were/are classified
- Consult with subject matter experts
- Consult with compliance officials
- Review Statutory Guidance
Background Research

- Contact external entities
- Consult with physical plant experts
- Consult with physical security
- Reviewed other Federal cybersecurity plans
Define “Final” Deliverables

- Risk Assessment
- Business Impact Analysis
- Business Continuity Planning
- Disaster Recovery Planning
- Enterprise IT Security Plan
- Unit IT Security Plan
- Laboratory IT Security Plan
Project Team

• Executive Sponsors
• Business Continuity Planner
• Technical Writer
• Area Subject Matter Expert
• Security Professional
• Administrative Support
Overall Methodology

PDCA Cycle
Plan

- Evolving List of “Final Deliverables”
- Firm Drop Dead Date
- Small Focused Project Team
- Methodology & Best Practices Review/Selection
- Develop the project plan
  - Work backward from Drop Dead Date
  - Identify/incorporate Additional Deliverables
  - Be Flexible
Methodologies & Best Practices

• Risk Assessment & Business Impact Analysis
  – Octave

• Business Continuity Planning/Disaster Recovery
  – DRII
  – ISO17799 Toolkit
  – NIST
Methodologies & Best Practices

- Security Plan
  - ISO17799
  - NIST
  - COBIT
  - ITIL
Methodologies & Best Practices

• Policies and Procedures
  – SANS
  – Educause
  – ISO17799
  – COBIT
  – ITIL
  – NIST
• Project Planning
  – Develop the plan
  – Clear and Mark Project Team Calendars
• Definitive Milestones
• Risk Assessment
  – Threats and Exposure
  – Risk Identification
  – Mitigation
• Business Impact Analysis
• Identify Critical Resources
  – Tour of Facilities
  – Document by Building
    • Software
    • Hardware
    • Processes/Procedures
    • Building Controls
• Prioritize Critical Resources
• Business Continuity Plan
  – Call Trees/Notification
  – Emergency Response
    • Role of IT
    • Role of Physical Plant
    • Role of Principle Investigator
    • Role of Administration
    • Role of Research Compliance
    • Role of Law Enforcement/Fire Protection
• Disaster Recovery
  – What to do when a catastrophic problem occurs
• Policies and Procedures
  – New and modified
• Enterprise IT Security Plan
• Unit Level IT Security Plan
Cybersecurity Plan
Table of Contents

- Revisions and Additions Made
- Select Agent Program Review
- Oklahoma State University Information System Security Plan
- Center for Veterinary Health Sciences Information System Security Plan
- Center for Veterinary Health Sciences Policies and Procedures
- Center for Veterinary Health Sciences Project Plan
Cybersecurity Plan

Table of Contents - Continued

- Technology Resources Contingency Plan
- Senior Information Technology Management Survey and Analysis
- Risk Assessment Training
- Asset Identification Training
- Asset Assessment Training
• Asset Security Requirements Training
• Prioritize Assets/Identify Existing Asset Controls Training
• Risk Assessments Data
• Impact Probability Matrix and Asset Strategy Worksheets
• CVHS Critical Assets Summary, Worksheets and Security Requirements
• CVHS BSL Physical Access Control System (Doors/Surveillance)
• CVHS BSL Environmental Control System (HVAC)
• Business Continuity Planning Exercise
• Oklahoma Information Security Policy, Procedures and Guidelines
• Security Committee Report
• Oklahoma State University Information Technology Staffing Assessment
• Audit Deliverables
• CDC Site Visit Review
• Continuous Quality Improvement
• Monitor Regulatory Changes
• Monitor Operational Changes
• Response to Issues
• Response to Incidents
• Response to Regulatory Changes
• Response to Operational Changes
• Change Management Process
  – Discover
  – Document
  – Resolve
  – Approve
  – Communicate
  – Track
Current State

- We made it and now we are hanging on
- Re-licensing this year
Take Home Lessons

• Buy In
• Communication
• Inclusion of all affected parties
• Coordination
• Resources Required
• Who pays for what
• Share/Secured Document Repositories
• Security Clearance over and under reactions
  – I want one too syndrome
  – Over my dead body syndrome
Take Home Lessons

• Constant awareness of changing research environment by IT professionals

• Business continuity, disaster recovery, and incident response plans must be exercised in a structured manner; otherwise they will be exercised the hard way (Fire trucks, ambulances and FBI.)

• Continuous Process Improvement with Feedback
CD Contents

- Statutes
- Select Agents List
- PowerPoint Slides
- Cybersecurity Plan Table of Contents
- Methodology Forms
- Sample Security Plan
- Sample Business Continuity Plan
- List of Resources and Links
Outcomes

- Learn what Select Agents are
- Learn about the scope of Select Agent cybersecurity
- Develop and maintain successful partnerships
- Accelerate development of policies and procedures.
- Determine business requirements
- Conduct risk assessments
- Develop a security plan
- Develop a business continuity plan
- Exercise the plans
Questions