Case Study: SSCC's Silo Service for Restricted Data and the Risk Management Framework

Andrew Arnold
Ryan Horrisberger
www.ssc.wisc.edu
Social Science Computing Cooperative (SSCC)

- Computing cooperative created by and for researchers; 30+ years in existence
- About 1,200 members and 1,600 instructional users
- Member Agencies:
  - Center for Demography and Ecology
  - Center for Demography of Health and Aging
  - Center on Wisconsin Strategy
  - Economics Department
  - Institute for Research on Poverty
  - School of Human Ecology
  - Sociology Department
  - UW Survey Center
Social Science Computing Cooperative (SSCC)

Providing a complete research computing environment focused on statistics plus the expert help you need to use it.

- Statistical Consultants
- Training on Statistical Software
- Powerful Windows and Linux Servers
- Secure Data Storage
- Help Desk
What is Silo?

- Isolated network environment for storing and analyzing HIPAA protected and other restricted research data
- Extension of existing research computing services
- Scalable (not standalone workstation setups)
Risk Management Framework

1. Initiate
2. Design
3. Implement
4. Operate & Maintain
Why was Silo built?

- High profile attacks are more prolific
- Federal and State agencies requiring stricter security controls
- We really didn’t know what types of data all our supported researchers are working with
- We wanted to comply with various UW IT policies:
  - Data Classification Policy
  - Restricted Data Security Management Policy
  - Restricted Data Security Management Procedures
- Reduce administrative burden on researchers by streamlining the IRB/RSP approval process
- No central/shared service was available on campus
Risk Management Framework

1. Initiate
2. Design
3. Implement
4. Operate & Maintain
3 MAJOR SURPRISES
timeline
Kickoff
April 2015
Meetings
April 2015
Meetings
April 2016
Not Really
Risk Management Framework

Operate it Securely

Categorize the Information System
Monitor and Mitigate (CDM)
Operate & Maintain
Initiate
Select Security Controls
Design
Implement Security Controls
Implement
Assess Security Controls
Authorize System at Defined Risk Level
Build it Right
process
Security and Privacy Controls for Federal Information Systems and Organizations

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

April 2013
INCLUDES UPDATES AS OF 01-22-2015

U.S. Department of Commerce
Rebecca M. Blank, Acting Secretary
National Institute of Standards and Technology
Patrick D. Gallagher, Under Secretary of Commerce for Standards and Technology and Director
<table>
<thead>
<tr>
<th>Tag#</th>
<th>Group Name</th>
<th>Regulation References</th>
<th>NIST Control Map</th>
<th>Interview Question / Checks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.0</td>
<td>Access Program</td>
<td>§164.308(a)(4) §164.308(a)(4)(ii)(B) §164.312(a)(1) §164.310(a)(2)(ii) §164.308(a)(4)(ii)(c) §164.308(a)(3)</td>
<td>AC-1, PE-1</td>
<td>Does your practice have policies and procedures for controlling access to ePHI data, systems, and networking devices?</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>NOTE: If the covered entity has chosen not to fully implement this specification, the entity must have documentation on where they have chosen not to fully implement this specification and their rationale for doing so.</td>
</tr>
<tr>
<td>1.2.0</td>
<td>Access Program</td>
<td>§164.308(a)(3)(i)</td>
<td>AC-1, AC-5, AC-6, IA-1</td>
<td>Does your practice have procedures that make sure those who need access to ePHI have access and those who do not are denied such access?</td>
</tr>
<tr>
<td>1.3.0</td>
<td>Access Program</td>
<td>§164.312(a)(1) §164.310(a)(2)</td>
<td>AC-1, AC-3, AC-5, AC-6, IA-2, IA-3, IA-4, IA-5</td>
<td>Does your practice have procedures for establishing the security settings for each of its information systems and electronic devices that control access?</td>
</tr>
<tr>
<td>1.4.0</td>
<td>Access Program</td>
<td>§164.308(a)(3)(ii)(A) §164.310(a)(2)(6)</td>
<td>AC-1, AC-3, AC-4, MA-4, MA-5, MP-2, PS-1, PS-6, PS-7</td>
<td>Does your practice implement procedures for authorizing users and changing authorization (To any computer system, not necessarily ePHI systems)</td>
</tr>
<tr>
<td>1.5.0</td>
<td>Access Program</td>
<td>§164.308(a)(4)(ii)(B) §164.308(a)(4)(ii)(c) §164.308(a)(4)(ii)(f)</td>
<td>AC-1, AC-3, AC-3, AC-5, AC-6, AC-4, PS-4, PS-6, PS-7</td>
<td>Does your practice have procedures that explain how it grants access or limits access to ePHI to third party business associates (business associates)?</td>
</tr>
<tr>
<td>1.6.0</td>
<td>Access Program</td>
<td></td>
<td></td>
<td>Does your practice have technical controls to limit the number of invalid login attempts and lock the account when exceeded?</td>
</tr>
<tr>
<td>1.7.0</td>
<td>Access Program</td>
<td>§164.312(d)</td>
<td>AC-2, AC-3, IA-2, IA-3, IA-4</td>
<td>Does your practice use a standard banner for users to accept before logon to a system?</td>
</tr>
<tr>
<td>1.8.0</td>
<td>Access Program</td>
<td></td>
<td></td>
<td>Does your practice have procedures for the assignment of a unique identifier for each authorized user?</td>
</tr>
<tr>
<td>1.9.0</td>
<td>Access Program</td>
<td>§164.308(a)(3)(ii)(A)</td>
<td>AC-1, AC-3, AC-4, MA-5, MP-2, PS-1, PS-6, PS-7</td>
<td>Do your practice’s procedures for access authorization address the needs of those who are not members of its workforce?</td>
</tr>
<tr>
<td>1.10.0</td>
<td>Access Program</td>
<td>§164.312(c)(1)</td>
<td>CP-9, MP-2, MP-3, SC-8, SI-1, SI-7</td>
<td>Have all users who should have access to ePHI been identified?</td>
</tr>
<tr>
<td>1.11.0</td>
<td>Access Program</td>
<td>§164.312(a)(1)</td>
<td>AC-1, AC-3, AC-5, AC-6</td>
<td>Have all generic user or system IDs accounts been eliminated from the environment and prohibited from being re-created?</td>
</tr>
</tbody>
</table>
likelihood x impact = risk level
office of cybersecurity
We love the GRC team.
Risk Management Framework

1. Initiate
2. Design
3. Implement
4. Operate & Maintain
Architecture
Silo Network (LDS Area)

- Future Linux Farm
- Windows Farm
- Linux File Server
- Citrix Data Collector
- Linux Server
- Windows Server
- PHI Area
and everyone was happy
except for a few small problems...
We are thrilled with the results.
Thrilled with result.

Thanks.
Andrew Arnold
Ryan Horrisberger

www.ssc.wisc.edu