Security Beyond PCI Compliance

How to Protect Your Students’ Data

June 6, 2017

Jen Stone
Richard Chapman

About Us

• Jen Stone
  • MSCIS, CISSP, QSA
  • Security Analyst, SecurityMetrics

• Richard Chapman
  • Chief Privacy Officer
  • University of Kentucky HealthCare
Introduction

• Today we will cover:
  • Security beyond PCI compliance, using a Crosswalk Data Security approach
  • Why this is a hot topic for higher education
  • How Crosswalk can help, and potential limitations
  • How to start your own Crosswalk map

Crosswalk Data Security

What is Crosswalk Data Security?
**Security Taxonomy**

- Business Strategy
- IT Strategy
- Enterprise Architecture
- Solution Architecture

**Security Architecture (patterns)**

- Business Process
- Risk
- Threats
- Vulnerabilities

- Impact
- Remediate
- Affect
- Exposed to

- IT System and Data Assets
- Controls
- Standards and guidance

- Policies (Principles and Objectives)
- Laws and regulations

OSA is licensed according to Creative Commons Share-alike.
Please see http://www.opensecurityarchitecture.org/cms/about/license-terms.

---

**Crosswalk Means Mapping**

- Policies
- Procedures
- Security Controls

- Standards
- Laws
- Regulations

June 4-7, 2017

SCCE Higher Education Compliance Conference
Why Do We Need It?
Helping Colleges and Universities Navigate Standards and Regulations

Complex Systems

- Operate some of the largest, most powerful computer systems in the world
- Interdependencies with government and private sector
- Multiple paths for cardholder data to enter systems across multiple departments
A Myriad of Rules

- HIPAA
- FISMA
- FERPA
- PCI DSS
- NIST 800
- GBLA
- Other state and federal regulations
- PLUS International

Tough Questions

- How can I address requirements for policies, procedures and security controls across multiple, complex standards and regulations?
One Approach Doesn’t Fit All
Tackling Higher Education Complexities

June 4-7, 2017
SCCE Higher Education Compliance Conference

Diverse Institutions

Composition
• Size
• Funding sources
• Activities in which the schools engage
• Applicable regulations

Culture
• Autonomy
• Freedom
• Collaboration and sharing
• Decentralized administration
• Distributed decision-making

June 4-7, 2017
SCCE Higher Education Compliance Conference
Result?

- Cultural factors and limited resources make it a challenge to institute cybersecurity practices in higher education
HIPAA X NIST CSF

• Maps HIPAA administrative, physical and technical safeguard standards to NIST Cybersecurity Framework Subcategory

[Image: NIST and HIPAA logos]

June 4-7, 2017

SCCE Higher Education Compliance Conference

HIPAA X NIST CSF

<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Relevant Control Mappings</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID:AM-1: Physical devices and systems within the organization are inventoried</td>
<td>• COI: CIC 1</td>
<td></td>
<td>• COI: CIC 1&lt;br&gt;• COBRA 5.9: 36, BM39.02&lt;br&gt;• ISA: 52400.3-1:2009 4.1.5.4&lt;br&gt;• ISA: 52400.3-2:2013 5R 7.8&lt;br&gt;• ISO: 27000, 2010, 16.4.1&lt;br&gt;• NIST: SP 800-53 Rev. 4 CM-1&lt;br&gt;• HIPAA Security Rule 4.1.9 66&lt;br&gt;144-300(a)(1)(ii)(A), 144.310(a)(2)(ii)(A), 144.310(b)(1)</td>
</tr>
<tr>
<td>Asset Management (ID:AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization’s risk strategy.</td>
<td>• COI: CIC 1</td>
<td></td>
<td>• COI: CIC 1&lt;br&gt;• COBRA 5.9: 36, BM39.02, BMX9.05&lt;br&gt;• ISA: 52400.3-1:2009 4.1.5.4&lt;br&gt;• ISA: 52400.3-2:2013 5R 7.8&lt;br&gt;• ISO: 27000, 2010, 16.4.1&lt;br&gt;• NIST: SP 800-53 Rev. 4 CM-1&lt;br&gt;• HIPAA Security Rule 4.1.9 66&lt;br&gt;144-300(a)(1)(ii)(A), 144.310(a)(2)(ii)(A), 144.310(b)(1)</td>
</tr>
<tr>
<td>ID:AM-3: Organizational communication and data flows are mapped</td>
<td>• COI: CIC 1</td>
<td></td>
<td>• COI: CIC 1&lt;br&gt;• COBRA 5.9: 36, BM39.02, BMX9.05&lt;br&gt;• ISA: 52400.3-1:2009 4.1.5.4&lt;br&gt;• ISA: 52400.3-2:2013 5R 7.8&lt;br&gt;• ISO: 27000, 2010, 16.4.1&lt;br&gt;• NIST: SP 800-53 Rev. 4 CM-1&lt;br&gt;• HIPAA Security Rule 4.1.9 66&lt;br&gt;144-300(a)(1)(ii)(A), 144.310(a)(2)(ii)(A), 144.310(b)(1)</td>
</tr>
</tbody>
</table>

Benefits and Limitations

What can and can’t the Crosswalk do for me?
How Does This Help?

• Crosswalk Serves Two Purposes
  1. Offers insight within your organization
     • Planning
     • Implementing
     • Communicating
     • Leveraging across different groups
  2. Prepares you to demonstrate compliance to third parties

Make Metadata Accessible

• Regulations
• Standards
• Requirements
• Policies
• Procedures
• Security controls
• Evidence
• Timing
• Responsibility
Crosswalk Caution

- HIPAA X CSF
- OCR cautions us:
  - Mappings are intended to be an informative reference and do not imply or guarantee compliance with any laws or regulations
  - Users who have aligned their security program to the NIST CSF should not assume they are in full compliance with HIPAA

Mapping is High Level

- Great for:
  - Tracking
  - Communication
  - Planning
  - Organizing information for an assessment
- Not so great for:
  - Implementing security controls
  - Monitoring day-to-day security activities
  - Satisfying an assessment
Mapping Isn’t Evidence

- Typically, an assessor will examine your environment in the following ways:
  - Review policy and procedure documentation
  - Interview people to make sure real-world activities align with theory
  - Observe your systems first-hand to verify that they are configured the way documentation states
  - Request retainable evidence of what was seen

Mapping Helps You Provide Evidence

- Know which policies satisfy requested evidence
- Know which systems contain which information
- Know which people are responsible for which documents and security controls, and so can help provide detailed evidence
Create Your Own Map
How do I get started?

Start with People
• High-level support
• Clear responsibility in key places
• Team to bring it all together
Focus on the Information

• What am I protecting?
  • How many “buckets” of information?
  • Where does it live in my systems?
• What rules apply to that information?

Understand Your Audience

• What audience(s) will be served by mapping this information?
• What will they use the information for?
• How does this affect what we map?
Gather Key Information

- Regulations
- Standards
- Requirements
- Policies
- Procedures

- Security controls
- Evidence
- Timing
- Responsibility

Start EARLY

- Mapping takes time
- It’s hard
  - Cross-departmental
  - Cross-functional
  - Cross-regulatory
- It’s specific to you – you understand your organization and you need to drive it
Questions?