Tools for Compliance

Financial Officers and Technology Professionals Conference

November 12, 2015
Background: Me

- Patrick Gardella
  - Chief Technology Officer, Asbury Theological Seminary

- “New” to Higher Ed
  - 4 years

- Corporate world previously
  - IT Consulting
  - Infrastructure
  - Software Development
Background: Asbury

- Asbury Theological Seminary
  - Founded 1923
  - 1,529 Students

- “Locations”:
  - Wilmore, KY
  - Orlando, FL
  - Memphis, TN
  - Online/ExL
    - Authorized/Allowed/Exempt in 46 states* and District of Columbia
Background: Compliance

- My start:
  - Educause Security Professionals Conference (May 2012)
  - Indiana University presentation:
    - “Must comply with 360–something federal, state, local, and international laws and regulations.”
    - *Um, What did you say?*
Um, What?

As
Assets

Of
Org. Functions

COPPA

Ct
Citations

DISA

Rs
Research Sites

16 CFR Part 313

Re
Rec. Examples

Rc
Record Category

Au
Audit

Ad
Authority Docs

HIPPA

Cd
cDocs

FERPA

Ro
Roles

Sarbanes Oxley

Me
Metrics

Ot
Org. Tasks

NIST
Terminology

- Governance, Risk and Compliance (GRC) Management
- Authority Documents
- Controls
Asbury: To Date

- 40 Federal Laws + ??? State, Local, and International Laws
- 83 Authority Documents with Controls
- 913 Mandated Controls
- 128 Implied Controls
- 7294 Implementation Controls
Tools for Compliance

Tools today:
- NACUA—the National Association of College and University Attorneys
- Unified Compliance Framework®
- Security Onion
- Chef
- Tenable Nessus

Others?
National Association of College and University Attorneys

- Higher Education Compliance Alliance
  - http://www.higheredcompliance.org/
<table>
<thead>
<tr>
<th>Information Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Communications Assistance for Law Enforcement Act (CALEA)</strong></td>
</tr>
<tr>
<td>47 U.S.C. § 1001-1010</td>
</tr>
<tr>
<td>- CALEA requires a “telecommunications carrier,” as defined by the Act, to ensure that equipment, facilities, or services that allow a customer or subscriber to “originate, terminate, or direct communications,” enable law enforcement officials to conduct electronic surveillance pursuant to court order or other lawful authorization.</td>
</tr>
<tr>
<td><strong>Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003 (CAN-SPAM Act)</strong></td>
</tr>
<tr>
<td>16 C.F.R. § 316</td>
</tr>
<tr>
<td>- Prohibits the inclusion of deceptive or misleading information and subject headings, requires identifying information such as a return address in email messages, and prohibits sending emails to a recipient after an explicit response that the recipient does not want to continue receiving messages.</td>
</tr>
<tr>
<td>- In addition to bulk email, the law covers all commercial messages, which it defines as “any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service.”</td>
</tr>
<tr>
<td>- Each separate email in violation of the CAN-SPAM Act is subject to penalties of up to $16,000.</td>
</tr>
<tr>
<td><strong>Reporting Requirements &amp; Deadlines</strong></td>
</tr>
<tr>
<td><strong>Resources</strong></td>
</tr>
</tbody>
</table>
Unified Compliance Framework®

- Commercial Product
  - https://www.unifiedcompliance.com/
- Partnering with:
  - Content Providers – NIST, PCI-DSS, SANS Institute, ISO, etc.
  - Developers – Cisco, Microsoft, McAfee, NetIQ, RSA, etc.
  - Consultants – Accenture, IBM, SDG, etc.
- Goal: Streamline compliance by simplifying and unifying requirements.
Select applicable Authority Documents – What do we need to do?
  ◦ List Controls with links to Authority Documents
Generate Builds – Generate Excel file
Compare Lists – What changed?
Track – How are we doing?
### Authority Documents

#### Our Authority List

<table>
<thead>
<tr>
<th>Control Name</th>
<th>ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leadership and high level objectives</td>
<td>00597</td>
</tr>
<tr>
<td>Audits and risk management</td>
<td>00677</td>
</tr>
<tr>
<td>Monitoring and measurement</td>
<td>00636</td>
</tr>
<tr>
<td>Technical security</td>
<td>00508</td>
</tr>
<tr>
<td>Physical and environmental protection</td>
<td>00709</td>
</tr>
<tr>
<td>Systems continuity</td>
<td>00731</td>
</tr>
<tr>
<td>Human Resources management</td>
<td>00763</td>
</tr>
</tbody>
</table>

Common Controls: 913 Mandated, 131 Implied, 7293 Implementation
Controls

- What do you need to do?

- Establish and maintain information flow control policies inside the system.
- Control all methods of remote access and teleworking.
- Manage the use of encryption controls and cryptographic controls.
- Establish and maintain a malicious code protection program.
- Establish and maintain an application security policy.
- Establish and maintain a virtual environment and shared resources security policy.
- Physical and environmental protection

  - Systems continuity

    - Establish and maintain a system continuity framework.
    - Establish and maintain a system continuity plan philosophy.
    - Define the executive vision of the continuity planning process.
    - Establish and maintain system continuity roles and responsibilities.
    - Coordinate continuity planning with other business units responsible for related operations.
    - Include continuity wrap-up procedures and continuity normalization procedures.
Establish and maintain a system continuity framework.

<table>
<thead>
<tr>
<th>CONTROL ID</th>
<th>CONTROL TYPE</th>
<th>CLASSIFICATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>00732</td>
<td>Establish/Maintain Documentation</td>
<td>Preventive</td>
</tr>
</tbody>
</table>

**SUPPORTING AND SUPPORTED CONTROLS**

This Control directly supports the mandated Control:
- Systems continuity CC ID: 00731

This Control is supported by the following Control(s):
- Establish and maintain a system continuity plan philosophy. CC ID: 00734
- Define the executive vision of the continuity planning process. CC ID: 01243
- Establish and maintain system continuity roles and responsibilities. CC ID: 00733
- Coordinate continuity planning with other business units responsible for related continuity plans. CC ID: 01386
- Include continuity wrap-up procedures and continuity normalization procedures during continuity planning. CC ID: 00761
Finance Controls

Establish and maintain an information classification scheme.

<table>
<thead>
<tr>
<th>CONTROL ID</th>
<th>CONTROL TYPE</th>
<th>CLASSIFICATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>00601</td>
<td>Establish/Maintain Documentation</td>
<td>Preventive</td>
</tr>
</tbody>
</table>

SUPPORTING AND SUPPORTED CONTROLS

This Control directly supports the implied Control:
- Analyze organizational objectives, functions, and activities. CC ID: 00598

This Control is supported by the following Control(s):
- Update the information classification scheme regularly or when new threats are discovered. CC ID: 07048

SELECTED AUTHORITY DOCUMENTS COMPLIED WITH

- The organization should have an information classification policy and an information classification process. *(Table Ref 1.2.3, Generally Accepted Privacy Principles (GAPP), CPA and CA Practitioner Version, August 2009)*
The “Unified” part

- One control may cover several authority documents.

- Are security policies and operational procedures for protecting systems against malware documented, in use, and known to all affected parties? (PCI DSS Question 5.4, PCI DSS Self-Assessment Questionnaire D and Attestation of Compliance for Merchants, Version 3.0)

- The organization should implement controls to prevent viruses, malicious code, and unauthorized software on the systems. (Table Ref 8.2.2.j, Generally Accepted Privacy Principles (GAPP), CPA and CA Practitioner Version, August 2009)

- The system must be protected against malicious code attacks by implementing mechanisms (that can be automatically updated) to check for malicious code. (§ 5.6.16, Exhibit 4 SI-3, IRS Publication 1075: TAX INFORMATION SECURITY GUIDELINES FOR FEDERAL, STATE AND LOCAL AGENCIES AND ENTITIES; Safeguards for Protecting Federal Tax Returns and Return Information)
Tenable Nessus

- Commercial product, free for 501(c)(3) organizations

- **Description:** “Protect your IT environment by running vulnerability scans, configuration and compliance checks, malware detection, web application scanning and more.”
# Nessus Assessments

## Multiple Assessment Types

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability scanning</td>
<td>Assess systems, networks and applications for weaknesses</td>
</tr>
<tr>
<td>Configuration auditing</td>
<td>Ensure that IT assets are compliant with policy and standards</td>
</tr>
<tr>
<td>Compliance checks</td>
<td>Audit system configurations and content against standards</td>
</tr>
<tr>
<td>Malware detection</td>
<td>Detect malware as well as potentially unwanted and unmanaged software</td>
</tr>
<tr>
<td>Web application scanning</td>
<td>Discover web server and services weaknesses and OWASP vulnerabilities</td>
</tr>
<tr>
<td>Sensitive data searches</td>
<td>Identify private information on systems or in documents</td>
</tr>
<tr>
<td>Control system auditing</td>
<td>Scan SCADA systems, embedded devices and ICS applications</td>
</tr>
<tr>
<td>Cloud Support</td>
<td>Assess configuration weaknesses in Amazon Web Services, Microsoft Azure and Rackspace public clouds</td>
</tr>
</tbody>
</table>
### Heartbleed Scan

**CURRENT RESULTS: 04/09/14 AT 10:05 AM**

#### Scans > Hosts

<table>
<thead>
<tr>
<th>Host</th>
<th>Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.1.14</td>
<td>24 Critical, 6 High, 192 Info</td>
</tr>
<tr>
<td>10.1.1.56</td>
<td>17 Critical, 132 Info</td>
</tr>
<tr>
<td>10.1.1.11</td>
<td>14 Critical, 124 Info</td>
</tr>
<tr>
<td>10.1.1.58</td>
<td>12 Critical, 120 Info</td>
</tr>
<tr>
<td>10.1.1.223</td>
<td>14 Critical, 7 High, 84 Info</td>
</tr>
<tr>
<td>10.1.1.27</td>
<td>11 Critical, 79 Info</td>
</tr>
<tr>
<td>10.1.1.20</td>
<td>12 Critical, 75 Info</td>
</tr>
<tr>
<td>10.1.1.12</td>
<td>11 Critical, 74 Info</td>
</tr>
<tr>
<td>10.1.1.16</td>
<td>15 Critical, 62 Info</td>
</tr>
<tr>
<td>10.1.1.190</td>
<td>5 Critical, 60 Info</td>
</tr>
<tr>
<td>10.1.1.26</td>
<td>9 Critical, 55 Info</td>
</tr>
<tr>
<td>10.1.1.222</td>
<td>6 Critical, 62 Info</td>
</tr>
</tbody>
</table>

#### Scan Details

- **Name:** Heartbleed Scan
- **Status:** Completed
- **Policy:** Internal Network Scan
- **Folder:** My Scans
- **Start:** 04/09/14 at 10:05 AM
- **End:** 04/09/14 at 10:05 AM
- **Elapsed:** a few seconds
- **Targets:** 192.168.25.0/34, 10.1.1.0/24, 10.1.1.58, 10.0.0/24, 198.160.139.0/24

#### Vulnerabilities

- Critical
- High
- Medium
- Low
- Info
<table>
<thead>
<tr>
<th>Severity</th>
<th>Plugin Name</th>
<th>Plugin Family</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRITICAL</td>
<td>Compaq WBEM HTTP Server Remote Overflow</td>
<td>Web Servers</td>
<td>4</td>
</tr>
<tr>
<td>CRITICAL</td>
<td>VMware Security Updates for vCenter Server (VMSA-2013-0012)</td>
<td>Misc.</td>
<td>3</td>
</tr>
<tr>
<td>CRITICAL</td>
<td>Oracle Database Unsupported</td>
<td>Databases</td>
<td>2</td>
</tr>
<tr>
<td>CRITICAL</td>
<td>Samba ‘And0X’ Request Heap-Based Buffer Overflow</td>
<td>Misc.</td>
<td>2</td>
</tr>
<tr>
<td>CRITICAL</td>
<td>Apache Tomcat / JBoss EJBInvokerServlet / JMXInvokerServlet Marshalled Object Rem...</td>
<td>CGI abuses</td>
<td>1</td>
</tr>
<tr>
<td>CRITICAL</td>
<td>Microsoft Windows 2000 Unsupported Installation Detection</td>
<td>Windows</td>
<td>1</td>
</tr>
<tr>
<td>CRITICAL</td>
<td>MS02-061: Microsoft SQL Server Multiple Vulnerabilities (uncredentialled check)</td>
<td>Databases</td>
<td>1</td>
</tr>
<tr>
<td>CRITICAL</td>
<td>VERITAS Backup Exec Agent Unauthenticated Remote Registry Access</td>
<td>Gain a shell remotely</td>
<td>1</td>
</tr>
<tr>
<td>CRITICAL</td>
<td>VERITAS Backup Exec Remote Agent Static Password Arbitrary File Download</td>
<td>Misc.</td>
<td>1</td>
</tr>
<tr>
<td>CRITICAL</td>
<td>VMware Security Updates for vCenter Server (VMSA-2013-0008)</td>
<td>Misc.</td>
<td>1</td>
</tr>
<tr>
<td>HIGH</td>
<td>SNMP Agent Default Community Name (public)</td>
<td>SNMP</td>
<td>11</td>
</tr>
</tbody>
</table>
Taking the following actions across 22 hosts would resolve 31% of the vulnerabilities on the network:

<table>
<thead>
<tr>
<th>Action to take</th>
<th>Vuls</th>
<th>Hosts</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Security Updates for vCenter Server (VMSA-2013-0012): Upgrade to VMware vCenter 5.0 update 3, 5.1 update 2 or later.</td>
<td>102</td>
<td>3</td>
</tr>
<tr>
<td>Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness: - Force the use of SSL as a transport layer for this service if supported, or/and - Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.</td>
<td>13</td>
<td>13</td>
</tr>
<tr>
<td>Portable OpenSSH ssh-keysign ssh-rand-helper Utility File Descriptor Leak Local Information Disclosure: Upgrade to Portable OpenSSH 5.8p2 or later.</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>Symantec Backup Exec for Windows RPC Crafted ncaon_ip_tcp Request Remote Overflow: <a href="http://seer.entsupport.symantec.com/docs/269731.htm">http://seer.entsupport.symantec.com/docs/269731.htm</a></td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue: Upgrade to OpenSSL 0.9.8q / 1.0.0.c or later, or contact your vendor for a patch.</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Apache HTTP Server httpOnly Cookie Information Disclosure: Upgrade to Apache version 2.0.65 / 2.2.22 or later.</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>
Security Onion

- Open Source
- [https://security-onion-solutions.github.io/security-onion/](https://security-onion-solutions.github.io/security-onion/)

- Commercial Alternative: Metaflows ($8,000+)

- Description: “Security Onion is a Linux distro for intrusion detection, network security monitoring, and log management. It's based on Ubuntu and contains Snort, Suricata, Bro, OSSEC, Sguil, Squert, ELSA, Xplico, NetworkMiner, and many other security tools. The easy-to-use Setup wizard allows you to build an army of distributed sensors for your enterprise in minutes!”
Components

- **OSSEC** – Open Source Host-based Intrusion Detection System that performs log analysis, file integrity checking, policy monitoring, rootkit detection, real-time alerting and active response.
- **Sguil** – Analysis tool
- **Squert** – Web app on top of Squil
- **ELSA (with Syslog-ng)** – Log analysis
- **Snort & Suricata** – Alerting software
- **Snorby** – Web tool to look at Snort and Suricata alerts
### RealTime Events

<table>
<thead>
<tr>
<th>ST</th>
<th>CNV</th>
<th>Sensor</th>
<th>Alert ID</th>
<th>Date/Time</th>
<th>Src IP</th>
<th>Dst IP</th>
<th>Offset</th>
<th>IP</th>
<th>Event Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>fin-exit</td>
<td>3.313990</td>
<td>2014-11-07 00:44:43</td>
<td>222.186.21.55</td>
<td>4270</td>
<td>97.95.102.96</td>
<td>22</td>
<td>6</td>
<td>ET SCAN SSH Based SSH Connection - Often used as a BruteForce Tool</td>
</tr>
<tr>
<td>1</td>
<td>fin-exit</td>
<td>3.313991</td>
<td>2014-11-07 00:45:55</td>
<td>213.226.96.87</td>
<td>5073</td>
<td>97.95.102.96</td>
<td>5060</td>
<td>17</td>
<td>ET SCAN Suspicious User-Agent Detected (friendly-scanner)</td>
</tr>
<tr>
<td>1</td>
<td>fin-exit</td>
<td>3.313992</td>
<td>2014-11-07 00:45:55</td>
<td>213.226.96.87</td>
<td>5073</td>
<td>97.95.102.96</td>
<td>5060</td>
<td>17</td>
<td>ET SCAN Suspicious Scan</td>
</tr>
<tr>
<td>1</td>
<td>fin-exit</td>
<td>7.1033042</td>
<td>2014-11-07 00:50:06</td>
<td>23.215.46.133</td>
<td>80</td>
<td>192.168.6.77</td>
<td>55300</td>
<td>6</td>
<td>ET SHELLCODE Excessive Use of HeapLib Objects Likely Malicious Heap Spray Attempt</td>
</tr>
<tr>
<td>1</td>
<td>fin-exit</td>
<td>7.1033043</td>
<td>2014-11-07 00:50:20</td>
<td>192.168.6.77</td>
<td>55305</td>
<td>208.85.40.20</td>
<td>80</td>
<td>6</td>
<td>ET POLICY Pandora Usage</td>
</tr>
<tr>
<td>1</td>
<td>fin-exit</td>
<td>7.1033044</td>
<td>2014-11-07 00:50:20</td>
<td>192.168.6.77</td>
<td>55305</td>
<td>208.85.40.20</td>
<td>80</td>
<td>6</td>
<td>ET POLICY Pandora Usage</td>
</tr>
</tbody>
</table>

### Additional Information

- **IP Resolution**
- **Agent Status**
- **Short Statistics**
- **System Maps**
- **User Maps**

![Network Diagram](image-url)
Enterprise Log Search and Archive

Query: class=SSH_LOGIN

Start Time: 2011-04-22 18:35:51
End Time: 

Fields:
- Timestamp
- Accepted keyboard-interactive/pam for root from 127.0.0.1 port 5399 ssh2
  - host=127.10.105.1 program=sshd class=SSH_LOGIN port=5399 authmethod=keyboard-interactive/pam
  - user=root device=127.0.0.1 service=sshd
- Accepted keyboard-interactive/pam for root from 127.0.0.1 port 46996 ssh2
  - host=127.10.105.1 program=sshd class=SSH_LOGIN port=46996 authmethod=keyboard-interactive/pam
  - user=root device=127.0.0.1 service=sshd

Records: 2 / 2 1067 ms
Chef

- Open Source Product with Commercial Support
- [https://www.chef.io/](https://www.chef.io/) – Commercial
- [http://chef.github.io/](http://chef.github.io/) – Open Source

Description: “A systems integration framework, built to bring the benefits of configuration management to your entire infrastructure.”

Benefits:
- Change & Configuration Management
- Shared recipes/cookbooks
- Automatic updates*
- Rapid deployment of new servers
- Disaster Recovery
Chef Concepts

- **Node** – A “device” where Chef runs
  - Physical Server
  - Cloud Server
  - Virtual Machine
  - Network Device
  - Container

- **Recipe** – A definition for how to build a server.

- **Cookbooks** – A collection of recipes.

- **Chef Client** – The tool that runs periodically to update the server.
Chef Example: Web Server
Bottom Line

- Compliance and Risk Management is complicated.
- Tools (inexpensive or free) are available.
- It will still take time.
Thanks!

- Patrick Gardella
- patrick.gardella@asburyseminary.edu
- Office: 859–858–2130
- Cell: 443–370–2238