Cultivating a Training and Awareness Program: From Seedling to Sapling

Julie Boughn
Director,
Division of CMS Enterprise Standards
Centers for Medicare & Medicaid Services (CMS)

Environment & History

- Centers for Medicare & Medicaid Services (CMS)
  (formerly the Health Care Financing Administration [HCFA])
- Medicare
- Medicaid
- State Children’s Health Insurance Program (SCHIP)

www.cms.hhs.gov/it/security
CMS - Bird’s Eye View (FY2001)

- Personnel – 4,600 government employees
- Beneficiaries – 78 million
- Benefit Outlays - $359 billion
- Program Management - $2.29 billion
- Medicare Fiscal Intermediaries and Carriers – approximately 70

www.cms.hhs.gov/it/security
4 Pillars of the IT Security Program

CMS Information Security Program

- Policies & Procedures
- Training & Awareness
- Security Architecture
- Certification & Accreditation

CMS Security Organization

www.cms.hhs.gov/it/security
Where Did We Start ???

- Current Awareness & Training Report
- Awareness & Training Structure Report
- Framework Report
- Program Details
- Senior Executives Briefing

www.cms.hhs.gov/it/security
Centers for Medicare & Medicaid Services (CMS)

Training and Awareness

• Target Audiences
  – Management/Executives
  – End Users (include contractors)
  – System Developers/Maintainers

• Message Delivery
  – Formal briefings & classes
  – Awareness Day
  – Conferences
  – Cyber Tyger
  – Web
  – Newsletter
  – Computer Based Training

www.cms.hhs.gov/it/security
Senior Executive & Manager’s briefings

- Available on NIST FASP site
  (http://csrc.nist.gov/fasp/)
- Must have Executive and Managers support
- Simple
- Non-technical
- Peer led round-table discussion
- Publicize their Information Resources

www.cms.hhs.gov/it/security
ISSO & SSP courses

- Senior management backing
- Peer led round-table discussion
- Prepare for resistance
- Must provide continuous support resources
- Must provide “TOOLS”
“TOOLS” - Security in the SDLC

- System Security Levels
- Business Case Analysis
- Accept. Risk Safeguards
- System Req. Document
- Threat ID Resource

Identify Vulnerabilities

RA & SSP

www.cms.hhs.gov/it/security
<table>
<thead>
<tr>
<th>Security Level</th>
<th>Description</th>
<th>Explanation</th>
</tr>
</thead>
</table>
| Low           | Moderately serious| • Noticeable impact on an agency’s missions, functions, image, or reputation. A breach of this security level would result in a negative outcome; or  
• Would result in DAMAGE, requiring repairs, to an asset or resource. |
| Moderate      | Very serious      | • Severe impairment to an agency’s missions, functions, image, and reputation. The impact would place an agency at a significant disadvantage; or  
• Would result in MAJOR damage, requiring extensive repairs to assets or resources. |
| High          | Catastrophic      | • Complete loss of mission capability for an extended period; or  
• Would result in the loss of MAJOR assets or resources and could pose a threat to human life. |
# System Development “TOOLS”

## SSL - Information Categories

<table>
<thead>
<tr>
<th>Information Category</th>
<th>Explanation and Examples</th>
<th>System Security Level*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information about persons</td>
<td>Information related to personnel, medical, and similar data. Includes all information covered by the Privacy Act of 1974 (e.g., salary data, social security information, passwords, user identifiers (IDs), EEO, personnel profile (including home address and phone number), medical history, employment history (general and security clearance information), and arrest/criminal investigation history).</td>
<td>Moderate</td>
</tr>
<tr>
<td>Financial, budgetary, commercial, proprietary and trade secret information</td>
<td>Information related to financial information and applications, commercial information received in confidence, or trade secrets (i.e., proprietary, contract bidding information, sensitive information about patents, and information protected by the Cooperative Research and Development Agreement). Also included is information about payroll, automated decision making, procurement, inventory, other financially-related systems, and site operating and security expenditures.</td>
<td>Moderate</td>
</tr>
</tbody>
</table>
## System Development “TOOLS”

### Acceptable Risk Safeguards

<table>
<thead>
<tr>
<th>Organizational Security Standard</th>
<th>System Security Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Store and Operate Servers in Secure, Isolated Environments</td>
<td>Low: -protected from unauthorized access.</td>
</tr>
</tbody>
</table>
## TECHNICAL THREATS

<table>
<thead>
<tr>
<th>THREATS</th>
<th>DESCRIPTIONS</th>
<th>EXAMPLES</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Data Entry Errors</td>
<td>• Mistakes in keying or oversight to keyed data, which could affect system resources and the safeguards that are protecting other system resources.</td>
<td>• Entering incorrect values for sensitive information such as SSN, financial data or personally identifiable data could result in data inconsistency.</td>
</tr>
</tbody>
</table>

**System Impact**
Could significantly impact data integrity, and to a lesser extent data availability.
<table>
<thead>
<tr>
<th>Item No.</th>
<th>Threat Name</th>
<th>Vulnerability Name</th>
<th>Risk Description</th>
<th>Existing Controls</th>
<th>Likelihood of Occurrence</th>
<th>Impact Severity</th>
<th>Risk Level</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### System Development “TOOLS”

**RA – Likelihood of Occurrence**

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Negligible</td>
<td>Unlikely to occur.</td>
</tr>
<tr>
<td>Very Low</td>
<td>Likely to occur two/three times every five years.</td>
</tr>
<tr>
<td>Low</td>
<td>Likely to occur one every year or less.</td>
</tr>
<tr>
<td>Medium</td>
<td>Likely to occur once every six months or less.</td>
</tr>
<tr>
<td>High</td>
<td>Likely to occur once per month or less.</td>
</tr>
<tr>
<td>Very High</td>
<td>Likely to occur multiple times per month</td>
</tr>
<tr>
<td>Extreme</td>
<td>Likely to occur multiple times per day</td>
</tr>
<tr>
<td>Impact Severity</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Insignificant</td>
<td>Will have almost no impact if threat is realized and exploits vulnerability.</td>
</tr>
<tr>
<td>Minor</td>
<td>Will have some minor effect on the system. It will require minimal effort to repair or reconfigure the system.</td>
</tr>
<tr>
<td>Significant</td>
<td>Will result in some tangible harm, albeit negligible and perhaps only noted by a few individuals or agencies. May cause political embarrassment. Will require some expenditure of resources to repair.</td>
</tr>
<tr>
<td>Damaging</td>
<td>May cause damage to the reputation of system management, and/or notable loss of confidence in the system’s resources or services. It will require expenditure of significant resources to repair.</td>
</tr>
<tr>
<td>Serious</td>
<td>May cause considerable system outage, and/or loss of connected customers or business confidence. May result in compromise or large amount of Government information or services.</td>
</tr>
<tr>
<td>Critical</td>
<td>May cause system extended outage or to be permanently closed, causing operations to resume in a Hot Site environment. May result in complete compromise of Government agencies’ information or services.</td>
</tr>
<tr>
<td>Likelihood of Occurrence</td>
<td>Insignificant</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Negligible</td>
<td>Low</td>
</tr>
<tr>
<td>Very Low</td>
<td>Low</td>
</tr>
<tr>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Very High</td>
<td>Low</td>
</tr>
<tr>
<td>Extreme</td>
<td>Low</td>
</tr>
<tr>
<td>Item No.</td>
<td>Recommended Safeguard Description</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## System Development “TOOLS”

### Risk – Mitigating Actions

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Risk Level</th>
<th>Recommended Safeguard</th>
<th>Residual Risk</th>
<th>Status of Safeguard</th>
<th>Updated Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Entry Errors</td>
<td>High</td>
<td>Implement drop-down menus where appropriate</td>
<td>Low</td>
<td>50% of drop-down menu fields have been implemented</td>
<td>Moderate</td>
</tr>
</tbody>
</table>

**Centers for Medicare & Medicaid Services (CMS)**

[www.cms.hhs.gov/it/security](http://www.cms.hhs.gov/it/security)
Centers for Medicare & Medicaid Services (CMS)

Awareness Days & Conferences

- Target audiences
- Publicity
- Free-trinkets
- Format & time allocations
- Don’t be afraid to try something new

www.cms.hhs.gov/it/security
Centers for Medicare & Medicaid Services (CMS)

Cyber Tyger

- Everything’s coming up “Cyber Tygers”
- CyberTyger@cms.hhs.gov
CMS Information Security

CMS Information Security & Privacy End-User Training

CMS SSP Methodology V 2.1
(Released February 7, 2002)

CMS Risk Assessment Methodology (Coming Soon)

new CMS Threat Identification Resource
HELP! HELP! HELP! – I think I have a VIRUS…

“That is – my computer has a virus. Well I think it does, but I’m not sure. I received an e-mail from a friend of a friend’s sister who said that if a computer boots up on the first try then you should assume you have a virus and delete all of your files in order to stop the virus from spreading.”
Information Security & Privacy

End-User Computer Based Training (CBT)

• Web based
  – Currently intranet
  – On/about May 2003 – internet
    (www.CMS.hhs.gov/it/security)

• CMS employees – mandatory completion by December 31, 2002

• On/about May 2003, mandatory for CMS Userid annual recertification

www.cms.hhs.gov/it/security
What Do These Privacy Rules and Requirements Mean to You?

The Privacy Act and HIPAA Privacy Rule both state that if any agency fails to protect an individual's personal information in such a way as to have an adverse effect on the individual, that individual may bring civil action against the agency and the person responsible.

Hence, you could be the one responsible for the breach of confidentiality. CMS and you could be held liable for civil damages.
3. Which of the following is considered computer abuse:

- Reading or obtaining data that you are not authorized to access
- Making unauthorized copies of Government-owned software
- Using CMS resources to make personal profits or conduct personal business
- All of the above
Getting Started – Lessons Learned

• Follow NIST SP 800-50, Building an IT Security Training & Awareness Program instead of producing:
  – Current Awareness & Training Report
  – Awareness & Training Structure Report
  – Framework Report
  – Program Details

• Immediately begin work on:
  – Senior Executive briefing
  – End-User training
  – Managers briefing
  – ISSO course
Program - Lessons Learned

- Different target audiences with different needs
- Wanted a “perfect” CBT
- Start early with end user “reminders”
- Be prepared with answers, resources and tools

www.cms.hhs.gov/it/security
Best Practices

• Partner with Privacy Officer / Advocates
• End-user Awareness
  – Technology-based (web, CD’s etc.)
  – Awareness Days/Conferences/Trinkets
  – Paper-based (newsletter, tri-fold)
  – CyberTyger E-mail
• Management Awareness - especially for system development areas
• Technical Training - Developers/ Administrators/ISSOs
• Intranet Web Site
What’s Next

- e-Gov Initiatives
- Modernization
- Expanded audience

www.cms.hhs.gov/it/security
Registration

Please enter your Medicare Health Insurance Claim Number from your red, white, and blue card along with the additional required information and click on Register. This information will be compared with information from the Social Security Administration. If the information matches, an e-MSN password will be automatically mailed to you.

Is this a re-enrollment?  

Yes ☐  No ☐

Medicare Number:
Thank You !!!

- CyberTyger@cms.hhs.gov
- www.cms.hhs.gov/it/security

Julie Boughn
Director, CMS-OIS-SSG-DCES
Jboughn@cms.hhs.gov

Sharon Kavanagh
Training & Awareness Coordinator
Skavanagh@cms.hhs.gov