HIE: The Human Component of Information Security

James C. Murphy
GSEC, CISSP-ISSMP, CISA, CISM
Information Security Architect
NC DHHS, Office of MMIS Services
james.murphy@dhhs.nc.gov

Disclaimer:
This presentation reflects only the presenter's professional and/or personal views. The material presented herein is not intended to represent official statements or positions of NC DHHS or OMMISS.
HIE - Information Security

Information Security: Providing Protection - Controlling Access

Most important asset: Human Resource (internal)

Greatest source of threats/vulnerabilities: Human Resource (internal and external)

Most important capability: Personal Communication (all kinds)

Most difficult context: People/Information/Technology/Process
HIE: The Human Component

Patients/Recipients
Providers
Provider Tech Support
HIE - Others
Outsiders!

What are we in for??
“With the pervasiveness of information being made available electronically, healthcare organizations are increasingly attracting cybercriminals. As evidence of this, nearly one out of every six data breaches that occurred in 2009 was targeted at the healthcare industry, according to the Open Security Foundation. Certainly, that number is expected to grow.”
“Why? There are numerous reasons. For one, it pays. The World Privacy Forum has reported that the street cost for stolen medical information is $50, versus $1 for a stolen Social Security number. The average payout for a medical identity theft is $20,000, compared to $2,000 for a regular identity theft. Second, it is harder to detect. Medical information fraud takes more than twice as long to identify as compared to regular identity theft. Simply put, victims can close a compromised bank account, but they can’t delete or change their personal information, medical records or history of prescription use.”
Patients

From RSA White Paper (emphasis added):

According to RSA’s 2010 Global Online Consumer Security Survey:

- 64% of consumers stated they were concerned with their personal information being accessed or stolen on a healthcare site

- 59% of consumers stated their concerns with their personal information being stolen makes them less likely to submit personal information to a healthcare site

- 64% of consumers stated that healthcare sites should implement a stronger form of security to identify users when logging in

- 95% of consumers stated they would be willing to use stronger security if it was offered at the healthcare site(s) they regularly visit
Patients/Recipients

Patients
Parents/Guardians
Spouse
Dependents

Requirements:
Identification, Validation,
Verification
Authorization of alternates
Authorization of access

Responsibilities:
Ownership, integrity of the record
Patients/Recipients

**Technology:**
Tools for I., V., & V. -
Enrollment (Patient Identifier?)
Linking patients to family and guardians
Access control
Change management
Patient-controlled permissions


**Coalition Design for Secure Protocols** - How parties that don't trust each other can securely agree on inputs and compute results.

**Secure Property Titles with Owner Authority** - Secure agreements on name spaces and other property rights

**Formalizing and Securing Relationships on Public Networks** - A survey of security for smart contracts

**Trusted Services and Group Controls** - Making trusted third parties trustworthy, to some extent, and the tradeoffs involved.
Providers

Physicians

Nurses

Clinicians

Administrators
e.g., Billing Clerks, internal, external

Requirements:
- Policies, Procedures
- Confidentiality Statement
- Authorization, Authentication, Validation, Verification
- Audit, segregation of duties

Responsibilities:
- Ownership, integrity of the data
Provider Tech Support

Requirements:
- Policies, Procedures
- Confidentiality Statement
- Authorization, Authentication, Validation, Verification
- Audit, segregation of duties

Responsibilities:
- Stewardship and protection of the data: proactive defense, change management
Providers & Tech Support

**Technology:**

Access Control – Role-based Access Control


## HIE - Others

<table>
<thead>
<tr>
<th>Member HCOs</th>
<th><strong>Requirements:</strong> Policies, Usage agreements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway/Central Host</td>
<td>Identification, Authorization, Authentication, Validation, Verification</td>
</tr>
<tr>
<td>State Agencies</td>
<td>Audits, Reports</td>
</tr>
<tr>
<td>Federal Agencies</td>
<td></td>
</tr>
<tr>
<td>Incident/Crime Response</td>
<td></td>
</tr>
</tbody>
</table>

**Responsibilities:** Transmission services, investigation, oversight, research
Outsiders!!

- **HCO Staff** (Neighbors)
- **HCO Visitors** (Opportunists!)
- **ID Thieves**
- **Attackers (Money)**

**Requirements:**
- Active defense: Prevention, Deterrence, Detection, Isolation, Identification, (Forensics)
- Reporting
- Adjustment

**Responsibilities:**
- Absolutely NONE!
Marcus Ranum
Chief of Security
Tenable Network Security, Inc.
mjr@tenablesecurity.com

6th Annual Triangle InfoSeCon;
October 21, 2010.

“Advanced Persistent Threats:
Coping with the truth behind the hype”

Paraphrased quotes:
If organizations don’t have a strong technical support staff, they have lost the battle.
Can we all agree that malware signature detection is no longer sufficient?
• Petri Dishes – malware testing
• Honeynets – intrusion detection
• Thresholders – event counts
• Whitelisting – good (acceptable) stuff
• Burglar alarms – thresholds exceeded, bad (not on whitelist) stuff

**Customized coding** – log review, analysis, statistics, etc
Challenge!

Work Factor

Asymmetric: Efforts to accomplish goals are highly skewed against the network/server/data administrators

Transitive Trust

Workstation? Small HCO??
Technical Challenge!

Advanced Persistent Threats (APT)

**Advanced:** Technical skills/tools we (most of us) haven't seen yet

**Persistent:** Extreme patience, slow, careful, difficult to detect

**Threats:** Harmful intent - capture of valuable data

*How can we make attackers' costs go up??*

*How can we pass that on to the HIN??*