Revision
First, the news ... 

- Hospitals and ransomware
Security is a whole system issue

- Software
- Hardware
- Physical environment
- Personnel
- Corporate and legal structures

### Security properties to ensure

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Confidentiality</strong></td>
<td>No improper information gathering</td>
</tr>
<tr>
<td><strong>Integrity</strong></td>
<td>Data has not been (maliciously) altered</td>
</tr>
<tr>
<td><strong>Availability</strong></td>
<td>Data/services can be accessed as desired</td>
</tr>
<tr>
<td><strong>Accountability</strong></td>
<td>Actions are traceable to those responsible</td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td>User or data origin accurately identifiable</td>
</tr>
</tbody>
</table>
Cyber Security Essentials

- How might each of these protect against ransomware?

- Secure configuration
- Boundary firewalls and internet gateways
- Access control and administrative privilege management
- Patch management
- Malware protection
Access Control
The problem: Backups at hospitals

- Hospitals need to backup data, but they also need to be certain that only the backup server is writing the data.
- Security lattices to the rescue...
- H: Classifications and linear ordering of classifications
- C: Categories
- Ordering:
  - \((h_1, c_1) \leq (h_2, c_2) \iff h_1 \leq h_2, c_1 \subseteq c_2\)
Make this true:
\[(h_1, c_1) \leq (h_2, c_2) \iff h_1 \leq h_2, c_1 \subseteq c_2\]

Classifications (H):
- Backup
- Users

Categories (C):
- P (Phyc ward)
- T (Transplant ward)
Network attacks and defenses
What needs to be protected from ransomware?

How might Man-in-the-middle be used to add ransomware to a hospital network?

How might a firewall be used to limit the spread of ransomware?
Usable Security
What on this email can be trusted?

From: "Fletcher, Freya" <ffletcher@conejousd.org>
Subject: FW: ITS Administrative Support

To: undisclosed-recipients:

Dear User,

Your password will expire within 24hrs Click on: Staff & faculty update to validate your e-mail.

This email has been scanned by the Symantec Email Security.cloud service. For more information please visit http://www.symanteccloud.com

http://staffupgrade.moonfruit.com/
What on this email can be trusted?

The actual URL is the only one of the three generated by the local computer and not the attacker.

From: Fletcher, Freya <ffletcher@conejousd.org>
Subject: FW: ITS Administrative Support
To: undisclosed-recipients;

From: Fletcher, Freya
Sent: Thursday, March 05, 2015 4:47 AM
Subject: ITS Administrative Support

Dear User,

Your password will expire within 24hrs Click on: Staff & faculty update to validate your e-mail.

This email has been scanned by the Symantec Email Security.cloud service. For more information please visit http://www.symanteccloud.com

http://staffupgrade.moonfruit.com/
Problem: Private detectives

- People call into the main phone line claiming to be a relative and ask for information about their relation
- However, some “relatives” are really private detectives or reporters
- How might you train the phone staff to not fall for these phishing attempts?
Authentication
Authentication factors

• Something you **know**
  ◦ Password, mother’s maiden name, your address

• Something you **have**
  ◦ Student ID card, credit card chip, RSA key

• Something you **are**
  ◦ Finger prints, voice tones, iris, typing patterns