The “HealthPad” at BIDMC

John D. Halamka MD
Chief Information Officer
The Infrastructure

- 18000 user accounts
- 9000 desktops/laptops/tablets
- 3000 printers
- 600 iPads
- 1600 iPhones
- 450 servers (200 physical, 250 virtual)
- 1.5 petabytes of storage
The Applications

• Built and bought web applications
• CPOE in every site of care
• 100% adoption of EHR and eRx
• Paperless Emergency department
• Filmless since 2000
The Culture

• First hospital to achieve federal certification of its systems
• First hospital in the US to achieve meaningful use
• First hospital to receive federal IT stimulus
• Information Week #1 Healthcare IT organization in the US
• Users have insatiable demand for IT exceeding limited supply (2% of operating budget)
The Ideal Device for Physicians

• Under a pound
• 12 hour battery life
• Disinfectable
• Can be dropped from 5 feet on to carpet without significant damage
• Small enough to fit in a coat pocket but large enough for order entry
The Ideal Device for Nurses

- Vital sign capture
- Inputs/outputs
- Medication workflow
- Lab workflow
- Nurse call workflow
Challenges

- Security
  - the Angry Birds problem
  - Web content filtering
  - Cost
  - Network Access Control
  - Private verses Public networks
- Procurement and lifecycle management
- Enterprise Management
- Native Applications verses Web
- The Consumer IT evolution problem
### Compromise via Home Computer

<table>
<thead>
<tr>
<th>Drop Server</th>
<th>200.63.44.172</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finding Type</td>
<td>Corporate Credentials</td>
</tr>
<tr>
<td>Description</td>
<td>An authorized user accessed one of the organization's resources, BIDMC Portal, from an infected machine (a screenshot is attached). The Trojan horse captured the credentials.</td>
</tr>
<tr>
<td>IP Address</td>
<td>24.63.18.108</td>
</tr>
<tr>
<td>Timestamp</td>
<td>Wed, 17 Aug 2011 01:06:01 GMT</td>
</tr>
</tbody>
</table>

**Rawtext**

```
User input: lxxxxxaKxxxxx3
POST data:
___EVENTVALIDATION=/wEWBALh8vWcAgKvpuq2CALyveCRDwLjNCfD1DONbAiUFgw75ofRC13PVI8NZ
username=sxxxxxa
password=Kxxxxx13
LoginButton.x=0
LoginButton.y=0","24.63.18.108","US","1313543148"
```

Counter Measures

• Tighten Internet access to and from the datacenter

• Explicit closings of outbound ports
  - 5,866 ports with fewer than 20 connects
  - 12 ports with more than 1000 connects
  - 20% of outbound connections are on port 445

• Add Perimeter protection at data center

• Proxy all public facing web services

• Deploy active WAF protection rules

• Enhanced Log collection and correlation

• Introduction of comprehensive vulnerability scans
The Best Counter Measure ..... 

- User awareness ......
Questions?

• jhalamka@caregroup.harvard.edu
• http://geekdoctor.blogspot.com