Like what you hear? Tweet it using: #Sec360
How Do You Spell CISO?

Secure360

Wed. May 14, 2014
bcaplin1@fairview.org
bc@bjb.org @bcaplin
http://about.me/barrycaplin
http://securityandcoffee.blogspot.com

Barry Caplin
Chief Information Security Official
Fairview Health Services

http://about.me/barrycaplin
securityandcoffee.blogspot.com
@bcaplin
Fairview Overview

• Not-for-profit established in 1906
• Academic Health System since 1997 partnership with University of Minnesota
• >22K employees
• >3,300 aligned physicians
  ▪ Employed, faculty, independent
• 7 hospitals/medical centers (>2,500 staffed beds)
• 40-plus primary care clinics
• 55-plus specialty clinics
• 47 senior housing locations
• 30-plus retail pharmacies

2012 data

5.7 million outpatient encounters
74,649 inpatient admissions
$2.8 billion total assets
$3.2 billion total revenue
Who is Fairview?

- FAIRVIEW RIDGES HOSPITAL
- FAIRVIEW RANGE HEALTH SERVICES
- FAIRVIEW SOUTHDALE HOSPITAL
- FAIRVIEW NORTHLAND MEDICAL CENTER
- FAIRVIEW LAKES MEDICAL CENTER

M HEALTH UNIVERSITY OF MINNESOTA

UNIVERSITY OF MINNESOTA CHILDREN'S HOSPITAL
- FAIRVIEW

UNIVERSITY OF MINNESOTA MEDICAL CENTER
- FAIRVIEW

EBENEZER

PreferredOne

FAIRVIEW PHARMACY

MAPLE GROVE HOSPITAL

A partnership of North Memorial and Fairview

Columbia Park Medical Group

Institute of Athletic Medicine

Minnesota Sports Medicine
Did you ever think about...
Challenges

• Keep it simple
• Keep it High Level
• Don’t let ‘em pull you in to the weeds
Game Time!
First Quarter

- Learn the Business
- Culture of Security
- Baseline the Organization
Learn the Business

Business/Ops lead – not Security or IT

- Do you know?
  - Industry
  - Niche
  - Mission/Vision
  - Why/What/How
  - The Organization
Learn the Business

• Ask Questions
• Org Charts
• Get Out of the Building!
• 1:1’s; Divisional meetings; Leaders; C-suite
Learn the Business

• Agenda
  – Introduction
  – learn about the business area,
  – what works and what doesn't,
  – partnership opportunities,
  – what can I do for you?

• Establish your office; Create Champions
A Culture of Security

A journey of a thousand miles begins with a single step.

- Lao-tzu, *The Way of Lao-tzu*
  *Chinese philosopher (604 BC - 531 BC)*

You gotta start somewhere.

- *Me*
A Culture of Security

• Is there existing training?
• Train for Compliance
• Awareness to reinforce
• Create Evangelists
A Culture of Security

• Be Relevant

• Connect to the Business

• Seek out and Destroy controls that add no value
Baseline the Organization

Helps you:

• Know where things stand
• Show progress
Baseline the Organization

Methods:
• Compare against known standard
• Maturity Model

- CObIT Security Baseline
- CObIT Maturity Assessment Tool
- Gartner IT Score
- Homegrown
In your spare time...

• Low hanging fruit
• Other duties as assigned
Second Quarter

• Strategic Planning
• Tactical Planning
• Roadmap
Security is not a Project.... It’s a Lifestyle!
Strategic Planning

- **5 year outcomes**
- **3 year support**
- **18 month execution**
- **Current goals**
Strategic Planning

- High-level
- Outcomes
- Framework
  - NIST
  - CObIT
  - HITRUST
  - ISO27001
Strategic Planning

- Business info +
- Baseline analysis +
- Risk Assessment +
  - Threat Assessment
    - Assets; Actors; Actions
- Vision =
  - Time Travel
Threat Modeling/Assessment

• Elevation of Privilege

• Cntl-Alt-Hack
  http://www.controlalthack.com/

• UW Security Cards
  http://securitycards.cs.washington.edu/
Tactical Planning

• Tactics are “How?”
  – Support each strategy
  – More granular
  – Shorter timeframe (1-3 yrs.)
Strategy/Tactics

Improve Situational Awareness

- Improve Access Management capability
- Build a Vulnerability Management program
- Detect malicious software, block disallowed software, allow approved software and detect unauthorized changes
# Roadmap

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
<th>I</th>
<th>J</th>
<th>K</th>
<th>L</th>
<th>M</th>
<th>N</th>
<th>O</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2014</td>
<td>2015</td>
<td>2016</td>
<td>2017</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1Q</td>
<td>2Q</td>
<td>3Q</td>
<td>4Q</td>
<td>1Q</td>
<td>2Q</td>
<td>3Q</td>
<td>4Q</td>
<td>1Q</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| 2 | A1. Strategy 1/Tactic 1
Initiative
project
project
project
project
project
project
project
project
project
| | | | | | | | | | | | | | | |
| 3 | X | | | | | | | | | | | | | |
| 4 | | | | | | | | | | | | | | | |
| 5 | | | | | | | | | | | | | | | |
| 6 | | | | | | | | | | | | | | | |
| 7 | | | | | | | | | | | | | | | |
| 8 | | | | | | | | | | | | | | | |
| 9 | | | | | | | | | | | | | | | |
| 10 | | | | | | | | | | | | | | | |
| 11 | | | | | | | | | | | | | | | |
| 12 | | | | | | | | | | | | | | | |
| 13 | A2. Strategy 1/Tactic 2
project
project
project
| | | | | | | | | | | | | | | | |
| 14 | | | | | | | | | | | | | | | |
| 15 | | | | | | | | | | | | | | | |
| 16 | | | | | | | | | | | | | | | |
| 17 | | | | | | | | | | | | | | | |
| 18 | A3. Strategy 1/Tactic 3
project
project
project
project
project
project
project
| | | | | | | | | | | | | | | | |
| 19 | | | | | | | | | | | | | | | |
| 20 | | | | | | | | | | | | | | | |
| 21 | | | | | | | | | | | | | | | |
| 22 | | | | | | | | | | | | | | | |
| 23 | | | | | | | | | | | | | | | |
| 24 | | | | | | | | | | | | | | | |
| 25 | | | | | | | | | | | | | | | |
Third Quarter...

- Execute!
- Metrics/KPIs/KRIs
- Communicating Risk
- BoD Reports
- Security Organization
...And Beyond

The “game” never ends.
• Iterative processes
• Support the “bridges”
• Living documents
• Review and refine