HEALTH IT SECURITY
USER EDUCATION
ROUNDTABLE:
A BEST PRACTICES SYMPOSIUM
WELCOME

Ben Steffen – Executive Director, Maryland Health Care Commission
A FRAMEWORK FOR IMPLEMENTING A ROBUST END-USER EDUCATION STRATEGY TO REDUCE RISK AND IMPROVE CYBERSECURITY POSTURE

Toby Gouker, PhD – Vice President of Strategy, First Health Advisory – Cybersecurity and Health IT Solutions
Framework for Implementing a Robust End-User Education Strategy
## Security Tools Implemented by Healthcare Providers

<table>
<thead>
<tr>
<th>Security Tool</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antivirus/malware</td>
<td>86.0%</td>
</tr>
<tr>
<td>Firewalls</td>
<td>80.7%</td>
</tr>
<tr>
<td>Data encryption (data in transit)</td>
<td>64.0%</td>
</tr>
<tr>
<td>Audit logs of each access to pt. health and financial records</td>
<td>60.0%</td>
</tr>
<tr>
<td>Data encryption (data at rest)</td>
<td>58.7%</td>
</tr>
<tr>
<td>Patch and vulnerability management</td>
<td>57.3%</td>
</tr>
<tr>
<td>Intrusion detection systems (IDS)</td>
<td>54.0%</td>
</tr>
<tr>
<td>Network monitoring tools</td>
<td>52.7%</td>
</tr>
<tr>
<td>Mobile device management (MDM)</td>
<td>52.0%</td>
</tr>
<tr>
<td>User access controls</td>
<td>50.7%</td>
</tr>
<tr>
<td>Intrusion prevention system</td>
<td>48.0%</td>
</tr>
<tr>
<td>Access control lists</td>
<td>47.3%</td>
</tr>
<tr>
<td>Single sign on</td>
<td>47.3%</td>
</tr>
</tbody>
</table>

Source: 2016 HIMSS Cybersecurity Survey
Awareness Program Spending

Source: 2016 SANS Security Awareness Report
• Awareness Compliance ≠ Security
• >75% of security events in healthcare involve “the human element”
• Improper workforce behavior is the highest threat, therefore…
• Creating a cyber-savvy workforce is the best first line of defense
Cyber-savvy Workforce

Awareness → Behavior Change

Level 1
- Working Towards Compliance

Level 2
- Education is simply delivered

Level 3
- Education is understood and remembered

Level 4
- Education is followed and acted upon
CyberHealth Workforce Clusters

Healthcare Delivery Organization

- Non-Clinical
- Clinical

- IT, Engineering, Research & Software
- Cybersecurity Staff
- C-Suite and Board
- Administrative, Finance, Legal
- Business Associates
<table>
<thead>
<tr>
<th>Education Program Maturity Level</th>
<th>Healthcare Delivery Organization</th>
<th>IT, Engineering, Research &amp; Software</th>
<th>Cybersecurity Staff</th>
<th>C-Suite and Board</th>
<th>Administrative</th>
<th>Business Associates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Level 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Level 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Level 4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Education Program Maturity Level</td>
<td>Healthcare Delivery Organization</td>
<td>IT, Engineering, Research &amp; Software</td>
<td>Cybersecurity Staff</td>
<td>C-Suite and Board</td>
<td>Administrative</td>
<td>Business Associates</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>----------------------------------</td>
<td>--------------------------------------</td>
<td>--------------------</td>
<td>------------------</td>
<td>----------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Level 4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Level 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Level 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Level 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
• Security is one of many training topics
• Only 15% of training can be recalled after 30 days

To affect behavior:
Training needs to be reinforced

• Posters, cafeteria signs, screensavers, etc.
• Monthly phishing
• Table-top exercises
• Gamification
• Time is of the essence for many employees
• Jobs are complicated
• Employees sneak in personal activities on work equipment

To affect behavior:
It needs to be simple

• No administrative access
• Provide automatic software & browser patch updates
• Password lockers
• Separate browser & email for personal activities
• Device trackers, full storage encryption
Key Lessons Learned

• No one cares about the "History of HIPAA"
• Quoting massive $$$ in breach fines has little impact
  To affect behavior: Make it personal
• Provide lessons on cybersecurity for the home
• Share on safe internet practices for children
• Share stories on employee’s personal compromises

Toby Gouker, PhD, GSLC
tgouker@fcp.com
(443) 570-0466
IMPROVING SECURITY CULTURE TO REDUCE HUMAN ERROR

Darren Lacey – Chief Information Security Officer and Director of IT Compliance, Johns Hopkins University and Johns Hopkins Medicine

Kevin Crain – Chief Information Security Officer and Director of IT Security, University of Maryland Medical System
Roundtable Discussion
Q&A
THANK YOU!