Cybersecurity is a Team Sport

Cyber Security Summit at Loyola Marymount University - October 22 2016

Dr. Robert Pittman, CISM
Chief Information Security Officer
County of Los Angeles Background

The County

• Largest populous County in the United States of America
• Serving 10+ million population speaking 140 languages
• Equivalent to 8th largest state just behind Ohio and ahead of Michigan
• Spans 4,043 square miles
• Comprised of 88 cities with more than 65% of County is unincorporated
• 19th largest economy in the world
County of Los Angeles Background (2)

The Government

• Five-member bipartisan elected Board of Supervisors
• 34 departments and over 140 commissions ~108,000 employees
• $28.7 billion FY 2016-17 Final Adopted Budget
• Serviced 700,000 patients, manage 14 major dams, care for 18,000 inmates/day, responded to over 300,000 emergency calls, 70 million visits to county beaches, cash assistance to 502,000 general relief recipients, maintain over 4,200 miles of roads and streets, issued 52,000 marriage licenses, loaned 16 million books, and collect taxes for 2.6 million households and commercial properties
Transformation in the County

September 13, 2001

“a transformation occurred …”
Is China our Friend or Foe?
Cyber Attacks
Life, Death, Taxes, and Breaches

World's Biggest Data Breaches
Selected losses greater than 30,000 records
(updated 16th Feb 2016)
Life, Death, Taxes, and Breaches (2)

California on guard after cyber attacks on elections databases in two states
Life, Death, Taxes, and Breaches (3)

ACTOR

- Nation-states
  - Cyber organized crime
    - Hacktivist
      - HBGary
    - Individual
      - Embarrass
      - Steal customer info
      - Disrupt operations and destroy property
      - Destroy business and future earnings
      - Widespread disruption and destruction

INTENT & IMPACT

- Sony
- Saudi Aramco
- JPMorganChase
- Target
- ??
Life, Death, Taxes, and **Breaches** (4)

### 2015 data breaches

**Number of data breach incidents by type**

- **4%** Nuisance
- **10%** Existential data
- **11%** Account access
- **22%** Financial access
- **53%** Identity theft

### Data records lost/stolen by industry

- **43%** Government
- **19%** Health care
- **17%** Other
- **12%** Technology
- **6%** Retail
- **3%** Education
- **<1%** Financial

*Source: Gemalto’s Breach Level Index 2015*
Who Participates in Cyber Crime?

Top 5 Threat Actors

- Cyber Criminals: 30%
- Hackers: 25%
- Non-Malicious Insiders: 21%
- Nation States: 13%
- Hactivists: 11%
Data Breaches Root Cause

Root Cause of Data Breach

- Malicious or criminal attack: 49%
- System glitch: 32%
- Human error: 19%
“Cybersecurity is a CEO level issue.”
Countywide Information Security Program (2)

Board of Supervisors

CEO
- Chief Info Security Officer
- **HW/SH Tools**

Dept’s
- Info Security Officer
- **Security**
- **Policies/Standards**

ISD/ITS
- Security Division
- **CERT**
# Countywide Information Security Program (4)

<table>
<thead>
<tr>
<th>R-Data</th>
<th>Data-at-Rest</th>
<th>Data-in-Transit (Annually)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drivers’ License</td>
<td>4.5M</td>
<td>1M</td>
</tr>
<tr>
<td>PCI</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PHI</td>
<td>6.5M</td>
<td>13M</td>
</tr>
<tr>
<td>PII</td>
<td>9.5M</td>
<td>13M</td>
</tr>
<tr>
<td>SSN</td>
<td>15.1M</td>
<td>13.1M</td>
</tr>
</tbody>
</table>
County’s Cyber Security Incidents

2015 Security Incidents by Month

2016 Security Incidents by Month

Malware Infection
Cease and Desist Order
Lost/Stolen Electronic Device
Data Breach (Reportable and Non-Reportable)
Social Engineering
Hacking/Unauthorized Access
Child Pornography
# County’s Cyber Security Incidents (2)

<table>
<thead>
<tr>
<th>Incident Categories</th>
<th>JAN</th>
<th>FEB</th>
<th>MAR</th>
<th>APR</th>
<th>MAY</th>
<th>JUN</th>
<th>JUL</th>
<th>AUG</th>
<th>SEP</th>
<th>OCT</th>
<th>NOV</th>
<th>DEC</th>
<th>YTD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware Infection</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>Cease and Desist Order</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Lost/Stolen Electronic Device</td>
<td>0</td>
<td>0</td>
<td>5</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>5</td>
<td>3</td>
<td>10</td>
<td>6</td>
<td>1</td>
<td>35</td>
</tr>
<tr>
<td>Data Breach (Reportable and Non-Reportable)</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>7</td>
</tr>
<tr>
<td>Hacking/Unauthorized Access</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Social Engineering</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>5</td>
<td>3</td>
<td>3</td>
<td>15</td>
</tr>
<tr>
<td>Child Pornography</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**TOTALS:** 0 2 6 3 2 0 5 7 4 17 10 4 60

<table>
<thead>
<tr>
<th>Incident Categories</th>
<th>JAN</th>
<th>FEB</th>
<th>MAR</th>
<th>APR</th>
<th>MAY</th>
<th>JUN</th>
<th>JUL</th>
<th>AUG</th>
<th>SEP</th>
<th>OCT</th>
<th>NOV</th>
<th>DEC</th>
<th>YTD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware Infection</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>2</td>
<td>4</td>
<td>3</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td>27</td>
</tr>
<tr>
<td>Cease and Desist Order</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>9</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td>13</td>
</tr>
<tr>
<td>Lost/Stolen Electronic Device</td>
<td>0</td>
<td>7</td>
<td>4</td>
<td>11</td>
<td>20</td>
<td>22</td>
<td>5</td>
<td>11</td>
<td>26</td>
<td></td>
<td></td>
<td></td>
<td>106</td>
</tr>
<tr>
<td>Data Breach</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>4</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td>11</td>
</tr>
<tr>
<td>Hacking/Unauthorized Access</td>
<td>0</td>
<td>1</td>
<td>5</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td>14</td>
</tr>
<tr>
<td>Social Engineering</td>
<td>0</td>
<td>2</td>
<td>9</td>
<td>16</td>
<td>11</td>
<td>9</td>
<td>20</td>
<td>32</td>
<td>24</td>
<td></td>
<td></td>
<td></td>
<td>123</td>
</tr>
<tr>
<td>Child Pornography</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td>0</td>
</tr>
</tbody>
</table>

**TOTALS:** 1 13 22 34 42 45 31 50 56     |     |     |     |     |     |     |     |     |     |     |     |     | 294 |
County IT Security Initiatives FY 2016-17

- **Board Motion Data-at-Rest**
  - County workstations ~90,000 (complete)
  - Contractors’ workstations and portable devices (New Board Policy #5.200)

- **Software License Consolidation for Endpoint Management**

- **Enterprise Mobility Suite**

- **Cyber Disruption Response Plan**

- **Enterprise IT Security Awareness & Training Content**

- **Phishing Campaign**

- **Cyber Security Liability Risk Insurance**
CISP Incident Response

CEO Office of Emergency Management (CEO OEM)

1) Active Shooter
2) Civil Unrest
3) Climate Control
4) Cyber
5) Earthquake
6) Pandemic / Infectious disease
7) Wildfires
CISP Incident Response (2)
CISP Incident Response (3)

“Signal or Noise”

County’s Email Gateway

<table>
<thead>
<tr>
<th>April 1 to Sept. 30, 2016</th>
<th>INBOUND EMAIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Threat Messages</td>
<td>88.80% 278,819,581</td>
</tr>
<tr>
<td>Total Graymails</td>
<td>5.40% 16,982,166</td>
</tr>
<tr>
<td>Clean Messages</td>
<td>5.80% 18,349,176</td>
</tr>
<tr>
<td>Total Attempted Messages</td>
<td></td>
</tr>
</tbody>
</table>

314,150,923
## CISP Incident Response (4)

### “Signal or Noise”

**County’s Web Application Firewall**

<table>
<thead>
<tr>
<th>Category</th>
<th>Year 2016</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>April</td>
</tr>
<tr>
<td>TRB</td>
<td>983,629</td>
</tr>
<tr>
<td>NTRB</td>
<td>354,057</td>
</tr>
<tr>
<td>NBFR</td>
<td>2,688,621</td>
</tr>
<tr>
<td><strong>MONTHLY TOTAL</strong></td>
<td>4,026,307</td>
</tr>
</tbody>
</table>
County Digest – October 2016

”The Nexus between 9/11 and Cyber Security in the County”