State Cybersecurity Legislation: 2017

NCSL Cybersecurity Task Force
April 21, 2017
Agenda

- Incidents/Threats
- Task Force Themes/Recommendations
- 2017 State Legislation/Trends
- Task Force Members’ Legislation
Pennsylvania Democrats' computers hit by ransomware cyberattack

Hacker group attacks state website apparently in response to 'religious freedom' law

California Senate Website Hit with Ransomware

'All of our shared drive files have been encrypted with software typically used in ransomware attacks,' said spokesman Andrew LaMar.

BY SAMANTHA YOUNG, TECHWIRE / JUNE 3, 2016
World's Biggest Data Breaches
Selected losses > 30,000 records

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
Most Common Vectors: Ransomware

<table>
<thead>
<tr>
<th>Application</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email link</td>
<td>31%</td>
</tr>
<tr>
<td>Email attachment</td>
<td>28%</td>
</tr>
<tr>
<td>A Web site or Web application other than email or social media</td>
<td>24%</td>
</tr>
<tr>
<td>Social media</td>
<td>4%</td>
</tr>
<tr>
<td>USB stick</td>
<td>3%</td>
</tr>
<tr>
<td>Business application</td>
<td>1%</td>
</tr>
<tr>
<td>We don’t know</td>
<td>9%</td>
</tr>
</tbody>
</table>

*Source: Osterman Research, Inc.*
# Most Common Vectors: Malware

<table>
<thead>
<tr>
<th>Safety 101: Main sources of threats penetration</th>
</tr>
</thead>
<tbody>
<tr>
<td>The most dangerous sources and ways of malware penetration are the following:</td>
</tr>
<tr>
<td>1. The Internet</td>
</tr>
<tr>
<td>2. Email</td>
</tr>
<tr>
<td>3. Software vulnerabilities</td>
</tr>
<tr>
<td>4. Removable data storage media</td>
</tr>
<tr>
<td>5. Users' actions</td>
</tr>
</tbody>
</table>

Source: Kaspersky Lab, https://support.kaspersky.com/viruses#block2
Themes and Recommendations
Cybersecurity Task Force Sessions

- Leadership Awareness and Expertise
- Budget for Cybersecurity
- Statewide IT Governance and Leadership
- Security Strategies/Cyber Hygiene/Combat Threats
- Incidence Response Preparation and Practice
- Promote Cybersecurity Workforce and Skills
What Are Legislatures Doing?

- **Awareness: Commissions and Studies**
- **Improving Governance & Security Practices**
- **Targeting Computer Crimes**
- **Promoting Workforce, Training, Economic Development**
- **Modifying Security Breach Notification Laws**
What Are Legislatures Doing?
2017 Introduced Cybersecurity Legislation

As of April 18, 2017
What Are Legislatures Doing?

Improving Governance and Security Practices

- Central, coord. governance, security practices:
  - 22 states: introduced
  - 4 states: enacted

- Incidence/emergency response:
  - 7 states: introduced
  - 4 states: enacted

- Exemptions from FOIA:
  - 8 states: introduced
  - 3 states: enacted
What Are Legislatures Doing?

Targeting Computer Crimes

Increasing penalties
7 states: introduced
2 states: enacted

Ransomware
11 states: introduced
1 state: enacted

Spyware/phishing/malware/DoS
7 states: introduced
1 state: enacted
What Are Legislatures Doing?

Workforce Training & Economic Development

Training/skills schools, higher ed
- 12 states: introduced
- 1 state: enacted

Econ. Devel., R & D, tax incentives
- 4 states: introduced
- 1 state: enacted
What Are Legislatures Doing?

Security Breach Notification

• New Mexico – 48th state
  (Legislation also pending in Alabama)

• Tennessee – restored exemption for encrypted information

• Virginia – requires notification to AG of breach of taxpayer ID
What Are Legislatures Doing?

Other Areas

• Energy, critical infrastructure

• Elections

• Student data
Task Force Members’ Sponsored Legislation