IT Cybersecurity for Counties

Wednesday, October 17
1:05-1:55 p.m.

Michael Cheng, Head of Information Security, Bexar County

This session will introduce an effective framework to quickly improve counties’ cybersecurity posture.
Michael Cheng, Head of Information Security, Bexar County, San Antonio

Cheng joined Bexar County Information Technology as the head of information security in June 2018. He is responsible for establishing and maintaining vision, strategy, and program to ensure Bexar County information assets and technologies are adequately protected. Prior to current position, Cheng was Chief Information Security Officer at Aviage Systems, one of GE Aviation’s joint ventures.
CYBERSECURITY AT COUNTIES

October, 2018

AGENDA

- Major Cybersecurity Threats
- Challenges
- Quick Wins and Long Term Strategy
MAJOR CYBERSECURITY THREATS

Worldwide Threat Assessment - 2017

Director of National Intelligence Dan Coates
to Senate Select Committee on Intelligence – May 11, 2017

Russia: Russia is assuming a more assertive posture based on its willingness to target critical infrastructure systems and conduct espionage operations even when detected and under increased public scrutiny.

China: China continues to have success in cyber espionage against the US Government, our allies and US companies. Beijing also selectively uses cyber attacks against targets it believes threaten Chinese domestic stability or regime legitimacy.

Iran: Iran used cyber espionage, propaganda, and attacks in 2015 to support its security priorities, influence events and counter threats—including against US allies in the region.

North Korea: North Korea probably remains capable and willing to launch disruptive or destructive cyber attacks to support its political objectives.

Non-State Actors: Terrorists continue to use the Internet to organize, recruit, spread propaganda, collect intelligence, raise funds and coordinate operations.
THREATS TO STATES/COUNTIES/CITIES

State and local governments face a disturbing cybersecurity threat
Commentary: Particularly in smart cities, the cyberattacks is as high as ever, says the CEO of Labs.

Atlanta’s ransomware attack cost $2.7M
A cyberattack that shut down most of the City of Atlanta’s network — a steeper price tag than the $50,000 ransom hackers had asked — cost the city $2.7 million in repairs. In an effort to recover its systems, the city spent $2.7 million on contracts the company signed to cybersecurity for assessing the damage and developing a plan. Atlanta signed with private technology companies to work on its systems.

They were probably not as protected as we probably thought," cybersecurity researcher Don Hunt, PhD, told Channel 2 Action News last year, when they’re spending a lot of money, so the damage is enormous.

Hack disrupted Baltimore 911 dispatch system for 17 hours, mayor says

WE ARE TARGETED

Organizations Investigated By Mandiant in 2017, By Industry

<table>
<thead>
<tr>
<th>Industry</th>
<th>Americas</th>
<th>APAC</th>
<th>EMEA</th>
<th>Global</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business and Professional Services</td>
<td>18%</td>
<td>10%</td>
<td>12%</td>
<td>16%</td>
</tr>
<tr>
<td>Energy</td>
<td>5%</td>
<td>2%</td>
<td>7%</td>
<td>5%</td>
</tr>
<tr>
<td>Entertainment and Media</td>
<td>11%</td>
<td>7%</td>
<td>5%</td>
<td>10%</td>
</tr>
<tr>
<td>Financial</td>
<td>17%</td>
<td>9%</td>
<td>24%</td>
<td>20%</td>
</tr>
<tr>
<td>Government</td>
<td>6%</td>
<td>7%</td>
<td>10%</td>
<td>8%</td>
</tr>
<tr>
<td>Healthcare</td>
<td>12%</td>
<td>2%</td>
<td>3%</td>
<td>9%</td>
</tr>
<tr>
<td>High Tech</td>
<td>9%</td>
<td>10%</td>
<td>7%</td>
<td>8%</td>
</tr>
<tr>
<td>Retail and Hospitality</td>
<td>10%</td>
<td>2%</td>
<td>4%</td>
<td>8%</td>
</tr>
<tr>
<td>Other</td>
<td>12%</td>
<td>20%</td>
<td>22%</td>
<td>15%</td>
</tr>
</tbody>
</table>

Government agencies are ranked #7 sectors in Americas, experiencing most cyber-attacks and system compromises in 2017
THINGS ARE AT RISK

- Election Systems & Election Information
- Criminal Justice Information (CJI) & Criminal History Record Information (CHRI)
- Personal Identified Information (PII)
- Personal Medical Information
- Payment Card Data
- Government Secrets

POSSIBLE ENTRY POINTS

- Phishing Emails
- System Vulnerabilities
- Incorrect Configurations
- Third Parties
CHALLENGES COUNTRIES ARE COMMONLY FACING

- Out-of-date IT Infrastructure
- Over-used Privileged Accounts
- Lack of Boundary Defense
- Ignorance of Security Incidents
- ...

We are extremely vulnerable
THINGS TO QUICKLY ENHANCE CYBERSECURITY

- Asset Management
  - Inventory and control of hardware devices
  - Inventory and control of software
  - Control security configurations of hardware and software
- Access Control
  - Control of Privileged Accounts
- Vulnerability Management
  - Continuous vulnerability management
- Security Monitoring
  - Maintenance, Monitoring and Analysis of Audit Logs
RESOURCES TO LEVERAGE

- MS-ISAC (https://www.cisecurity.org/ms-isac/)
- DHS
- Texas DIR contracts and services

LONG TERM STRATEGY

- Establish Cybersecurity Program
- Adopt Mature Cybersecurity Framework, CIS Top 20 Controls, NIST, etc.
- Transform IT Infrastructure, cloud based
THANKS

- Michael Cheng – Head of Information Security @ Bexar County, michael.cheng@bexar.org, 210-335-0208