Cybersecurity Showdown: Challenges and Strategies for States

Ashwini Jarral
Director of Operations
IJIS Institute
Adaptability to Technological Change

- Pace of Technological Change
- Human Adaptation
- Organizational Adaptation
- Policy Changes/Updates
Law Enforcement Data and Interaction

Next Generation 9-1-1
- 9-1-1 voice call data
- Text messages
- Still images
- Alarms/sensors
- Video links

Clock Sync

Fusion Centers

Social Media

Hospitals

Media (News)

EMS Mobile
- AVL
- Field Rpt

LE Mobile
- AVL
- Field Rpt

State LE Databases
- N-Dex
- State

Federal LE Databases
- N-Dex
- NCC

LE RMS

State EMS Databases
- N-Dex
- State

EMS RMS

State EMS RMS

NEMSIS

State LE Mobile

FD Toning

Rip & Run

Paging

Fire Mobile
- AVL

Alerting Systems
- FD Toning
- Rpt & Run
- Paging

Fire RMS

State Fire Databases
- State

Federal Fire Databases

NIFRS

Fire

State LE

Databases

LE

N-Dex

NCIC

LE

36 + Points of Interaction = 36 ++ ways to compromise Data

Connected = Risk?
Number of Reported Incidents by Federal Agencies

Number of reported incidents

80,000
70,000
60,000
50,000
40,000
30,000
20,000
10,000
0

2006 2007 2008 2009 2010 2011 2012 2013 2014

Fiscal year

Cyber Threats faced by Public Safety Agencies?

- Defaced Web Sites?
- Ransomware?
- Data Breaches?
- Compromised CJIS Data?
Threat Observations

Ransomware Attacks...

Cryptowall
Cryptolocker
Cryptoware
CTB Locker
Cryptobit
KEYHolder
Megacode

19.4% Restored from Backup
22.6% Paid for Key to Unlock
58.1% Lost Data
What do victims teach us?

We LACK good Metrics…

Federal
State
Local
Tribal
Territorial
(Attack data is not substantive)

Significant attacks of LEAs?
(IACP/CACP Research of 500 Agencies)

Majority of victims unprepared
IACP/NW3C Research; LEA Cybersecurity Challenges?

- IACP/CACP LEA Executive Cybersecurity Research 2013
- NW3C Research 2014/2015
- Observations?
  - Generally aware of the Threat
  - Understand potential Consequences
  - However, Do NOT manage Cybersecurity Risk
- Challenges?
  - Control of Infrastructure
  - Lack of Skill Sets
  - Resourcing Shortfalls

What Does this tell us about Incident Response?
Over a Billion Consumer Records Victimized in 2014

Open Security Foundation...
2014 saw 3 of the all-time worst breaches:

173 million Taxi & Limousine,
145 million e-commerce, and
104 million Credit Bureau.
Plus...
220 million Gaming sites,
1.2 billion allegedly stolen by Russian hackers

Does not include:
Target, Home Depot, JP Morgan/Chase, Anthem Health, etc...

Government Employees are Consumers...
Cybersecurity Policy

Executive Order #13636
Improving Critical Infrastructure Cybersecurity

- Develop voluntary cybersecurity framework
- Promote and incentivize adoption
- Increase cyber threat information sharing
- Privacy and civil liberties protections
- Explore the use of existing regulations

Presidential Policy Directive-21
Critical Infrastructure Security and Resilience

- Develop a situational awareness capability on how infrastructure is functioning in real time
- Understand cascading consequences of infrastructure failures
- Evaluate and mature the public-private partnership
- Update the National Infrastructure Plan
- Develop R&D plan

White House Executive Order & Presidential Policy Directive

- Implements new program across Critical Infrastructure sectors
- Sets in motion wide-ranging discussion on Cybersecurity Risk Management
Cybersecurity Needs

Simplify and enhance:

- Automated risk management integrated with continuous security testing, evaluation, and monitoring.
- Machine speed cybersecurity information sharing.
- Hardening of critical infrastructure and related technologies.
IACP Cyber Strategy:

• Identify, simplify, and address the Cyber needs of SLTT law enforcement via Executives

• Assist in the development and delivery of:
  • Webinars
  • Best practices and lessons learned
  • Model policies
  • Case studies

• Partner and Intuitively Link to Existing Resources
Thank You