2018 International Information Sharing Conference

Improving the Value of Information Sharing

Geographically-Based Community ISAOs

2018 International Information Sharing Conference

Dr. Greg White
Executive Director
ISAO Standards Organization

Geographically-Based Community ISAOs

EO 13691 described several possible types of ISAOs

“ISAOs may be organized on the basis of sector, sub-sector, **region**, or any other affinity, including in response to particular emerging threats or vulnerabilities. ISAO membership may be drawn from the public or private sectors, or consist of a combination of public and private sector organizations. ISAOs may be formed as for-profit or nonprofit entities.”

Geographically-Based Community ISAOs

At last year’s IISC the ISAO SO stated that it felt that the “sweet spot” for ISAOs in the coming years.

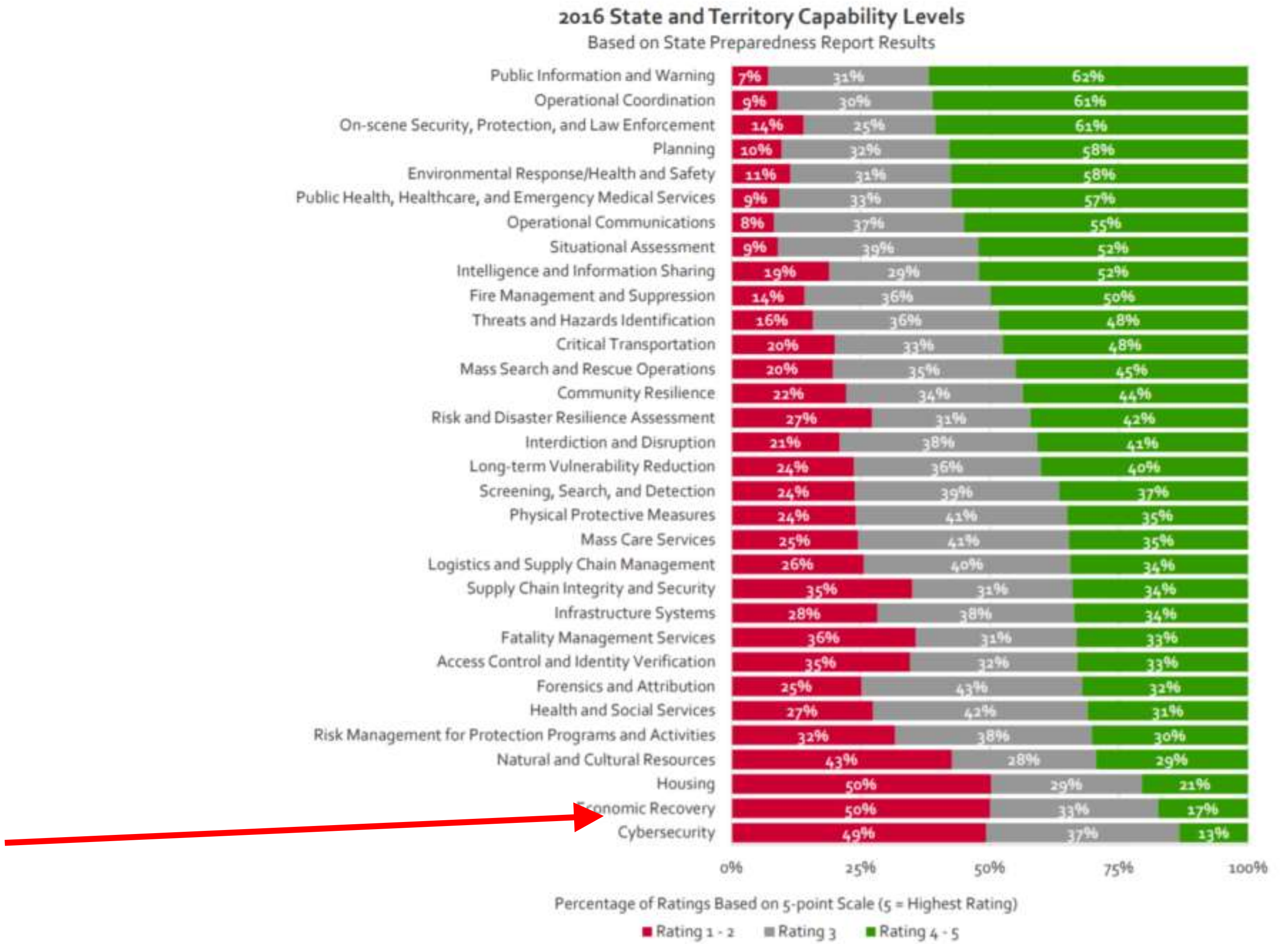
- Help to build trust between organizations
- Raise awareness on Cybersecurity issues especially for SMBs
- Encourage more public/private partnerships
- Encourage information sharing between sectors within the SLTT

Cyber implications at the state and local level

- Subject to growing number of cyber attacks
  - More high-profile attacks on states
  - Loss of millions of citizens PII
    - Social security numbers
    - DOB
    - Drivers license numbers
    - Payment card records
    - Tax data
  - These incidents have cost millions of dollars in clean-up costs, loss of revenue and public trust

DHS National Preparedness Report 2017

2018 International Information Sharing Conference



2016 State and Territory Capability Levels

Based on State Preparedness Report Results

Figure 4. States and territories reported the highest capability ratings in Public Information and Warning and the lowest capability ratings in Cybersecurity and Economic Recovery.

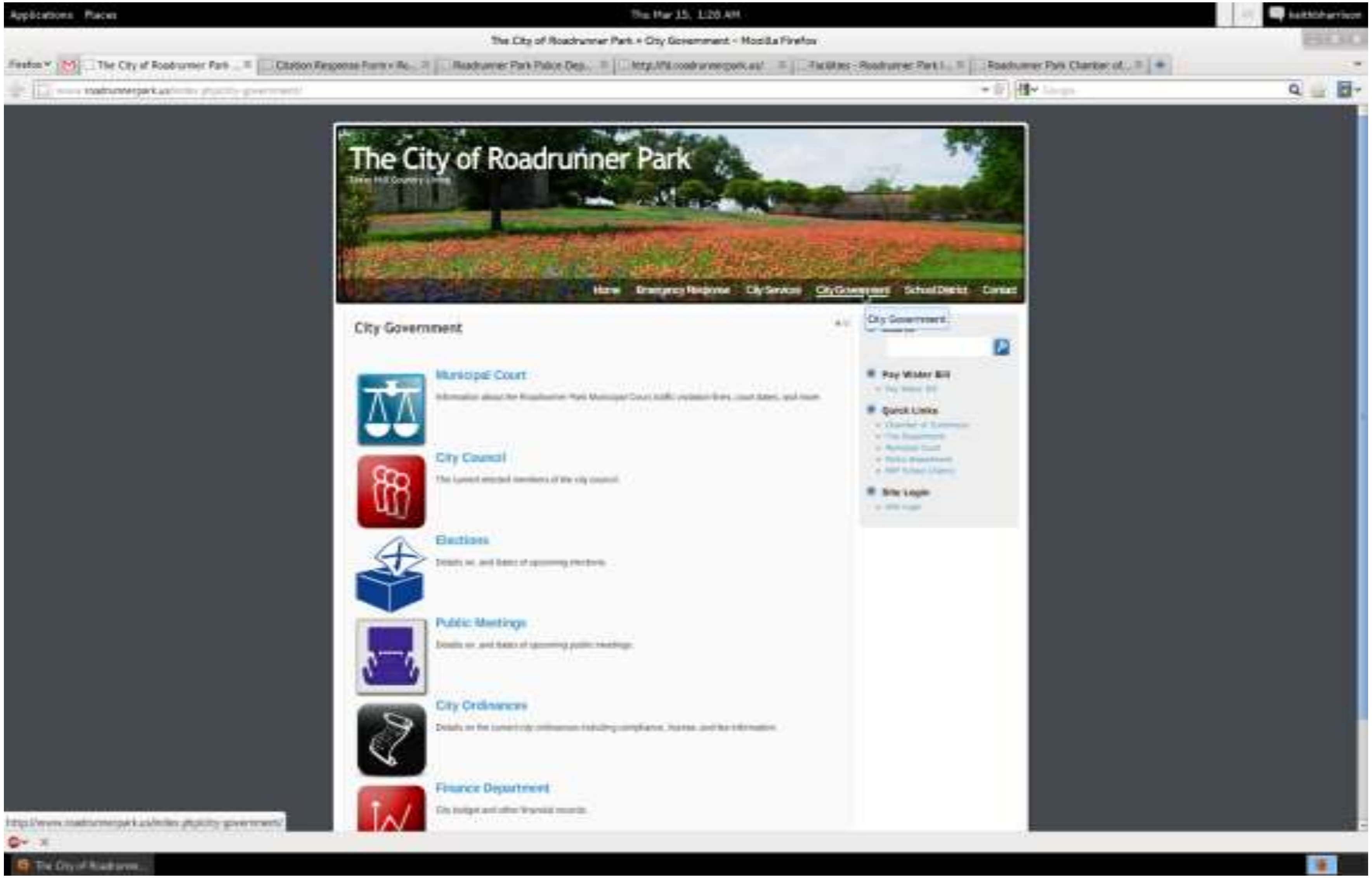
Cyber implications at the state and local level

- No clear strategy to implement a cybersecurity program for local jurisdictions
  - Cybersecurity threat is not understood
    - What is the scope of the cyber threat?
    - How can it impact a community?
    - Traditional incident response personnel in a community including Emergency Management generally do not understand the threat cyber attacks pose.
  - Roles are not understood
    - Who in the community should be involved?
    - How can the public and private sectors work together?
    - What can the federal government provide for you?

Why Information Sharing is Important Across an SLTT

- UTSA has conducted research into community incident detection and response since 2012
- Developed a “Honey Community” to gather data on attacks on a small community
- Patterned our website after a number of other small community websites in Texas
- Connected to the Internet and sat back and watched…

Our Original Honey Community


Applications Places
Thu Mar 15, 1:20 AM
The City of Roadrunner Park » City Government - Mozilla Firefox
Firefox
The City of Roadrunner Park ...
Citation Response Form « Ro...
Roadrunner Park Police Dep...
http://fd.roadrunnerpark.us/
Facilities - Roadrunner Park I...
Roadrunner Park Chamber of...
www.roadrunnerpark.us/index.php/city-government/
The City of Roadrunner Park
Home
Emergency Response
City Services
City Government
School District
Contact
City Government
http://www.roadrunnerpark.us/index.php/city-government/
The City of Roadrunner...

City Government

Municipal Court

Information about the Roadrunner Park Municipal Court, traffic violation fines, court dates, and more.

City Council

The current elected members of the city council.

Elections

Details on, and dates of upcoming elections.

Public Meetings

Details on, and dates of upcoming public meetings.

City Ordinances

Details on the current city ordinances including compliance, license, and fee information.

Finance Department

City budget and other financial records.

- **Pay Water Bill**
  - Pay Water Bill
- **Quick Links**
  - Chamber of Commerce
  - Fire Department
  - Municipal Court
  - Police Department
  - RRP School District
- **Site Login**
  - Site Login

Looking across multiple sectors is critical

Number of Sectors	Identified Attacks
*	1,402
1	1,430
2	151
3	52
4	16
5	9

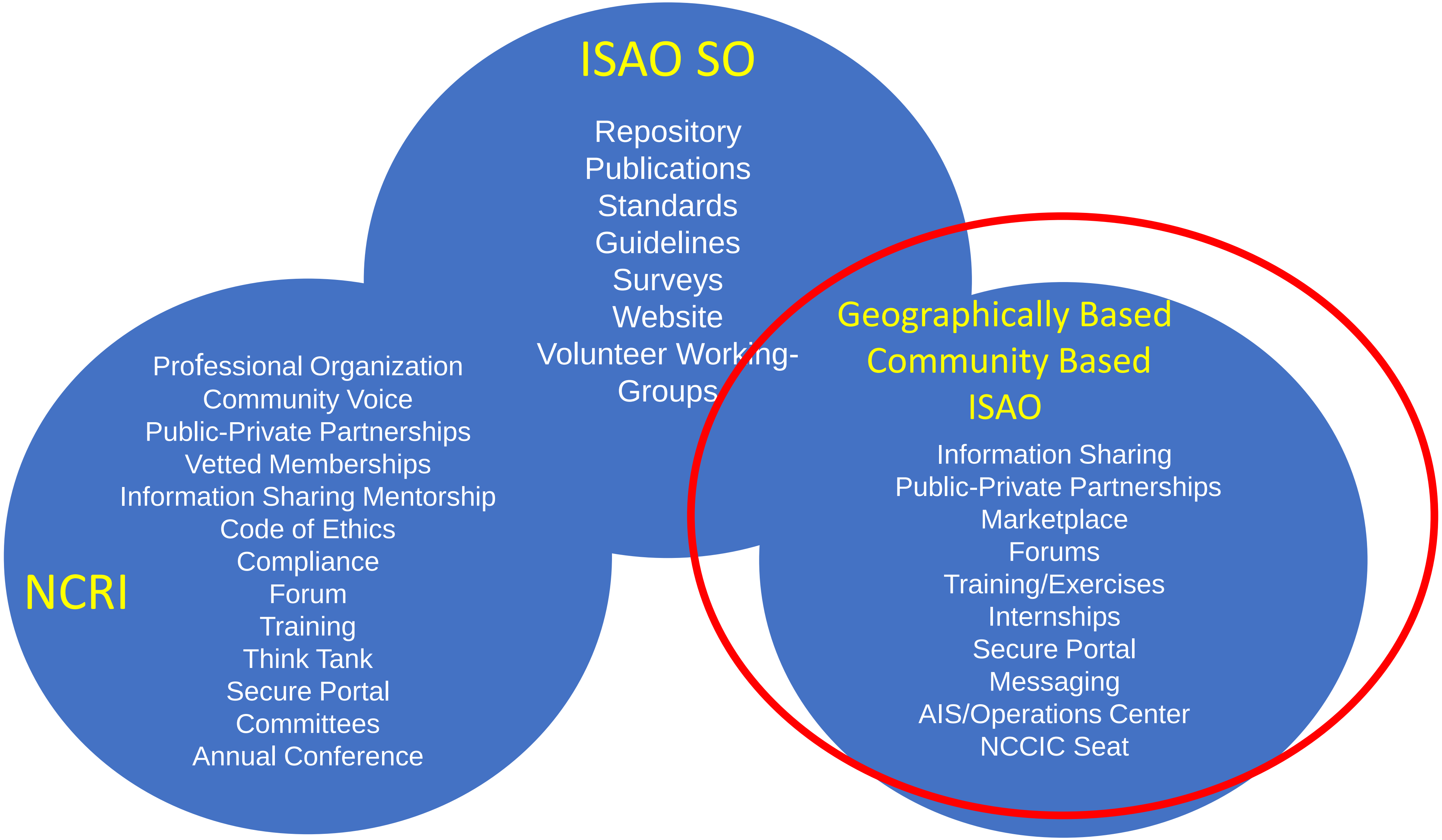
Sector	Identified Attacks
Community	2,319
Water and Sewer	369
Criminal Justice	345
Emergency Response	398
Education	381
Commerce	504

- 3,060 IDS alerts generated by SNORT
- 55% of attacks can be seen as an attack on 1 or more sectors
- 45% of attacks were not attributed to a sector but the effort could be seen across the entire enterprise (the * entry above)
- Attacks against 1 sector appeared to re-appear later against another sector

Harrison, Rutherford, and White. "The Honey Community: Use of Combined Organizational Data for Community Protection." *System Sciences (HICSS), 2015 48th Hawaii International Conference on*. IEEE, 2015.

Information Sharing Trifecta

GBC·ISAOs
GEOGRAPHICALLY-BASED COMMUNITY ISAOs



ISAO SO

Repository
Publications
Standards
Guidelines
Surveys
Website
Volunteer Working-Groups

NCRI

Professional Organization
Community Voice
Public-Private Partnerships
Vetted Memberships
Information Sharing Mentorship
Code of Ethics
Compliance
Forum
Training
Think Tank
Secure Portal
Committees
Annual Conference

Geographically Based Community Based ISAO

Information Sharing
Public-Private Partnerships
Marketplace
Forums
Training/Exercises
Internships
Secure Portal
Messaging
AIS/Operations Center
NCCIC Seat

Questions?

Gregory B. White, Ph.D.
Greg.white@utsa.edu