

# Bringing Data to Life

Presented by Michael Echols



# DHS Responsibilities



Emergency  
Communications  
Capabilities



Secure *dot-gov*



Assist in Protecting  
*dot-com*



Assist in Securing  
Critical Infrastructure



National Security  
Communications



Coordinate Cyber  
and Communications  
Incident Response

# Cyber and Communications Ecosystem for the Future

## Today

- Many unknown vulnerabilities
- Incidents spread at network speed and defenses are manual
- Many attacks are undetected
- Independently defended systems
- Inconsistent security policies
- Users do not follow best practices
- Attacks increasing in number and virulence

## Future

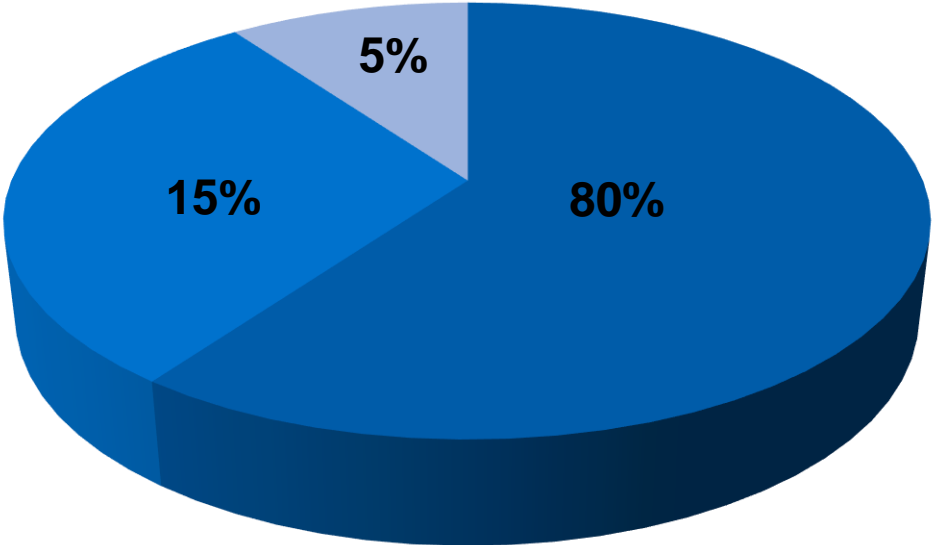
- Baked in security = fewer vulnerabilities
- Near real-time response with more automated defenses
- Many attacks, but less impact
- Information sharing and increasingly collaborative defenses
- Consistent security practices
- Unauthorized activity quickly identified
- Visualize cybersecurity
- Ability to learn and adapt defenses in near-real time

*Emerging nexus between cyber and physical will continue to grow*

*Adversaries will continue to have robust and evolving capabilities*



# Cyber Risk Management



- **Best Practices**
- **Information Sharing**
- **Incident Response**

# Best Practices

Cybersecurity Framework

Critical Infrastructure Cyber Community  
(C<sup>3</sup>) Voluntary Program

Risk Assessments

Cyber Resiliency Review

Joint Information Bulletins

Public Private Partnerships

[www.us-cert.gov/ccubedvp](http://www.us-cert.gov/ccubedvp)

# Improving Awareness

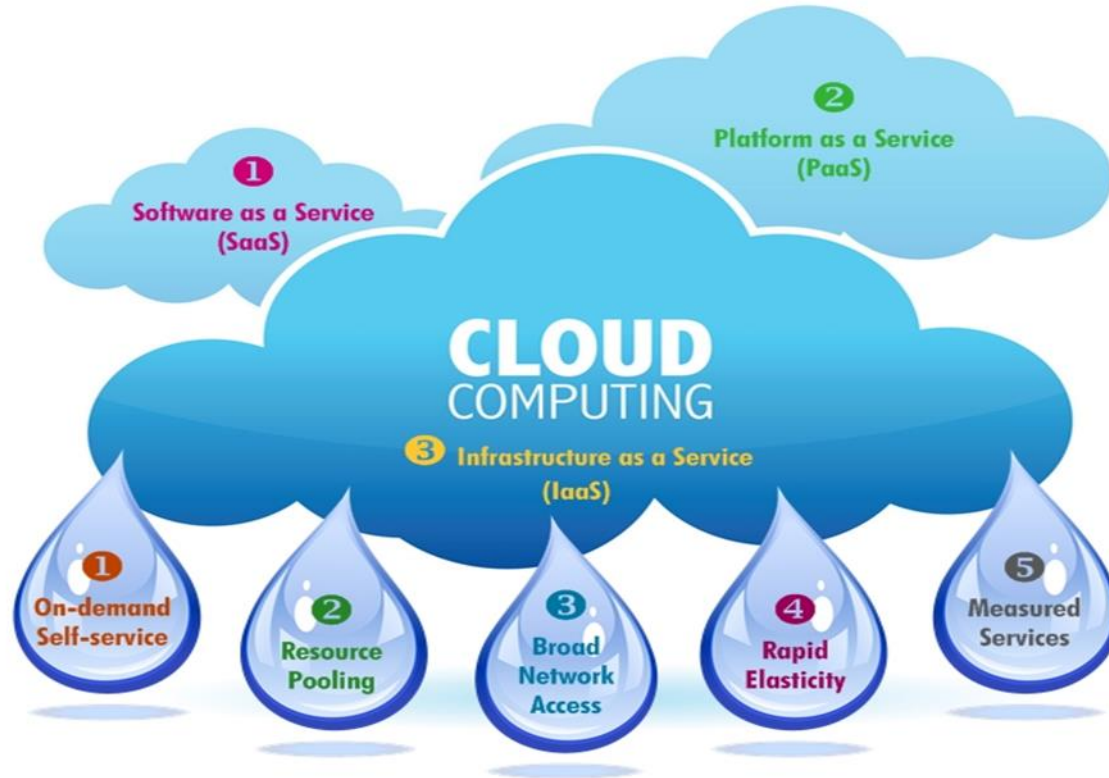
- The President tasked the Department of Homeland Security (DHS) to build and manage a new Information Sharing and Analysis Organization model (ISAO model), under Executive Order 13691 (ISAO E.O.).
- A new ISAO model is the next step in the information sharing maturity process.
  - Enhance the Nations cyber defenses by adding a new layer of network defense, expands sharing relationships beyond traditional CIKR Sectors down into the fabric of America, and expands potential partnerships with private sector entities.
  - Build upon the foundation established by Executive Order 13636 – Improving Critical Infrastructure Cybersecurity.
- The ISAO E.O. advances DHS' Cybersecurity and Communications (CS&C) efforts to assist private sector partners in building their cybersecurity capacity and resilience.

## Motivation or Lack of.....

- *As cybersecurity incidents multiply in frequency and cost, the cybersecurity programs of US organizations do not rival the persistence and technological prowess of their cyber adversaries.*
- *Organizations do not adequately address employee and insider vulnerabilities, nor do they assess the security practices of third-party partners and supply chains. Most do not strategically invest in cybersecurity and ensure that it is aligned with their overall business strategy.*

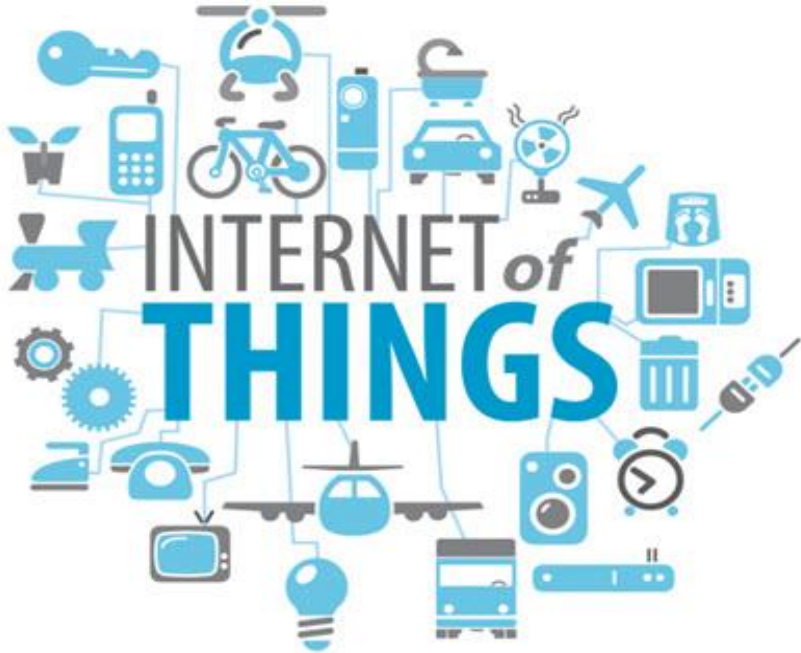


# Cloud Computing





# Connecting Everything



- Smart Parking**

Monitoring of parking spaces availability in the city.

- Structural Health**

Monitoring of vibrations and material conditions in buildings and bridges.

- Traffic Congestion**

Monitoring of vehicles and pedestrian levels to optimize driving and walking routes.

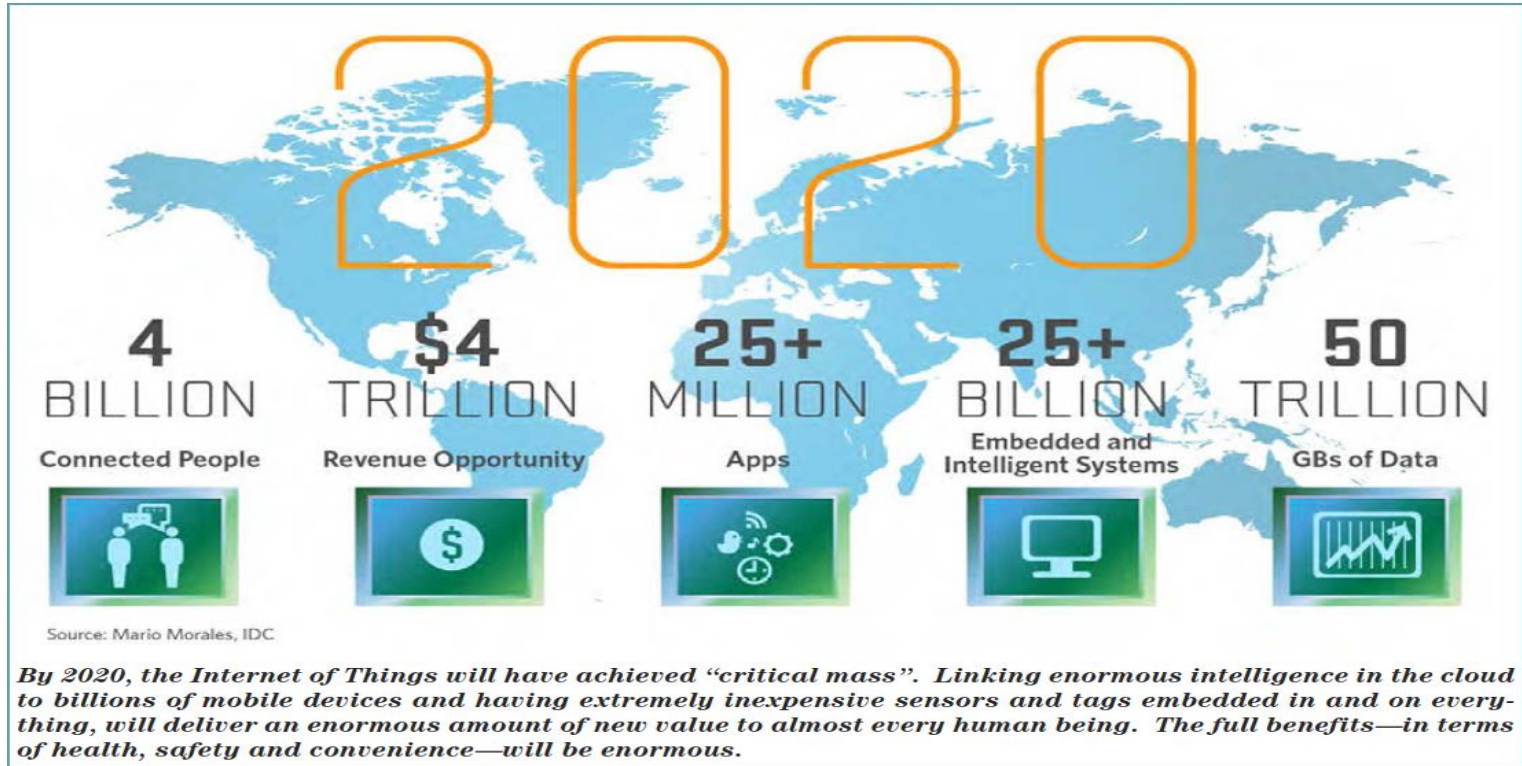
- Smart Lighting**

Intelligent and weather adaptive lighting in street lights.

- Smart Roads**

Intelligent Highways with warning messages and diversions according to climate conditions and unexpected events

# Internet of Everything



# People Problem



# Awareness



Analytics is defined as the scientific process of transforming data into insight for making better decisions.

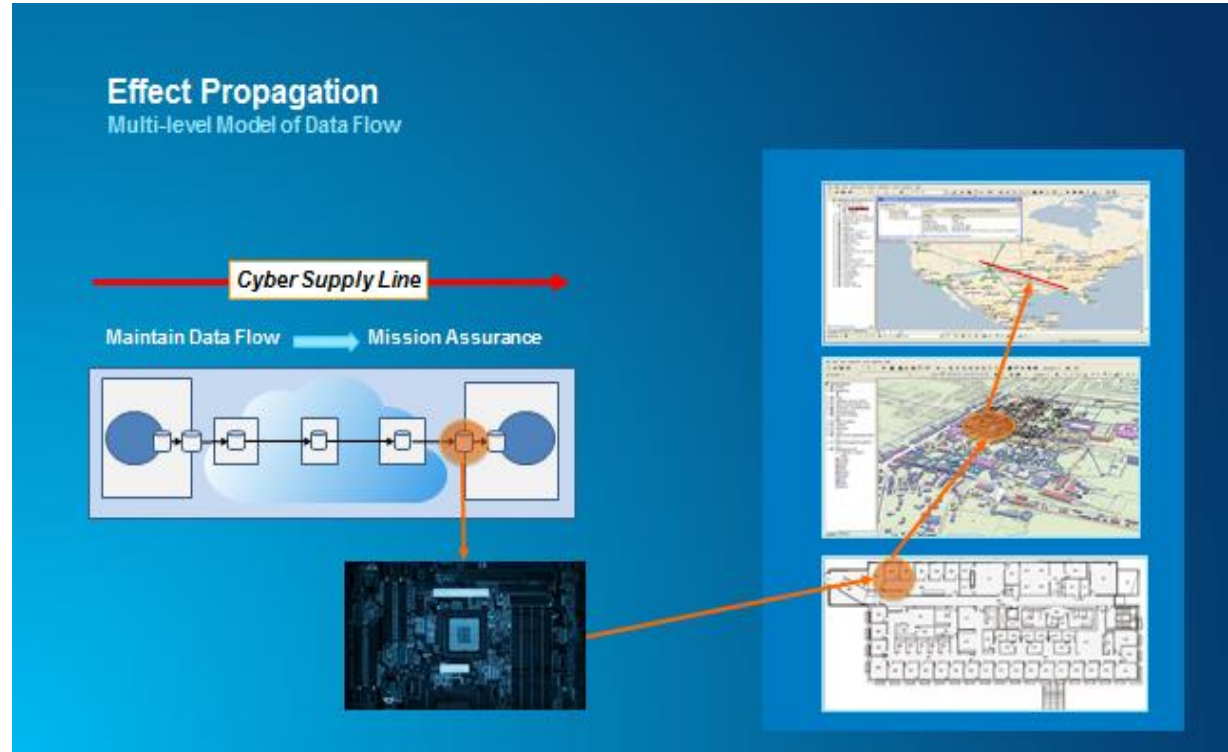
Data Analytics is critical to meeting the challenge our adversary is launching. We must however, make the data come to life to take advantage of the data.



# Bringing Analytics to Life

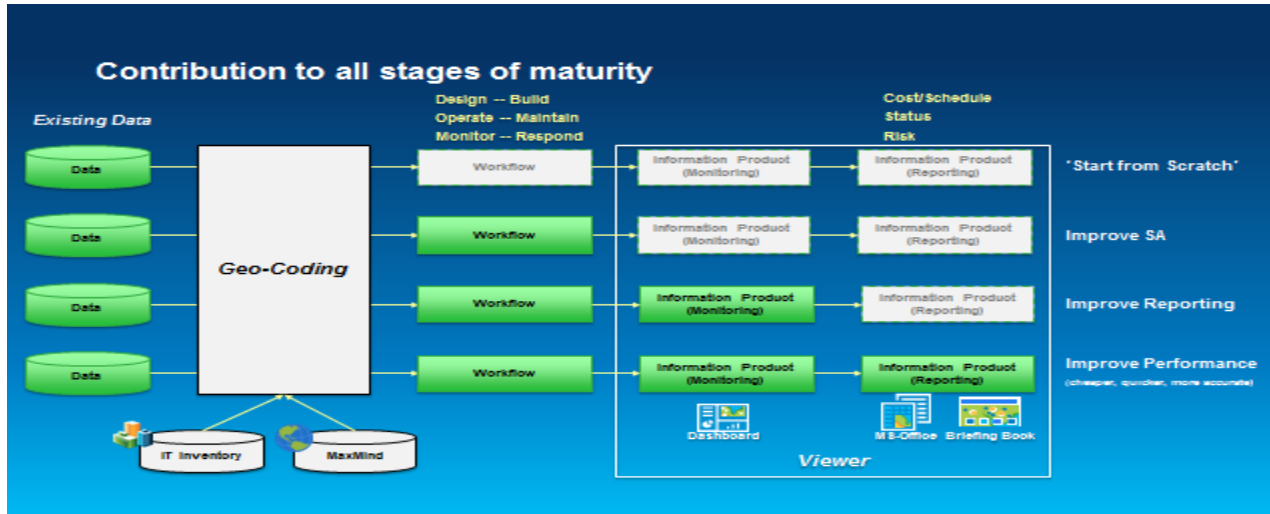
Entities are concerned about timely, actionable information

- Develop tool to assist analysts
- Measure effort
- Realize that making changes causes impacts to flow through community
- Assist with network defense
- Recognize the time it takes to know information
- Time it takes to be informed of information
- Time it takes to make information actionable



# Why does it matter?

- A logical map: what does the network look like?
- How are they connected?





# Perspective

- Visual display with contextual management will be a key to delivering a higher level of resilience.
  - Effects on trust
    - Decrease in false positives
    - Signal/noise ratio
  - Reallocating resources
    - Analysts become bored with lines of data and code review now let machines do machine work and humans do human work.
- A new paradigm for security awareness will also assist with the challenge of cost effective security management. And, eventually we will gain a handle of the cyber threat we face as a nation.

## Contact Information

Michael Echols

Michael.Echols@hq.dhs.gov

Director, Cyber JPMO

Department of Homeland Security



# Questions

Please wait for the **microphone** before asking your questions



State your **name & organization**

# Please don't forget to...

Complete the Survey for this session



The Power of Data  
DECISION READY IN REAL-TIME

## Evaluation Form (Seminar Location - Date)

Name: \_\_\_\_\_ Company: \_\_\_\_\_

Email: \_\_\_\_\_

Quality and content of the presentations	Poor	Good	Excellent	N/A
Welcome	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The Journey To Real-Time Operational Intelligence	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The Power of Connection	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tank Level Management System	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Using the FI System to Aid in Troubleshooting Operational Aspects of Oil and Gas Well Drilling and Completion	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Unleash your Infrastructure	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Information on the Spot	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Wrap-up/Seminar Conclusion	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<b>Quality and organization of the seminar</b>				
Choice of date	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Time allowed for lunch/breaks	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Choice of presentations	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Break and time allowed for the presentation	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>