Law Enforcement Agencies, Intelligence & The Big Data Challenge

Threat Prediction & Prevention

Steve Stennett
US Federal Information Management Brand CTO
International Business Machines (IBM)
Today’s Discussion
If you only remember four things

1. **Intensifying mission & threat pressures coupled with and explosion in Big Data have pushed agencies to a tipping point**

2. **Many leaders embrace this – defining the new requirements and are demonstrating success**

3. **Achieving transformation requires a broad set of capabilities and a combination of technology and expertise**

4. **Act Now – best practices, patterns, and assets exist to help you define a strategy and a roadmap to guide your transformation**
The Big Data Challenge…

*Big Data Is An Explosion In Volume, Variety, Velocity, & Veracity*

We create 2.5 Quintillion bytes, or 2.5 Exabytes of data each day — so much that 90% of the data in the world today has been created in the last two years alone.

“We have for the first time an economy based on a key resource [Information] that is not only renewable, but self-generating. Running out of it is not a problem, but drowning in it is.”

- John Naisbitt

**Volume**

- 50 X growth in the volume of data to 25 Zettabytes by 2020

**Velocity**

- 30 Billion RFID sensors and counting

**Variety**

- 80% of the world’s data is unstructured

**Veracity**

- 1 in 3 business leaders don’t trust the information they use to make decisions

“For every 1 minute in Realtime, 60 hours of video is uploaded to youtube”

Time Magazine, “Is You Tube Too Big To Fail?”, 2012

© 2013 IBM Corporation
Big Data at the Speed of Business

Big Data Creates A Challenge – And an Opportunity
What If You Could...

Traditional                Big Data Approach

Leverage All of the Data
Captured

Reduce Effort
Required to Leverage
Data

Let Data Lead The Way, and
continuously explore

Leverage data as it is
captured – In Motion
(Real-Time Analytics)
The Thorny Issue of Identity Only Makes It Harder…
Multiple Levels Of Identity Ambiguities

Intermediaries, Introducers, Beneficiaries,

Nefarious Un-Identified Third Parties

Data Degradation / Data Drift

Data Islands/Silos

Name / Address / DOB Deception

Maiden Names, Deaths, Moves, New Accounts

Name Order, “Maria del Carmen Bustamante de la Fuente”

Phonetic Transposition Errors, Lester - Leicester

Multiple Titles, Prefixes
Dr., Rev, Haj, Sri., Col Abdul, Fitz, O’, De La

Online & Remote Interaction

Nicknames:
Hammed, Mogs

Multiple Name Variants
Today’s intensifying challenges mandate a fresh approach to managing information

Intensifying operational tempo, and frequency of incidents

New sense of urgency around Insider Threat

Incidents & Threats are becoming increasingly asymmetric

Threats increasingly cross theater

Social Media and “Big Data” playing an increasingly important role

All that is true physically, is true in Cyber

Internet enabling “Open Source” Non-traditional collaboration

Transparency is clouding

Citizen, Policy Maker and Regulatory expectations and pressures are increasing

Traditional Approaches have become obsolete

Information is still in silos – lack of full integration obscures visibility

Limited Sharing, but evolving

Untimely – Sense & Respond vs. Predict & Act

Query State limits ability to address complexity of threats in real time

Acute issues around “Veracity” of data – deceptive identities and unreliable sources

Inability to manage and search across an expanding array of unstructured data sources

Inability to link unstructured content with structured data and manage together

Cutting through the clutter – mass visualization and bringing the data to the analyst and to the battlefield
Smarter Agencies Leading The Way – Think Big – Start Small
Optimize decision making with actionable insights

All perspectives
Past (historical, aggregated)
Present (real-time)
Future (predictive)

All people
All departments
Experts and non-experts
Executives and employees
Partners and customers

All decisions
Major and minor
Strategic and tactical
Routine and exceptions
Manual and automated

From structured, linear, repeatable, Push, IT-driven, information delivery, at rest
To creative, dynamic, iterative, autonomic, persistent, business-driven, in motion

All information
...analytics is moving closer to the data
Leading the Way

Government Leaders Moving to Address These Challenges

Streamlined Information Sharing Across Fed and Local Agencies

Child Predator Investigation

Protecting the homeland

Insider Threat & Physical Security

Insider Threat

Centralized Screening Database

Western National Law Enforcement

Registry of Identities, Objects and Events

Automated content extraction, entity resolution and analysis from seized assets

Connect the dots, predict and prevent threats

Perpetual credentialing and vetting across branches and bases

Proactive enterprise data activity monitoring & extrusion prevention
Leading the Way
Government Leaders Moving to Address These Challenges

- **Warfighter Care**
  - DARPA
  - Greatly reduced frequency and severity of Traumatic Brain Injury

- **National Border & Security**
  - TerraEchos
  - State of The Art covert surveillance system based on Streams platform

- **Crime Prediction & Prevention**
  - Police Department City of New York
  - Real time Information Sharing, Discovery & analysis

- **National Borders & Security: Cyber Security**
  - BROCADE
  - Real time network intrusion detection, sub-millisecond analysis and response

- **Crime Prediction & Prevention**
  - Memphis Police Department
  - 30% Reduction in Violent Crime

© 2013 IBM Corporation
Maritime Situational Awareness

Adversaries are unlikely to attempt conventional force-on-force conflict and, to the extent that maritime forces could be openly challenged, their plans will almost certainly rely on asymmetric attack and surprise, achieved through stealth, deception, or ambiguity.

A Cooperative Strategy for 21st Century Seapower
Today’s Discussion

1. **Intensifying mission & threat pressures coupled with and explosion in Big Data have pushed agencies to a tipping point**

2. **Many leaders embrace this – defining the new requirements and are demonstrating success**

3. **Achieving transformation requires a broad set of capabilities and a combination of technology and expertise**

4. **Act Now – best practices, patterns, and assets exist to help you define a strategy and a roadmap to guide your transformation**