GFIRST 2012 8th Annual National Conference
August 19-24 | Atlanta Marriott Marquis | Atlanta, Georgia

Operationalizing Data:
An Intelligent and Systematic Approach

Cory Mazzola, Cyber Systems

Gerald Derrick, Cyber Systems




GENERAL DYNAMICS
Advanced Information Systems

Agenda

- **Overview**
  - Current state
- **Problems**
  - Common problem sets
  - Issues and pitfalls
- **Solutions**
  - System based solutions
  - Centralized information flow
- **Thoughts & Ideas**

Does this sound familiar?

You, as a seasoned cyber analyst, arrive at work for your shift and during the morning "changing of the guard" are assigned to finish working on a tasking that an analyst from the previous shift was working on. Unfortunately, that analyst had to leave 30 minutes early and didn't realize the pass on email never made it out of his outbox. Oh, and to make things even more fun phones are ringing off the hook with calls about monitors suddenly displaying the screen upside down…

What do you do?

Your Options

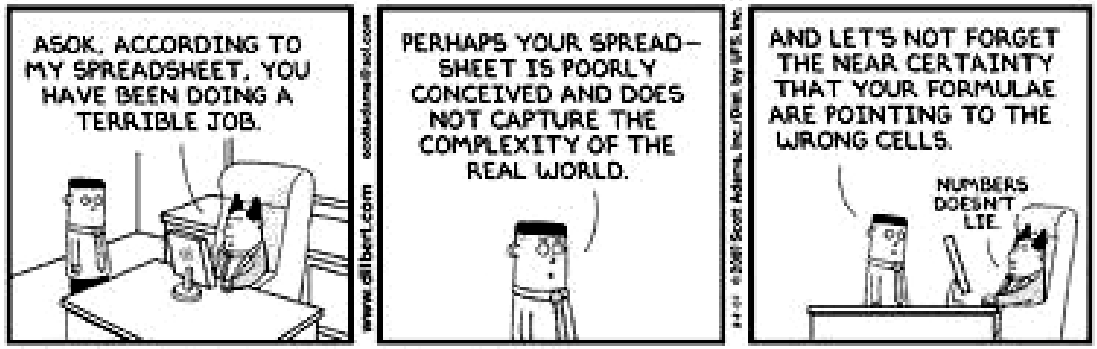
- Ask around to see if anyone else received his email
- Look blankly at your inbox for the next 8 hours
- Start working the tasking from scratch
- Tell all the callers to turn their monitors upside down and call the next shift
- Access a centralized data and workflow repository

30,000 Foot View of Problem

- Disparate data sources and systems
- Lack of proper system capabilities or tools
- Problem isn't getting smaller
- Finite resources/people
- Mission often dictates/derails workflow
- Analysis often can't be finished
- Lack of enterprise situational awareness

10,000 Foot View of Problems

- Threats constantly changing
- Data access/aggregation issues
- Managed workflow and information silos
- Too much data and the "drive-by tasking"



Proposed Solutions

- **Operationalize data**
  - Put data at your fingertips
    - Centralize data and process flow
    - Make data readily available and searchable
    - Googlize logs, audit data, system info

Best Practices – Holistic Approach

- **Organizational makeup**
  - Integrate organization and operations
    - Physically and logically
    - Process – People – Technology
      - *People, Systems and how they interact*

        (Carnegie Mellon ISSM)

Swingsoftware

Process

- **Build process flow around information sharing and enterprise flow**
  - Institutionalize operating divisions/sections
    - Disallow single points of failure if possible
    - Ensure group comms (distros/paths/etc.) are in place and properly resourced
  - Ensure hooks bridge leadership and disparate mission areas
  - Shift pass-on's / team meetings / etc.
    - Regular meetings with key stakeholders/essential personnel

People

- **People do not scale**
  - Number of network flows and data may not conform to people
  - Need technological solutions to augment, support, automate, etc.

Eticorporate.com

People

- **Floor charts matter**
  - Facilitate face-to-face information exchange
- **Group similar mission sets**
- **Cross Functional Synergy**
- **Ensure leadership is close and accessible**

Technology

- **Map enterprise mission requirements and strategic objectives –>**
  - Then design and develop technology solutions to fit

Technology (cont.)

- **Data information management**
  - Aggregate and index data
    - Ensure data stores are accessible/queryable
  - Build capabilities off of ‘data’ and not technology

Enhanced System Design

- **Leverage information and system resources**
  - Intelligent design
    - Develop systems with an intelligent, methodical, holistic approach in mind
    - Integrate information repositories
    - Provide one-stop search and reporting capabilities
      - Centralized front-end
        - *TOSS-IT*
    - Include auto-caching workspaces (reduce silos)
      - Instant indexing
      - Information on-demand
      - Expanded search/correlation capability

Leverage Data and Resources

- Single authoritative data source
- Automated analysis and reporting
- Data cubes
- Machine learning
- Tool and platform agnostic
- A picture is worth a thousand words

Goal is to enable the analyst….

Step Outside of the Box

- **Leverage partnerships**
  - What resources are available in-house?
    - Sister organizations
    - Internal departments
    - Personal / professional relationships
  - What resources are available externally?
    - Professional associations and organizations
      - *GFIRST-JACKE, FIRST, ISSA, ACM, etc.*
    - Research groups / projects / whitepapers
    - Commercial and professional services
    - Open / closed sources
    - Private Partners

Scope & Focus

- **Identify and inventory critical systems**
  - Focus resources where it matters
  - Scope program resources and selectively target efforts

Considerations

- **When mapping requirements:**
  - Involve key stakeholders
    - Socialize and secure management buy-in
    - Ensure all necessary departments and mission areas are represented
  - Roadmap implementation/adoption plans
    - Policy and technology rollout
    - Map timelines

Takeaways

- **Identify and address common problems/challenges**
- **Evaluate/focus on Process – People – Technology**
  - Integrate enterprise capabilities
  - Leverage existing systems/infrastructure
  - Centralize data/information stores
- **Where do we go from here?**

Questions

???