INFORMATION EXCHANGE FRAMEWORK

POLICY-DRIVEN, DATA-CENTRIC INFORMATION SHARING AND SAFEGUARDING (ISS)

SUPPORTING CYBER SITUATIONAL AWARENESS

September 2016
DISCUSSION OBJECTIVES

1. Can the approach and technology being employed on the Information Exchange Framework be adapted to address cyber challenges (e.g., Information Sharing and Safeguarding)

2. Benefits of the approach

3. Approach / Roadmap
The ability to maintain cognizance or awareness of the pertinent elements and events in the environment in order to effectively conduct operations and achieve desired outcomes.
The ability to maintain cognizance or awareness of the pertinent elements and events in the environment in order to effectively conduct operations and achieve desired outcomes.

Network Awareness

Threat / Risk Awareness

Mission / Operational Awareness
IEF Focuses On
Maximizing the availability of quality information for authorized users, while simultaneously protecting sensitive data from unauthorized access, manipulation and release.

Provide this Capability At Machine Speeds In Real-World Timeframes
User wants Information that has the following qualities:

- Timely
- Accurate
- Current
- Actionable
- Complete
- Concise
- Accessible
- Relevant
- Consumable / Understandable
- Reliable
- Trusted

**Information:**

1. Data in context
2. Data that informs decisions

Right Information, Right Person, Right Time
SITUATIONAL AWARENESS CHALLENGE
Is An Information Sharing and Safeguarding Challenge

Data Rich - Information Poor
Providing Information that informs decisions (Actionable)

Delivering the “Right Information – Right Person – Right Time”
Achieving a Historic and Future Requirement

Increasing the Willingness of Internal/External Partners to Share Information
Both Partners Inside and Outside an Organization are Reluctant to Share Cyber Information
Change Culture across a Broad Community of Partners
Require Policy that Authorizes the Sharing of Cyber Information

Adapting to Change
Threats Change, Missions/Operations Change, Partners Change, Policies Change
No plan survives first contact with adversaries

Designing Capabilities and Solutions for Tomorrow’s Requirements
The only constant about ISS requirements is change
Flexibility, Agility, adaptability and sustainability need to be architected into ISS solutions
BUILDING BLOCKS OF A SA STRATEGY/SOLUTION

1. Separation of Concerns
   - Policy Development separated from Application/System Development
   - Best Practices for the Development & Management of the Policies governing ‘access to’ and the ‘release of’
     data and information elements (translation of policy into machine executively rules and constraints)

2. Policy-driven Data-centric Information Sharing and Safeguarding (ISS)
   - Traceability from Policy Instrument to Implementation
   - Defence in depth (Securing the data (‘THE ASSET’) vs. the networks, platforms, infrastructure and
     applications)
   - Increased flexibility, agility and adaptability
   - User (Data Owner) control over the release of information

3. Open Standards (Community Accepted Specifications)
   - Access to industry leading practices and knowledge
   - Higher levels of interoperability
   - Competitive Procurement / Multiple vendors and integrators
   - Shared (common) services, platforms and infrastructure (Available through multiple sources / vendors,
     Interoperable)
   - Risk Mitigation

4. Integration of User Solutions and Infrastructure
There is a lot more to the delivery of interoperability than Semantics defined by the common canonical information models (e.g., NIEM, CAP, EDXL, etc.)

The Information Exchange Framework (IEF) is seeking to:

- Align the required capability
- While leveraging the user’s own services and infrastructure
SELECTIVE SHARING OF CONTENT
SECURITY / TRUST / QOS / ...

Low Trust

Moderate Trust

High Trust

Information Packaging & Processing Services
SHARING USING DIFFERENT PROTOCOLS

Foundation Layer
Links policy model to Physical Data Element

Transactional Layer
Defines rules for aggregating, transforming, marking, and redacting data and information elements in conformance to policy instruments.

Semantic Layer
Groups the datasets into meaningful and releasable datasets

IES Layer
Aligns the information to its format/protocol and the agreed/authorized distribution channel

Protocol Data Unit
NIEM XML
JSON Exchanges

Canonical Data
Community Focus
Local Focus

Copyright by Advanced Systems Management Group Ltd. 1999-2016
Mike Abramson
Special Adviser on public safety/security Open Interoperability Standards to Centre for Security Sciences (CSS)
Co-Chair C4I DTF
Chair IEF WG
President Advanced Systems Management Group (ASMG) Ltd.
265 Carling Ave, Suite 630, Ottawa, Ontario, K1S2E1
Fax: 613-231-2556
Phone: 613-567-7097 x222
Email: abramson@asmg-ltd.com
IEF OBJECTIVES

1. **Separation of Concerns**: Separate the development and management of ISS rules from the technology needed to enforce it.

2. **Policy-driven Data-centric Information Sharing and Safeguarding**: Automating ISS to individual data and Information Elements.

3. **Selective Sharing of Information**: Elements between users based on explicit rules and constraints mapped to policy instruments and trust profiles.

4. **Rapid Adaptation**: To ISS to accommodate changes in operational context (threats, missions, partners, roles, ...).

5. **Raise Stakeholder Trust Levels**: Through explicit capture of ISS policy, integrated into architecture, and governance.
ENABLE MULTIPLE EXCHANGE CAPABILITIES AND USER CAPABILITIES

Packaging policy derived from local policy instruments:
- Legislation
- Regulation
- MOUs
- SLAs

Processing Policy

Processing & Processing Service

Middleware PEP

Releasable content mapped to published canonical model (e.g., NIEM)

Policy Management

Packaging & Processing Service

IM PEP
WEB PEP
Email PEP
File Share PEP

Policy Management

Middleware

Middleware PEP

Middleware PEP

Packaging Policy

Middleware

Data

Data mapped to local data structures, taxonomies, and vocabularies

Data mapped to local data structures, taxonomies, and vocabularies

Access / Release Policy

Access / Release Policy

Access / Release Policy

TrustMark Registry

TrustMark Registry

ICAM

ICAM

Copyright by Advanced Systems Management Group Ltd. 1999-2016
IEF – IMPLEMENTATION GOALS

• **NOT a rip-and-replace capability:** Leverage existing investments in infrastructure and systems, providing an efficient mechanism to integrate and interoperate

• **Eating the elephant in small bites:** Approach encourages incremental implementation

• **Customer Self Served:** Add new data, data sources, policies and rules as needed

• **Maturity and Risk controls:** Implementation pace aligned with organizational maturity and risk tolerance
IEF Services

1. Application integrated Labeling Services
2. Gateway to Client Infrastructure:
   a) Domain Management
   b) Identity Management (Privilege Management)
   c) Secure Storage
   d) Identity Query
   e) Crypto (Symmetric Key)
3. Policy Enforcement for off-the-shelf:
   a) File Client/Server
   b) Email Client/Server
   c) Web Services
   d) Instant Messaging Client/Server
   e) Middleware Services
4. Decision Support Services
5. Communications layer (XMPP)To services (not data) Separate data from control
6. Logging and Audit services
7. Policy Management and Administration
WHY OPEN STANDARDS

• Targeting open standards will lower total costs (TOC) and increase returns on investment (ROI) by providing the following benefits:
  • Increased Levels of Interoperability
  • Vendor neutrality / Competition
  • Efficient use of existing resources
  • Greater use of automation
  • Increased Flexibility and Agility
  • More options provide more opportunities to optimize
  • Lower and manageable risk
  • Robustness and durability
  • Higher Quality
  • Increase available skills
  • Reduced Life-cycle Cost

• Open Standards will enable users to address unique operational needs, while enabling interoperability with partners

• Provide access to subject matter expertise that is not locally available
COMMUNITY CHALLENGES

• Acquisition & Development
  • Developing a comprehensive Specifications
  • Overlapping and conflicting Requirements from Regulations, MoUs, SLAs, and Operating Procedures
  • Rapid change
  • Avoid Vendor lock-in
  • Cost and Risk

• Operations
  • Balancing Information Sharing with Information Safeguarding (Need-to-Share vs. Need-to-Know)
  • Machine speed control over information access and release
  • Rapid change (e.g., information needs, threat, Risk, severity, scope & technology)
  • Rapid changes in Operational Partners, Roles, Responsibilities and Trust
  • Machine speed Tagging and Labeling
  • Data Quality / Quantity
  • Reduce Cost and Risk
  • Expanding technology footprint

Gathered during workshops and information sessions with US & international Government, Academia & Private sector organizations
COMMUNITY CHALLENGES

• **Support and Maintenance**
  • Managing Change
  • Flexible & agile development
  • Aging – IT
  • Retention of Institutional Memory
  • Governance
  • Control Life-Cycle-Cost / Total-Cost-of-Ownership

• **Data Management**
  • Data quality
  • Governance

• **Information** (Data in Context)
  • Providing information that informs a decision
  • Marking information elements (aggregated, integrated and fused data)
  • User trust of provided information

Gathered during workshops and information sessions with US & international Government, Academia & Private sector organizations
The ASMG effort to develop the IEF Standards as demonstrated by the IEF TDP is seeking to:

1. Enable Policy-driven Data-centric information sharing and safeguarding to balance:
   1. Need to Share
   2. Need to know
2. Maximize the availability information while protecting sensitive element – foundational to Situational Awareness
3. Deliver these advancements using shared, common, reusable services and technology
4. Enable users to evolve capability over time
5. Assure the retention of institutional memory
BENEFITS OF THE APPROACH
(Reduced cost and Risk)

- Integration of policy development into architecture frameworks in order to:
  - Provide traceability to legislation, regulation, MOUs, SLA, and Operating Procedures
  - Retain Institutional Memory (knowledge and information)
  - Deliver model driven management and model driven architecture (MDA), which reduces development time, risk and cost
- Enable a Policy development life-cycle, auditing and governance
- Separate the policy development and solution development life-cycles enabling and evolutionary development of ISS capability – do not need all the requirement on day one
- Moving to a standards based approach that will deliver more vendors, products and services, yielding:
  - Competitive acquisition
  - Reduced risk of vendor lock-in
  - Reduce the risks associated with aging IT
  - Increased opportunity for leveraging shared services (as-a-service)
  - Higher adoption rate with partner agencies
- Broad-based Information Sharing and Safeguarding capability using a common framework, services and infrastructure
WHAT ARE THE DIFFERENCES BETWEEN THESE DOMAINS

THE DATA
Each community works with their own semantics

THE SEMANTICS
Content (/Meaning), Structure, & Format)
(at rest, in transit and in use)

THE RULES
Packaging (aggregation, transformation, marking, redaction, and formatting)
Processing (parsing, transformation, marshaling)
Access / Release Control

Little or no differences in the core Tools, Techniques or Technologies
Though the bells and whistles may change