TURNING THE TABLE THROUGH FEDERATED INFORMATION SHARING

Kathleen Moriarty
EMC Corporation

Patrick Curry
British Business Federation Authority (BBFA)

RSA CONFERENCE EUROPE 2013

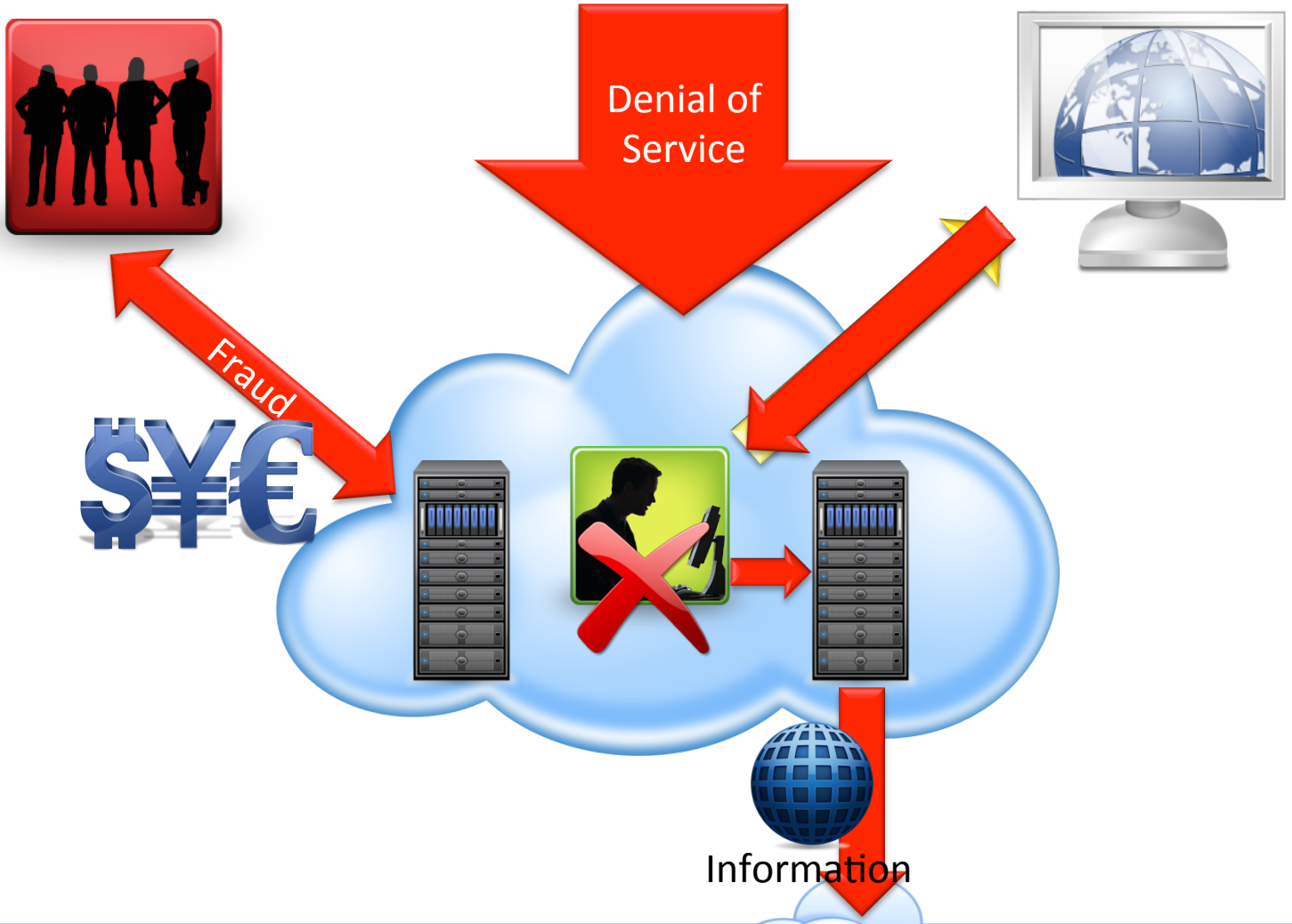
Session ID: GRC-W09

Session Classification: Intermediate

Turning the Table through Federated Information Sharing

- Drivers
  - The growing impact of fraud
  - Regulations
  - Reduce costs
- Cross Industry and Government Initiatives
  - Experiments, Re-Use and Proofs of Concept
  - Frameworks & Standards
- Effective information sharing
  - Use case driven, resulting in directed exchanges
  - Leverage the few analytic resources for broad impact!

What are We Trying to Solve?



Growing Impact of Fraud

- **Fraud-as-a-business is becoming more sophisticated and effective day by day.**
  - Costs are rising- 2011. UK £73 Bn, EU €500 bn, Global $2 trl.
  - Fraudsters using big data to increase attack effectiveness
- **Hactivism and Advanced Threats.**
  - Increasingly, organised crime hired for DDoS attacks, pushing ideological and political agendas.
  - PDoS part of deception tactics for multiphase attacks
  - Reported cyber incidents up 65% each year
- **Mobile movement.**
  - BYOD is a fraud vector, creating new challenges for enterprises
- *Result*
  - *Governments introducing laws and collaborating on protections*
  - *Industries collaborating to comply and to protect*
  - *Technology responding, numerous examples*

Global Information Sharing

- EU
  - EU Cyber Security Strategy ←→ NATO CDAP
  - eID, Authentication, Digital Signature regulation = law
  - Network Information Security Directive
  - Secure information sharing between CERTs
- US
  - 9/11 - HSPD12 – Federated Identity
  - Executive Order - Improving Critical Infrastructure
    - Draft Cyber security framework
  - PPD 21 – Critical Infrastructure Security & Resilience
- Global
  - 5 EYES, ASEAN, PACRIM, Middle East, South America…

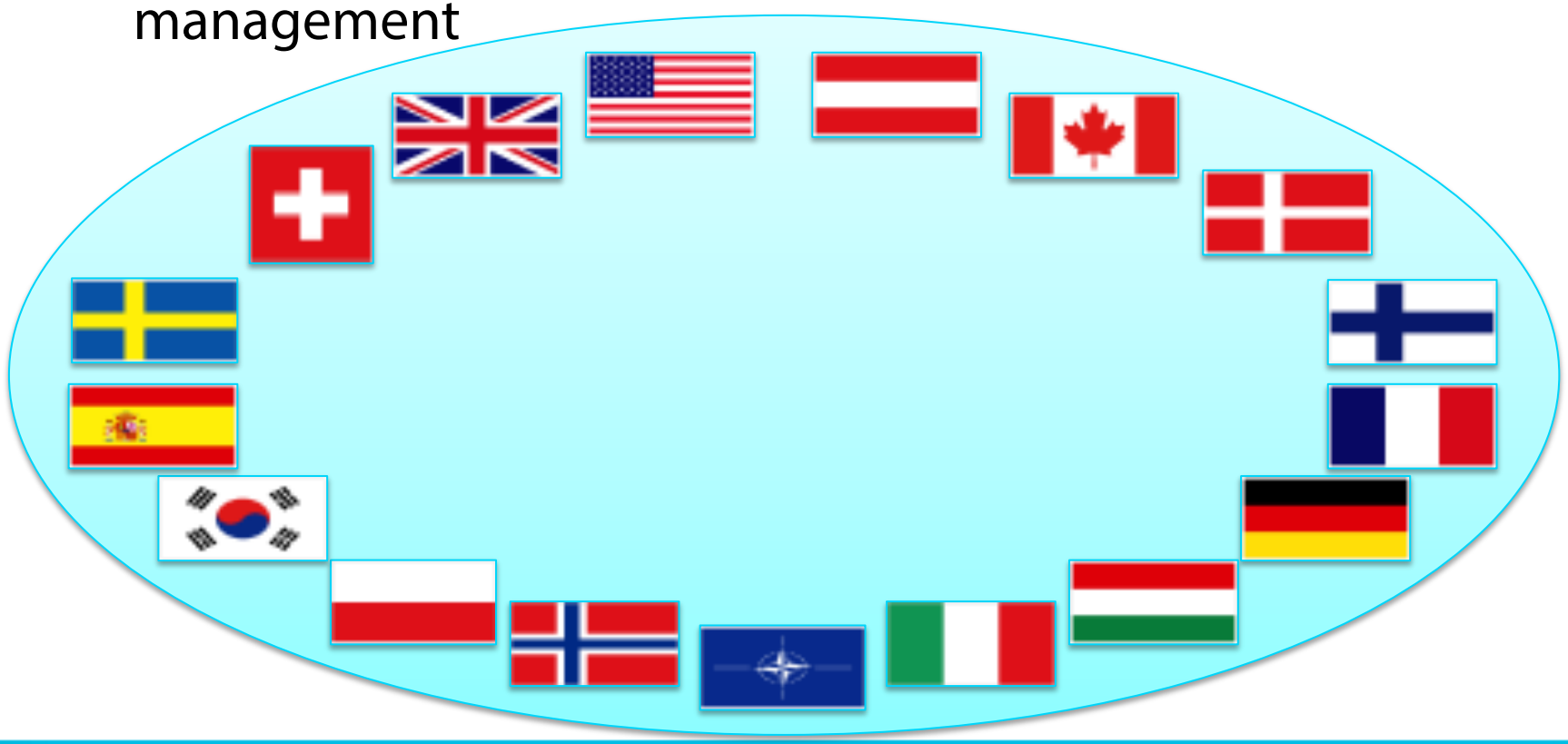
Cross Industry and Government Experiments and Frameworks

#RSAC

RSA CONFERENCE EUROPE 2013

Across Industries & Governments

- Multi-national experiment 7 (MNE7)
- Industries: telecom, power, defense, and air traffic management

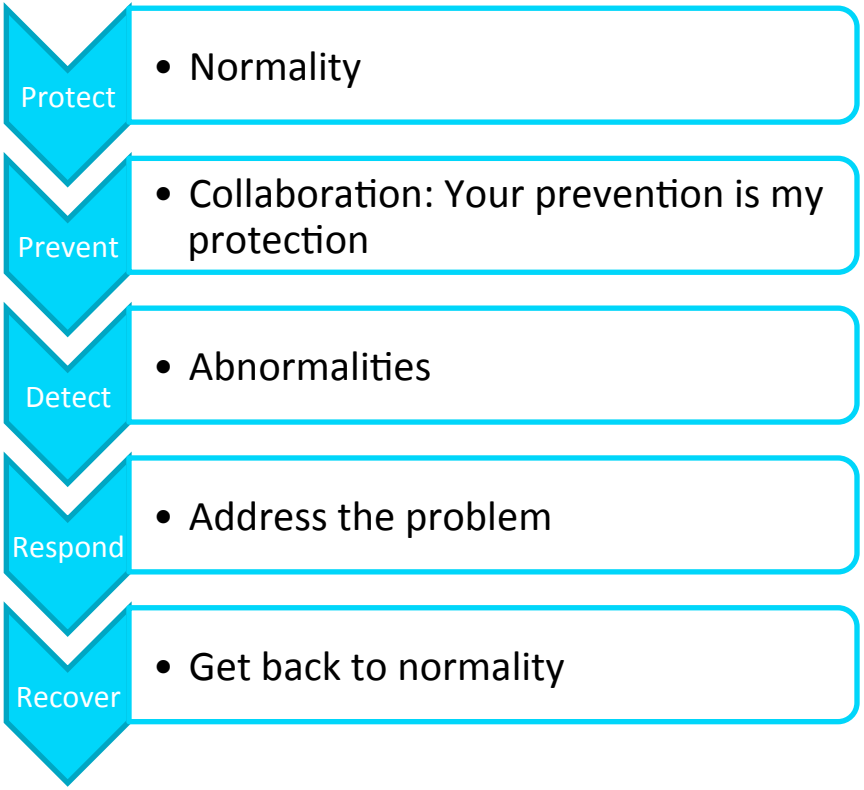


Lessons Learned from MNE7

One size does not fit all!

- Don't collaborate = 90% ineffective. Enemy wins.
- 80% major cyber incidents have real-world crisis impacts
- Mesh - Hubs, Nodes, CERTs/CSIRTs, WARPs
- Core cyber security exchanges can be met using existing capabilities based on international standards
  - IODEF - hierarchical, flexible, and extensible data format
  - RID – transport and security automation, including M2M
- Industry specific exchanges require enhancement
- Faster strategic level decisions and information sharing may be better suited to the Common Alerting Protocol (CAP) by OASIS and the ITU-T

Lifecycle to Preserve "Normality"

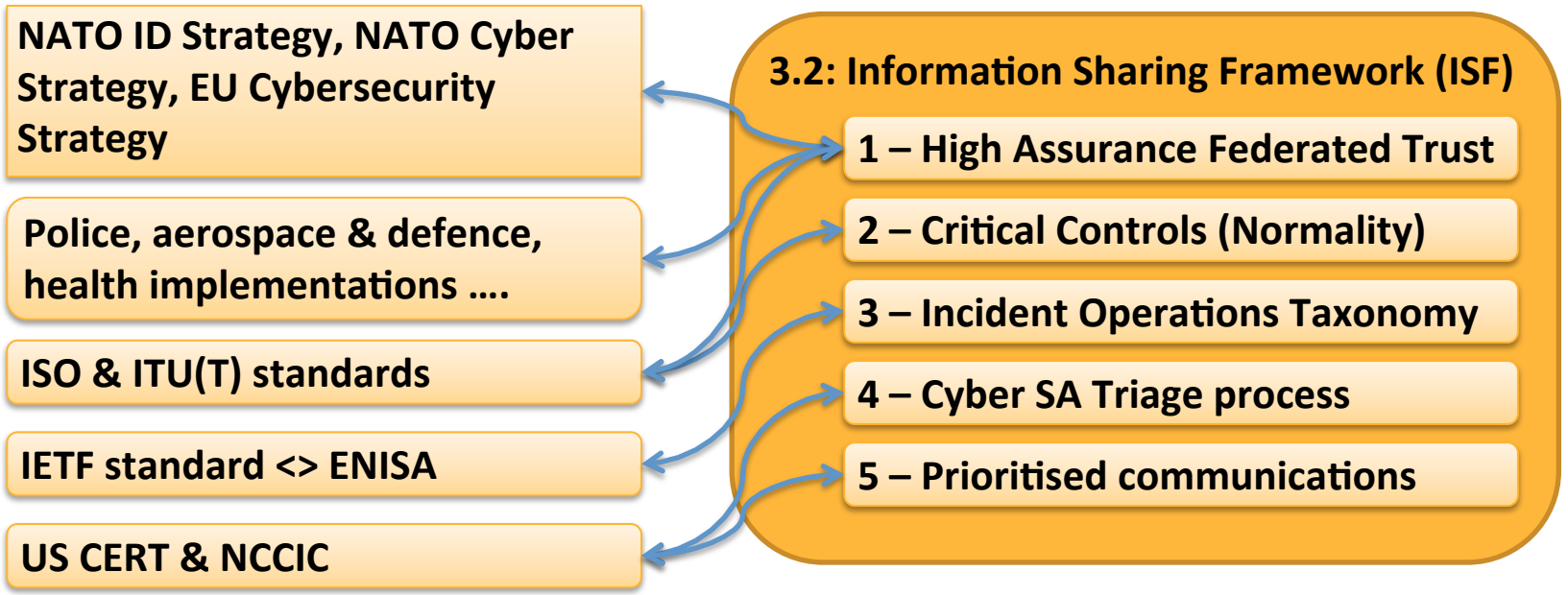


Lifecycle provided through MACCSA:

- Federated trust with 4 Levels of Assurance (LoA)
- Cyber control frameworks to manage expected normalcy:
  - ISO 270XX plus 29XXX, US SP800-53 R4, Australian Top 35, SANS
  - UK Cyber Defence Capability Assessment Tool (CDCAT) includes ITIL and LoAs

Multinational Alliance for Collaborative Cyber Situational Awareness (MACCSA) – Information Sharing Framework (ISF)

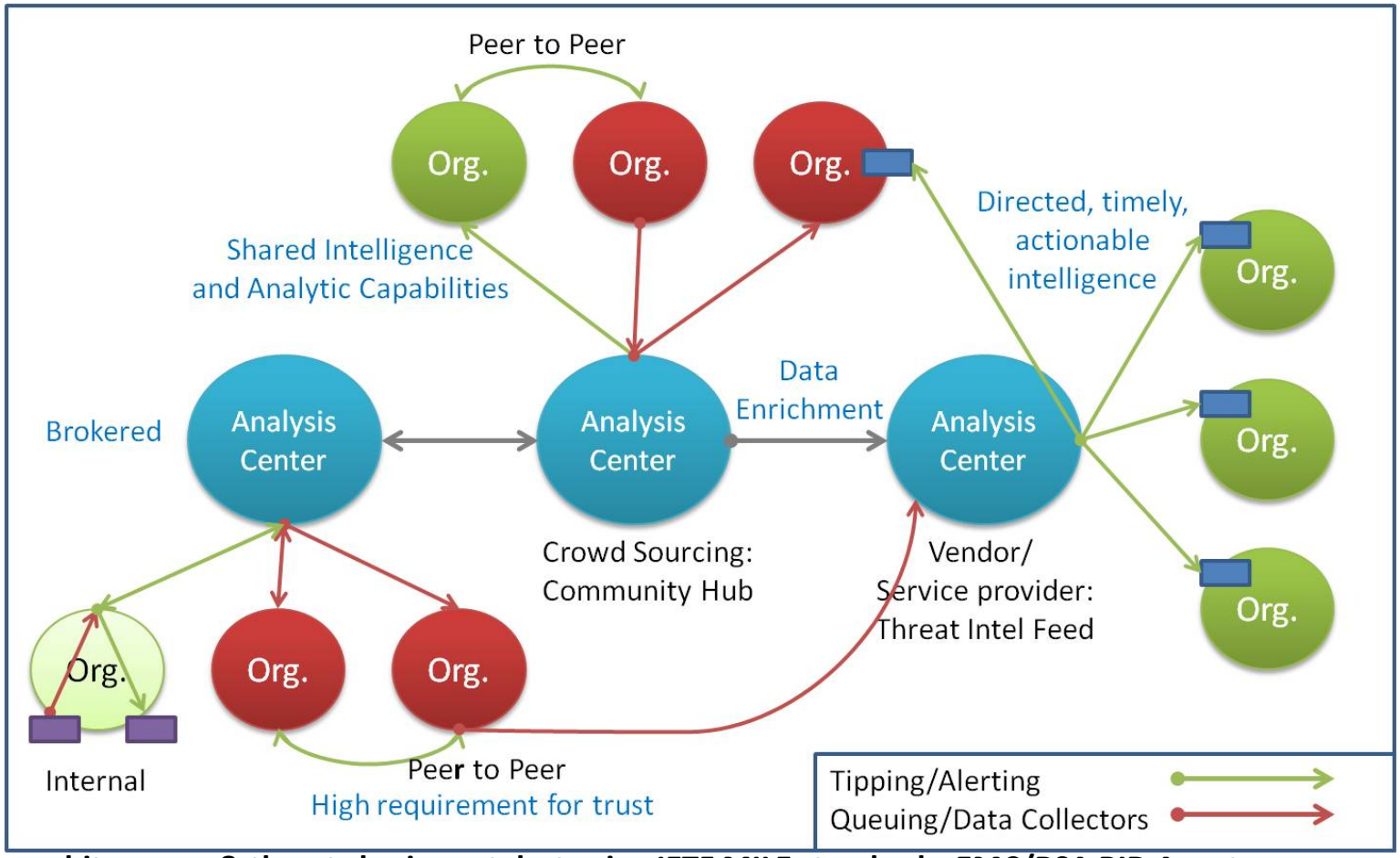
Organisations from 35 nations, 22 governments, EU, UN, ITU, FIRST….



BBFA

Proprietary - British Business Federation Authority – office@federatedbusiness.org

Telecommunication Management Forum (TM Forum): Sharing Threat Intelligence to Mitigate Cyber Attacks



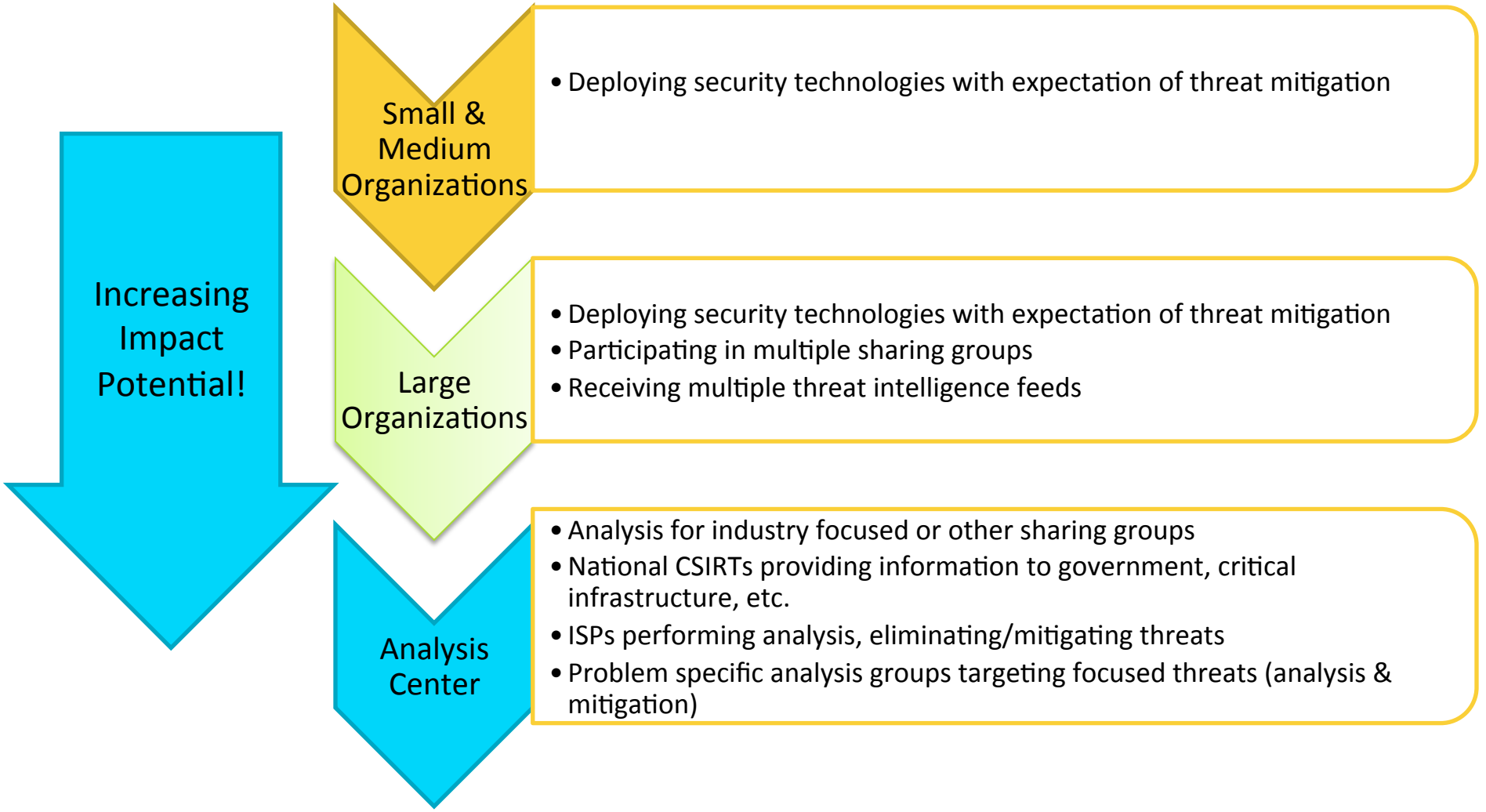
*** TM Forum white paper & threat sharing catalyst using IETF MILE standards, EMC/RSA RID Agent:**
http://www.tmforum.org/Management-World-2013/SharingThreatIntelligence/14646/home.html

Effective Information Sharing

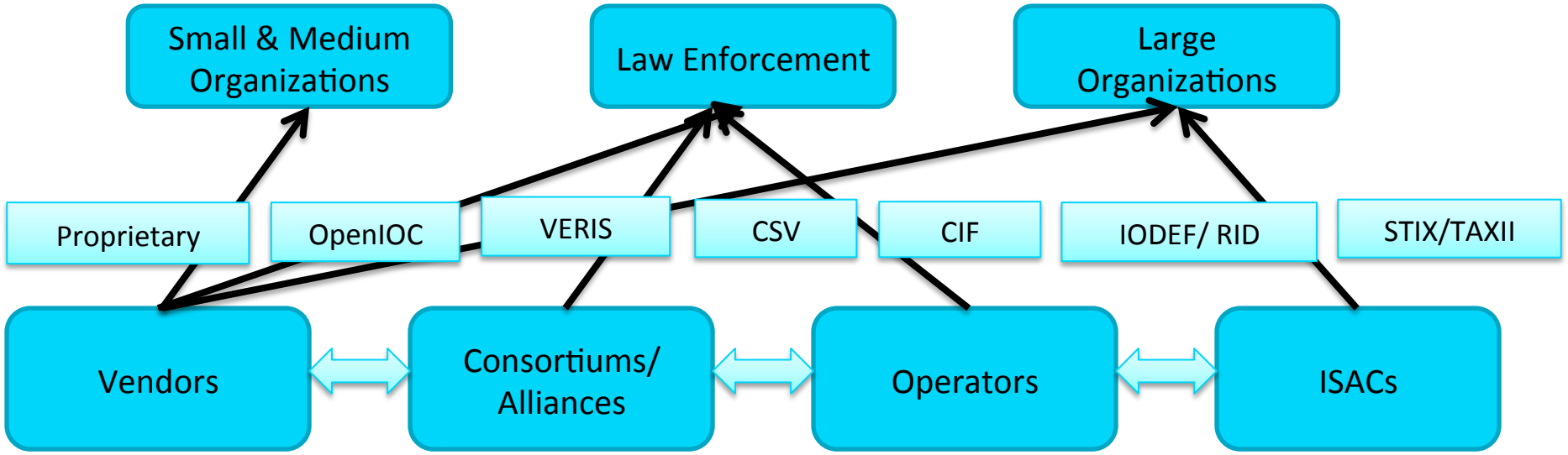
#RSAC

RSA CONFERENCE EUROPE 2013

Who is Sharing Data? What is Useful?



Use Case Driven Standards Adoption



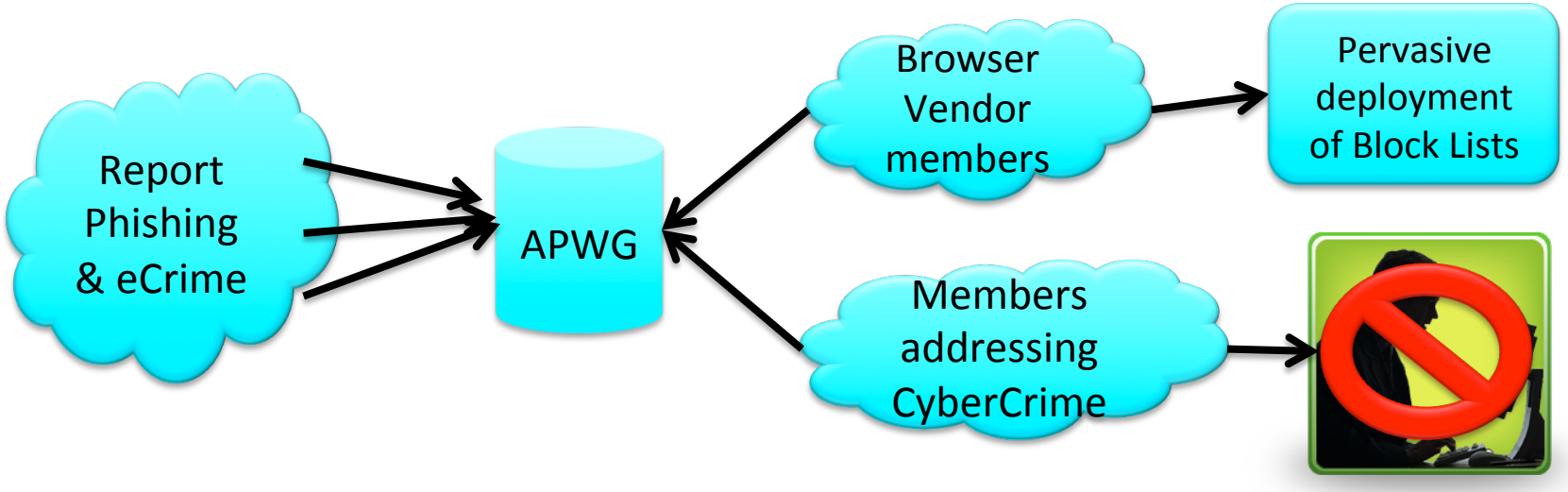
- Shared threat intelligence must be:
  - **Directed**: Intelligence received must be relevant to the organization
  - **Actionable**: Intelligence must identify an immediate and active security response that mitigates the risk
  - **Automated**: Remediation based on intelligence must NOT impact the user experience

Effective Information Sharing

- Industry or regional focused sharing groups
  - Grow strong with **shared** challenges, thus similar risks and security concerns
- Effective information-sharing models are **use case** driven
  - **Standards** selected to fit needs of the use case
  - Focus on requirements
  - Leverages information sharing ecosystem for a broad impact!
- **Automated** corrective measures alter sharing patterns
  - Enables broad protections while leveraging **common analytic resources**
- **Pools** expertise to solve problems in parallel, resolve threats faster

APWG: Use Case Driven Sharing

- Anti-phishing & eCrime use cases
- APWG hosted clearinghouse of Cybercrime data
  - Members: Financial sector, vendors, law enforcement, etc.
- Formats:
  - RFC5070 (IODEF) + RFC5901 (Anti-phishing ext.) + eCrime ext.



Next Steps for Organizations

- Identify key use cases for information sharing
  - Develop efficient sharing models, actively avoid a big data problem that is too big to solve
  - Automated sharing does not mean all users get all data
- Work with sharing groups and vendors to map out requirements for sharing models
  - What do you need to share with whom?
  - What type of exchange is needed?
    - Federated
    - Peer-to-peer
    - Repository access
    - Vendor threat intelligence feeds
- Last Step: Automate Interoperable Exchanges
  - Iterate and improve from lessons learned

Summary

- We aren't winning. We aren't smart enough.
  - Nature – herds and swarms survive. Individuals don't.
  - Collaborate to compete. Not the other way around.
- Advancing the current state:
  - Use case driven sharing is essential
  - Start by answering the question: What do you share with whom for effective response capabilities?
  - Identify requirements before worrying about automation
  - Increment capabilities over time, Keep It Simple!
- Leverage International frameworks and standards where possible
- MACCSA Information Sharing Framework identifies key international standards:
  - Federated trust – high assurance federation (ISO, ITU)
  - Data formats and transports for automation (IETF)
  - Cyber control frameworks (ISO, ITIL)

Thank you!

Kathleen Moriarty

Global Lead Security Architect

EMC Corporation

Kathleen.Moriarty@emc.com

Patrick Curry

Director, British Business Federation Authority (BBFA)

#RSAC

RSA CONFERENCE EUROPE 2013