What "REALLY" matters in Cyber?

RE: Internet of *things* – security and beyond

INCOSE Mini-Conference

HOW to best integrate Security and SE?

*And what is a "**thing**" – is that MORE we have to do???*

Nov2, 2013

Mike Davis

mike@sciap.org ← ***"easy button"***

ElectEngr/MSEE, CISSP, SysEngr

ISSA / ISC2 / SOeC… AFCEA / NDIA… IEEE / INCOSE / et al…

Cyber Security – Overall Status

(Senior IA/Cyber VIP - *same issues as 40-50 years ago*, but better in last 10)

			trending	
Technology	---	G	↗	We have what we NEED NOW
Business	---	Y	→	Some LSIs resist change
Policy	---	Y	→	Legislation poor Can't be voluntary
Procedures / standards	---	G	↗	NIST done well Need uniform implementation
Education	---	G	↗	170+ CAEs (schools) 10,000+ / year
Leadership	---	R	↘	Complexity vs CISO C-suite complacency and inability to absorb
Awareness	---	G	↗	Education starting earlier, STEM, NICE

We all need to provide an integrated, cyber package that is affordable

SysEngr Activities Overview

(Why might folks think they are different / at odds with each other?)

"SE"	**"SecuritySE"**
State the Problem	State the Security Objective / Threats / *Risk Tolerance*
Investigate Alternatives	Investigate Security Alternatives (BUY vs build)
Model the System	Model the System Security – End-to-end / Enterprise
Integrate	Integrate – Build in cyber T&E/metrics methods up front
Launch the System	Launch the System Securely – representative environment
Assess Performance	Assess Security Performance (STIGs / NACS, "*use case*")
Re-evaluate	Re-evaluate (remediate and mitigate security flaws)
Variations	IA Variations (Not meet IA controls – covert channels)

SSE 'is' SE, with a security focus versus functional!

Building cyber security in

(note - it should *already be a normal part of SE*!)

1 – Get the requirements "right" first – when in doubt, go over them again!

"ROI" – we know it is10s-100 times cheaper to fix things early vs deployed

2 – Concurrent engineering principles apply to all aspects – security too

The 'integrated package" is what counts most – secure AND producible

3 – The INCOSE SE activities are the SAME for both, the WHAT is different

re: earlier slide – both need to use same standards, protocols (PPSM), profiles, etc

4 – System Engineers (SE) and Security SE (SSE) harmonize "SoS / I&I" efforts

Both must support "system of systems (**SoS**)" / "integration & interoperability (**I&I**)" collaboration

5 – The risk management plan should include functional *and* cyber aspects

Risk is an enterprise / system-wide construct – trade-offs, mission assurance, etc

6 – Follow the SAME enterprise architecture (EA) – standards and use "APLs"

Must design to the same picture, leverage open architecture principles, use commodity items, etc

SSE 'is' SE,

with a security focus versus functional!

SO… what does matter in Cyber?

CYBER is fundamentally all about **TRUST** and **DATA**

It's NOT about expensive new "cyber capabilities / toys"

but more **about the SoS / I&I "glue"** (distributed trust, resiliency, automation, profiles, etc)

90+% of security incidents are from lack of doing the basics!

Conduct Effective **Security Continuous Monitoring (SCM / SIEM)** – a MUST DO!

USE enforced: cyber hygiene, enterprise access control, & reduce complexity (*APLs*)

Embrace your Risk Management Plan – *LIVE IT*!

Have an *enforceable security policy* – what is allowed / not – train to it

KNOW your baseline - Protect the business from the unknown risks as well

Employ a due diligence level of security – then **transfer residual risks!**

When in doubt, do the cyber BASICS well!!!

An **achievable 90-95% solution** to MOST vulnerabilities – ***stabilize the environment*!**

Threat Vectors of Interest (examples)

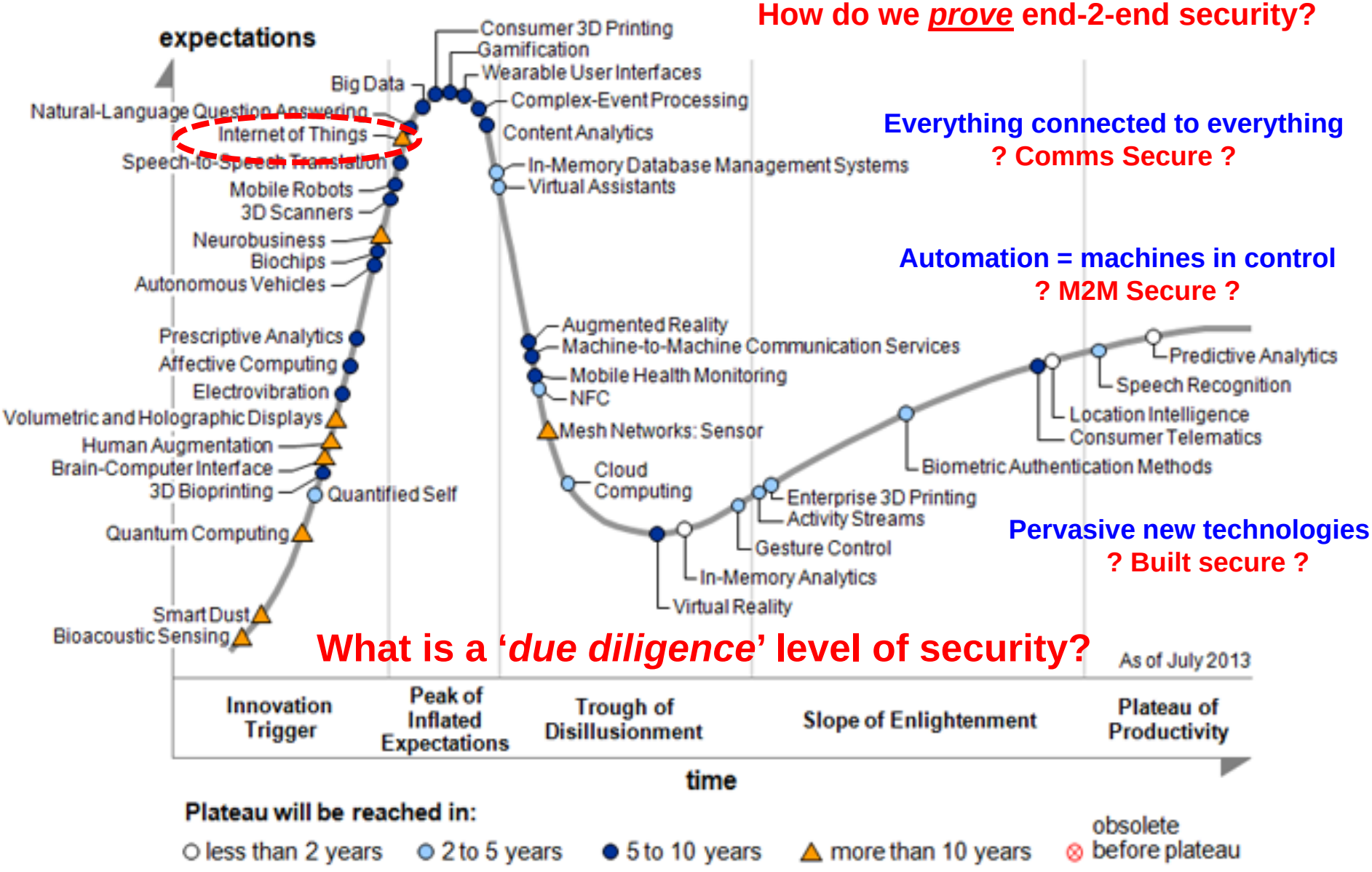
- **Mobile devices … and wireless** always predicted, *yet proliferates in 2013/4*
  - Increasing Android Trojans, **digital wallets**, USER provided network services / access points!
  - Wireless security issues expand (besides 802.11 & WiMAX, to Zigbee, Z-Wave, ARM, etc.) …
  - **BYOD** – many hidden costs, legalities and risks than it appears at first…
- **Cyber crime: easy money, minimal downside and growing** (**ransomware**, etc)
  - Illicit cyber revenues has essentially equaled all illegal drug trafficking dollars
- **The insider threat is much more "*impactful*" than given credit for**
  - Considering compromised services and computing devices of all kinds (aka, *supply chain security*). With Improved social engineering attacks… and… stealth exfiltration techniques… etc…

- **Verizon Data Breach Report – MOST breaches avoidable!**
  - 96% attacks not difficult; - 85% **took weeks to discover** (average is 416 days); - 92% discovered by a third party; 85 - ***97% data breaches / security incidents avoidable*** through simple or intermediate controls
- **Forbes - The Biggest Cybersecurity Threats of 2013**
  - Social Engineering; APTs; Internal Threats; BYOD; HTML5; Botnets; & Targeted Malware
  - AND Cloud security - pretty good, SLAs not enough, but ISPs / data centers better than most

Mobile devices and *cloud infrastructure* hacking are two of the biggest attack vectors in crime / terrorism in 2013 and beyond…

Gartner's 2013 Hype Cycle for Emerging Technologies

How do we *prove* end-2-end security?



Everything connected to everything
? Comms Secure ?

Automation = machines in control
? M2M Secure ?

Pervasive new technologies
? Built secure ?

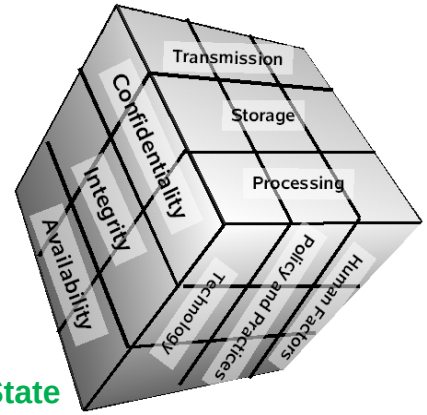
What is a '*due diligence*' level of security?

"ALL" the technologies / connections need built in security

What's a "simple" IA/Cyber vision / end-state look like?

AND what are the "requirements"?

Notional Representation of IA Vulnerabilities and Architectural Approach to Layered Defense in a NetCentric World



Identity, access control and authorization are critical in this environment, significant work on distributed access control systems needs to be completed for High Assurance Solution for ID certification using distributed solutions

Cyber is ALL about TRUST, Rules/MOAs & State

KEY C-I-A entities / touch points

Protected Infrastructure, QOS, COS and Routing Grid

Intelligent Content and Cryptography aware Boundary Proxy/Guard and Policy Enforcement Functions.

comms

things

Certified Platforms with Tamper Resistance/Indication built into platform and certified software load

IoT = things + comms

In the Net Centric world data in motion and data at rest become indistinguishable there is a need to protect storage, queues, and memory locations across the grid from information exfiltration.

AND DATA - Is yours assured / with a pedigree? *"4Vs" satisfied*?

Common Services from Geo Targeting to DNS must be protected at the level required by the highest risk applications using themyou cannot consume anything that you do not trust if affects your decision cycle in a way you cannot adapt to. Aggregate risk **compounds** the protection level required for the components and is **seldom** accounted for properly.

A cyber end-state stresses *encapsulation* using *secure communications*

SO… what **MUST** WE ALL DO???

*NIST's "**absolutely necessary**" Security Protections*

NIST - National Institute of Standards and Technology

- Protect information/systems/networks from **damage by viruses, spyware, and other malicious code**. (IA suite, A/V, encryption, etc)
- Provide security for your **Internet connection / ISP**
- Install and activate **software firewalls** on all your business systems
- **Patch** your operating systems & applications (*and now "things" too!*)
- Make **backup copies** of important business data/information
- **Control physical access** to your computers and network components
- **Secure your wireless** access point and networks
- **Train your employees** in basic security principles
- Require **individual user accounts** for each employee on business computers and for business applications
- **Limit employee access** to data and information, and **limit authority to install software**

MUST DO tasks – consider this your 'due diligence' list
Where ALL have "CM / hygiene / IA&A" aspects

KEY Enabling Technology Areas

Value / need

high

- ***Distributed Trust***
- ***Resilient Architectures***
- ***Response and Cyber Maneuver***
- ***Visualization and Decision Support***

---

med

- **Component Trust**
- **Recovery and Reconstitution**
- **Detection and Autonomic Response**

---

low

- **Advanced Cross-Domain Solutions**
- **Advanced Cryptography**
- **Quantum Computing, Comms, and Crypto**
- **Biometrics**
- **Code Verification and Compliance**
- **Correct (Assured) by Construction Software**
- **Deception and Information Hiding**
- **Human Factors and Training**
- **Malware/Forensics Analysis and Reverse Engineering**
- **Resilient Infrastructure and Comms**
- **Scientific Theory and Measures**
- **Sensing and Data Fusion**
- **Software Pedigree and Provenance**

CYBER is fundamentally about
distributed trust / assured DATA / secure messaging!

Define the systems requirements

(*Example* - CNO's **I**nformational **D**ominance, **operational** requirements -> **technical)**

First Principles Include:

- Every platform is a *sensor*
- Every sensor is networked
- Build a little; test a lot
- Spiral development/acquisition
- Plug-n-play sensor *payloads*
- Reduce afloat/airborne manning
- Transition to remoted, automated
- Collectors dynamically tasked

ID capabilities need to be both prioritized and aligned and **accommodate SoS/I&I factors**

- One operator controls multiple platforms (multi-task / multi-mission)
- Emphasize UAS and autonomous platforms
- UAS's increasingly sea-based
- *Data discoverable and accessible*
- Missions drive requirements
- Commonality in interfaces, data links and control stations
- Every shooter capable of using target *data derived* from any sensor

ID – *decision superiority* - is all about TRUST & DATA

Common Architectural Flaws,
(which exacerbate Cyber Security AND SE execution)

- Fragile Chain of Services
- Large Real-time Overhead
- Central Administration Mis-alignment with Practical Administrative boundaries
- Lack of Support for multiple:
  - Weak / ineffective “enterprise” Access Control Models
  - No Concept of Risk or Domain Asymmetry or Support for Multiple Mission Vectors
- Rigid Inheritance Model
- Use of Hard-coded Rigid Monolithic Access Control Frameworks and Products
- No Enterprise Concept of Domain Delegation or RAdAC
- Lack of Appropriate Layering and Abstraction

Common Architectural Flaws (cont)

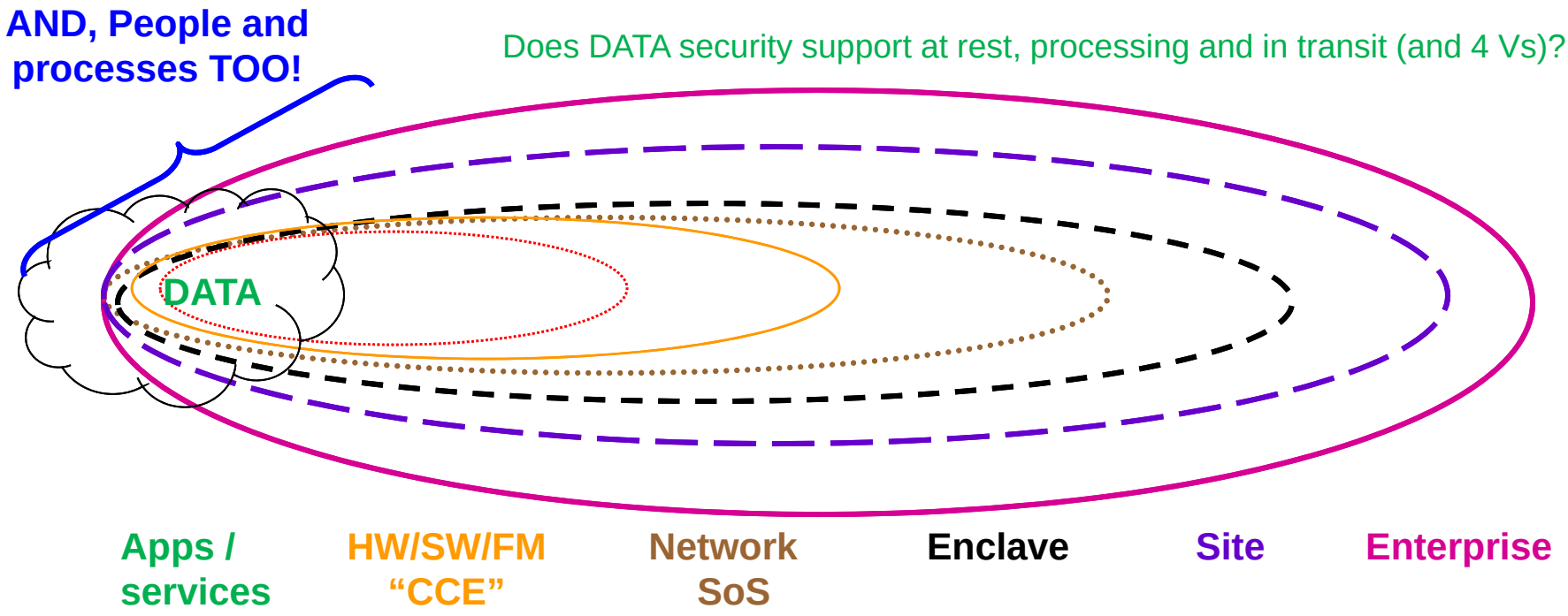
- **Inability to Support Multiple and Legacy Models**
  - Schema and Ontology often Incompatible
  - Attributes do not Align
  - Methods and Protocols Differ
  - Technology and the Embedded Dependencies Differ

- **Difficult or Inflexible Integration Paths**
  - Lack of Trustworthiness
  - No Support for Unanticipated Users
  - Transformations Limited
  - Lack of Flexible Rapid Application Development and Modeling Tools with IA Built in to the Framework
  - Lack of Fidelity or Use of Modeling to Test Performance at Scale

These are *systemic issues*, predicated on lack of a common "EA"

Cyber / trust and DATA must be E2E!

WE have a "natural" hierarchy in our enterprise IT/network environment, where complexities arise in the numerous interfaces and many to many communications paths typically involved in end-to-end (E2E) transactions



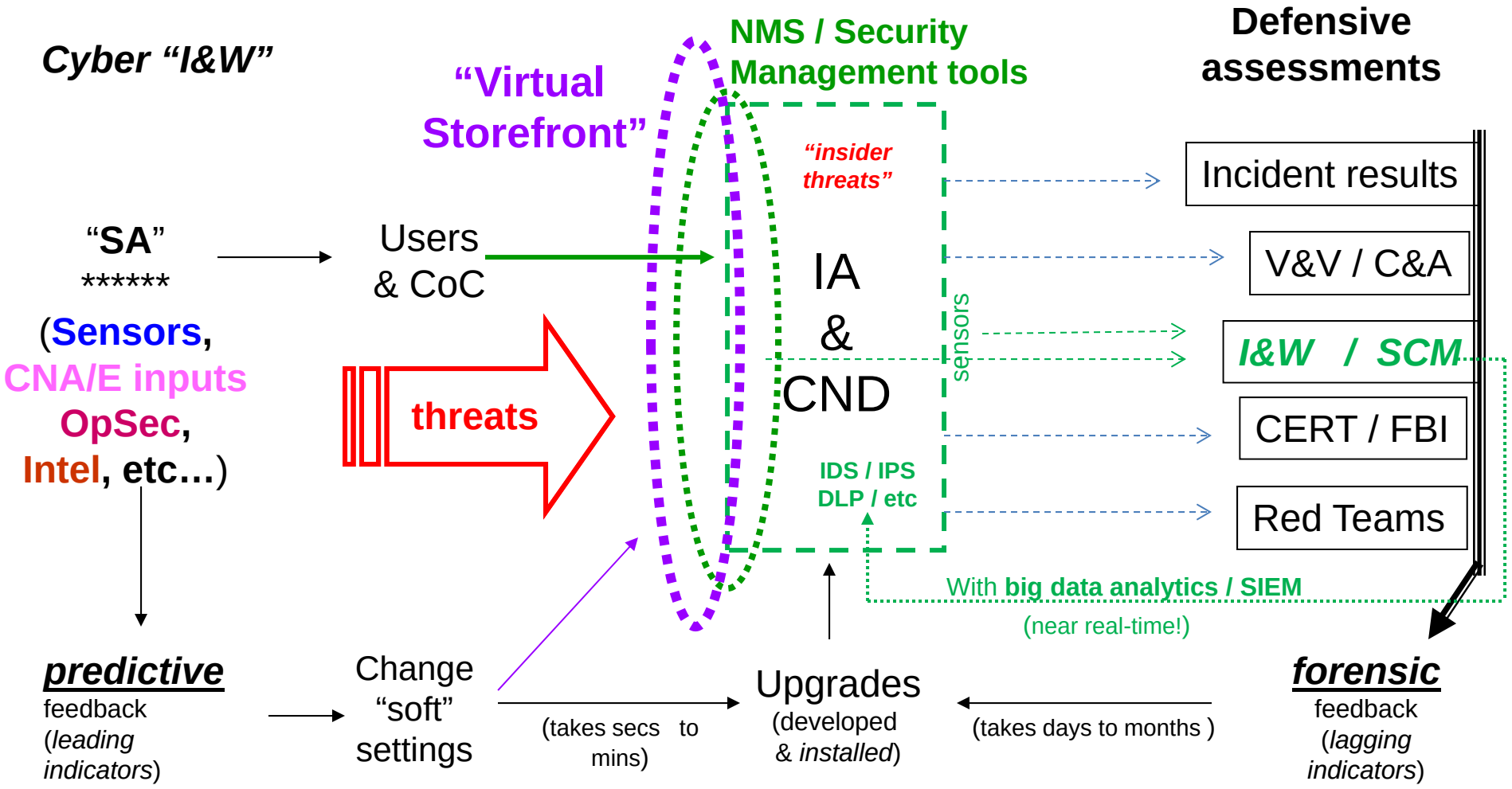
Each sub-aggregation is responsible for the data / controls within their boundaries *and also* inherit the controls of their environment – and need to formalize reciprocity therein!

Thus, the DATA, IA/cyber controls, interfaces and *profiles* in <u>each</u> element / boundary must be quantified / agreed to upfront!

SO just what are were trying to orchestrate?

An integrated "*Cyber Defense in Depth / Breadth*" SYSTEM

using dynamic lead & lag feedback, ***establish proactive, dynamic CND / IA Defense***)



All SE / SSE capabilities must be integrated into the cyber 'system'

Integration, execution is everything

as if you can't implement well, it costs you everywhere!!!

The quantitative benefits of systems integration and interoperability are:

1. Shorter/reduced steps in business processes
2. Time taken to process one application/record
3. Less complaints from members of the public
4. No. of applications/records processed over a period
5. Less complaints from end- users
6. Reduced number of errors
7. Reduced software development time/effort
8. Reduced maintenance
9. Reduced no. of IT personnel

*The qualitative benefits of **I&I** are:*

1. Improved working procedures
2. Better communication with other related organizations
3. Job satisfaction
4. Redefine job specification
5. Improved data accessibility
6. One-stop service
7. More friendly public service

Until the user is happy using / benefitting from the new capability, it has no value

Buying stuff is "easy"
getting it to work in your environment is hard…

Plan for "I&I"
- Integration & Interoperability -
then double it

The best capability means little, if it stays in the box

IA/security resources

Main sites

https://infosec.navy.mil Requires "CAC"

http://iase.disa.mil/index2.html

http://csrc.nist.gov/
http://nvd.nist.gov/ SCAP / CVE / etc

http://www.nsa.gov/ia/index.shtml

SSE sites / docs:

http://csrc.nist.gov/groups/SMA/fasp/documents/incident_response/SSAIRBSP/SSECMMv2Final.pdf

ISO/IEC 21827 – SSE CMM
http://csrc.nist.gov/nissc/2000/proceedings/papers/916slide.pdf
http://csrc.nist.gov/groups/SMA/fasp/documents/incident_response/SSAIRBSP/SSECMMv2Final.pdf

Net-Centric Enterprise solutions for I&I
http://nesipublic.spawar.navy.mil/

other IA/Security sites (cont):

http://www.cert.org/

https://www.niap-ccevs.org/Documents_and_Guidance/

http://www.commoncriteriaportal.org/

https://www.sans.org/security-resources/

http://iac.dtic.mil/csiac/

https://www.thecsiac.com/resources/reports/132

http://www.cerias.purdue.edu/site/tools_and_resources/

http://iase.disa.mil/stigs/index.html

SUMMARY
SO…. What "really" matters in Cyber?

- **OSD / federal S&T activities**
  - Distributed Trust
  - Resilient Architectures
  - Response and Cyber Maneuver
  - Visualization and Decision Support
  - Dynamic policy management (RaDaC)
  - Detection and Autonomic Response
  - Recovery and Reconstitution

- **NSA / agency S&T activities**
  - Mobility, wireless, & secure mobile services
  - Platform integrity / compliance assurance
  - End client security
  - Cyber indications and warning (I&W)
  - Mitigation engineering (affordability)
  - Massive data – (date centric security)
  - Advanced technology…. (targeted)
  - Virtualization – secure capabilities

It's all about **TRUST** and **DATA**

It's NOT all about expensive new "cyber capabilities"
but more **about the SoS / I&I "glue"**

AND doing **the BASICS**:
(1) enforced cyber **hygiene**,
(2) effective **access** control,
(3) reduced **complexity** in IA / cyber (APLs / NIAP / *approved products*),
*** **(4) IT / IA / Cyber "SCM / SIEM"** ***
(ongoing diagnostics AND mitigations / SIEM)

DO the cyber BASICS well, for things, people & processes
invest in KEY new capabilities, **build IA in** & follow your RMP!!!

Take ***ACTION***: (1) security assessment, (2) SCM/SIEM, & (3) manage risks!

mike@sciap.org