Getting to the essence of ‘Cyber’

A security model proposal for

Privacy by Design (PbD)

(using data centric security methods accommodating data’s controls and protections)

A talking points brief to socialize issues and propose global, common security ‘implementation’ methods

Mike Davis

Mike.Davis.SD@gmail.com

Business Risk Management / Cyber Security Consultant & Enthusiast

ElectEngr / MSEE, CISSP & CISO, SysEngr
ISC2 / SOeC / ISSA / Infragard...  AFCEA / NDIA...  IEEE / INCOSE / et al
Privacy? I have my hands full with Security!

What is your greatest asset (besides good people)

**DATA** – so where is it, who has it, is it well protected?

How is your current “FUD” cyber approach working?

**Struggle** – at best, too many threats, too little resources

When is your turn at a data breach recovery & law suit?

**Privacy** – more than just PII, HIPAA – many laws & FINES!

Surveillance attacks our most primal notions of freedom

**Spying** creates a prison in the mind - fostering compliance

A **Cyber Enabled Privacy by Design** approach
Can simplify and *clarify the “fog of cyber complexity”*
What’s Wrong With This Security?
What level of protection is really provided here – how about privacy?

The gates were fully locked, properly configured and validated.
I could not get through *them*. But.... Thus Cyber can be an *illusion*...
Why Privacy matters (even if you have ‘nothing to hide’)

1. **Limit on Power** - on government power, as well as the power of private sector companies.

2. **Respect for Individuals** - your individual decisions are personal / not public need to know.

3. **Reputation Management** - depends on protecting against not only falsehoods but also certain truths.

4. **Maintaining Appropriate Social Boundaries** - are both physical and informational. We need solitude.

5. **Trust** - In relationships we depend upon trusting the other party. Breaches of confidentiality betray that trust.

6. **Control Over One’s Life** - data is essential to decisions, freedom is autonomy and control over data.

7. **Freedom of Thought and Speech** - speaking unpopular messages, explore ideas that others do not like.

8. **Freedom of Social and Political Activities** - protect ability to associate with others, groups, activities.

9. **Ability to Change and Second Chances** - move beyond a mistake, to be able to reinvent oneself.

10. **Not Having to Explain or Justify Oneself** - not judged from afar by others lacking complete knowledge.

Privacy mandated by laws with significant fines and *unconstrained 3rd party liability!*
# Cyber Security – Overall Status

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

<table>
<thead>
<tr>
<th>Category</th>
<th>Trend</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology</td>
<td></td>
<td>We have what we <em>NEED NOW</em></td>
</tr>
<tr>
<td>Business</td>
<td></td>
<td>Some LSIs resist change</td>
</tr>
<tr>
<td>Policy</td>
<td></td>
<td>Legislation poor Can’t be voluntary</td>
</tr>
<tr>
<td>Procedures / standards</td>
<td></td>
<td>NIST done well Need uniform implementation</td>
</tr>
<tr>
<td>Education</td>
<td></td>
<td>NICE, 170+ CAEs (schools) 10,000+ / year</td>
</tr>
<tr>
<td>Leadership</td>
<td></td>
<td>Complexity vs CISO C-suite complacency and ability to absorb</td>
</tr>
<tr>
<td>Awareness</td>
<td></td>
<td>Education starting earlier, STEM, NICE</td>
</tr>
</tbody>
</table>

We must provide an **integrated, interoperable cyber package** that is affordable.
What’s new in cyber, and **what matters**?

Sensor + WiFi = device --- **Things** -> systems, machines, equipment, and devices — all connected to each other

The Internet of Things

RFID, Apps, MEMS, WSN, sensors, SCADA, PLC, ASIC, API, ETC, etc

**Is all this stuff secure?**

**How much is needed?**

Sensor + WiFi = device

---

**Things**

- systems
- machines
- equipment
- devices

---

The “Internet of things (IoT)” is not really new...

IoT requires ALL the cyber protections we already know - and still need to implement!
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 ?

What is an ‘adequate’ / **due diligence** level of security???

Pervasive new technologies ? Built secure ?

“ALL” the technologies need built in security ... *for secure data, comms & privacy*!
SO.... what **REALLY** matters in Cyber?

**CYBER** is fundamentally all about **TRUST** and **DATA**
(Identity, authentication, secure comms --- provenance, quality, pedigree, assured)

It’s **NOT** about expensive new cyber capabilities / “toys”
but more **about the interoperability “glue”** (distributed trust, resiliency, automation, profiles)

90+% of security incidents are from **lack of doing the basics**!
USE effective **Security Continuous Monitoring (SCM / SIEM)** – a MUST DO!
With enforced: cyber hygiene, enterprise access control, & reduced complexity (**APLs**)
**Shift from only protecting the network, to the **DATA security itself** – information centric view**

Embrace your **Risk Management Plan (RMP)** – **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!

You can **NOT** buy cyber, so **do the cyber BASICS well!!!**
An achievable 90-95% reduction in security incidents – **stabilize the environment**!
Yes, It really is ALL about the **DATA**

---

2020 Data Vision

(Courtesy of Dan Green / SPAWAR):

*Themes and Memes* (Technology vs Technology Adoption)

**Convergence** = Genomics, Robotics, Informatics, Nanotech (each a $B+$ market)

"**CBAD**" = Cloud, Big Data, Analytics, Data Science (are you ‘all-in?’)

**Telematics** = Sensing robotics, Cyber Physical Systems (will kids need to learn to drive?)

**Interactive 3D** = Augmented Reality, HTML 5, Three.js (3D graphics for WebGL)

**Embedded Computing** = eHPC, Tessel (mCPU / Java), Programmable hardware

**LBS** = Location Based Services, IPS, Beaconing, NFC

**IoT** = Internet of Things, M2M, Quantified Self

**Mobilization** = Preparation for Conflict/Competition, Autonomy, The Draft

**STEM** = Science Technology Engineering Math, Generation NOW, Old Dogs *(YOU)*

It’s a data-centric world; thus **we need Privacy by Design (PbD)**

*Meme:* an idea, behavior, or style that spreads from person to person within a culture

* and TRUST!

A huge sample size! This includes your business category too!!!

10 year series, 63,437 incidents, 1367 breaches, 95 countries

WHAT
- 92% incidents described by just nine patterns
- shift from geopolitical attacks to large-scale attacks on payment card system

Sectors
- Public (47, 479), Information (1132) and Finance (856)

Threats (%)
- POS intrusions - 31
- Web App Attacks - 21
- Cyber espionage - 15
- Card Skimmers - 14
- Insider misuse - 8
- Crimeware - 4

See also - Ponemon Institute’s cyber report
Key threats – from cost based activities
Malware, malicious insiders and web-based attacks

Forbes lists these: Social Engineering; APTs; Internal Threats; BYOD; HTML5; Botnets; & Targeted Malware

Mitigations
- restrict remote access
- enforce password policies
- Minimize “non” POS activity on those terminals
- Deploy A/V (everywhere, POS too)
- evaluate threats to prioritize treatments
- Look for suspicious network activity
- Use two-factor authentication

We have met the cyber enemy, and they are US(ers)

HYGIENE Factors
MORE “FUD” – Data Breaches are expensive

Cost Of A Data Breach Jumps By 23% - average cost of an attack is $639,462
(Ponemon - Energy and utility organizations the highest($13.18 million), followed by financial services ($12.97 million). Healthcare the fewest ($1.38 million)- $201 / record)
(Average to resolve a cyber attack climbing to 45 days, from 32 days, averaging $20,000)
http://essextec.com/sites/default/files/2014%20Cost%20of%20Data%20Breach%20Study.PDF

Target, Home Depot, Chase.. Just the visible big ones
• Heartland Payment Systems, 2008-2009: 130 million records
• Sony online entertainment services, 2011: 102 million records
• National Archive and Records Administration, 2008: 76 million records
• Epsilon, 2011: 60 million to 250 million records
• Home Depot, 2014: 56 million payment cards
• 2013 – 575, 486, 661 data records lost... 2014 – (1st 3 months ) – over 200 million
• the data breaches just go on and on... (with 3rd party lawsuits piling up...)

What about a Data Breach and the Cloud Multiplier Effect.
Increasing use of cloud services can increase the probability of a $20 million data breach by as much as 3x..... http://cloudtweaks.com/2014/07/cloud-infographic-cost-data-breach/

Due diligence security posture required and use a privacy protection approach
MORE “FUD” – FEW pay attention to data security

Poneman report - “State of Data Centric Security (DCS)”

1 - Data in the dark keeps IT practitioners up at night.
57% said not knowing where the organization’s sensitive or confidential data is located.
51% said migration to new mobile platforms.

2 - Sensitive or confidential data is often invisible to IT security.
16% believe they know where all sensitive structured data is located
Only 7% know where their unstructured data resides.
(41% are in the dark about their organization's unstructured data)

3- Data security is a serious threat but often not a priority.
Most not conducting data asset security processes, methods or tools...
65% have no comprehensive digital forensics capability
61% are not monitoring data transfers between third party location, including cloud
59% are not enforcing data access policies across applications, locations, departments  (DLP anyone?)

4 - Organizations mainly rely upon the classification of sensitive data to safeguard data assets.
2 most popular technologies for structured data: sensitive data classification and application-level access controls.
Only 19% say they use centralized access control management and 14% use file system and access audits.

5 - Automated sensitive data-discovery solutions reduce data risk & increase security effectiveness.
60% say they are not using automated solutions to discover where sensitive or confidential data is located.

Due diligence security posture required and use a privacy protection approach

SO.... What is “Privacy”?
(it’s not as clear as you might think)

Definition: The state or condition of being free from being observed or disturbed by others
Also, the state of being free from public attention...
And the recent EU’s top court’s decision (on Google) - the right to be forgotten!!!

"Personally identifiable information" (PII), as used in US privacy law and information security, is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

Business view: In general, the right to be free from secret surveillance and to determine whether, when, how, and to whom, one's personal or organizational information is to be revealed. In specific, privacy may be divided into four categories
(1) Physical: restriction to experience a person or situation through one or more of the human senses;
(2) Informational: restriction on searching or revealing facts that are unknown or unknowable to others;
(3) Decisional: restriction on interfering in decisions that are exclusive to an entity;
(4) Dispositional: restriction on attempts to know an individual's state of mind

Some ‘quirk’s’ to consider – where/how does privacy really matter... is it for people only?
- The Internet of things / everything - sensors, modules, smart devices have critical data.
- The notion of PII (12 major attributes) or HIPAA PHI (18 key attributes) is likely not enough. http://cphs.berkeley.edu/hipaa/hipaa18.html (even medical metadata / anonymization has a ‘common rule” to follow)
http://en.wikipedia.org/wiki/Personally_identifiable_information (NIST Special Publication 800-122 has it’s own list)
- There are 100-1000s+ other attributes (from what you do, search) that can pinpoint you!

Solution – a cyber model for privacy by design (PbD) that is agnostic to the environment
So what’s the problem?
(Privacy is not about secrecy (I have nothing to hide), rather anonymity of YOUR decisions!)

Privacy is a simple concept but complex endeavor to protect. Privacy definitions are equally diverse, where the related requirements are naturally diffuse, varied, complex and change depending on where your data resides – city, state, country (for example, the US laws are relatively weak and European Union enforcement is much stricter).

Chances are if you don’t have a chief privacy officer or data protection officer, your organization is lacking in protecting critical data, let alone all the laws and statutory regulations dealing with privacy (e.g., Personal Identifiable Information (PII), Health Insurance Privacy and Accountability Act (HIPAA), Payment Card Industry Security Standards (PCI), etc.).

Thus lacking common, ubiquitous privacy requirements, few (if any) implementation level, definitive privacy specifications exist for developers to build privacy enhancing technologies (PET).

So how does one start to protect critical data and associated privacy aspects with many of the privacy environmental variables themselves in flux?

We need a global, open privacy framework (OPF) to design and measure to within a unified, integrated open privacy enterprise architecture (EA)
So what’s the problem?
(Privacy is not about secrecy (I have nothing to hide), rather anonymity of YOUR decisions!)

Given the varied privacy requirements, we developed our **cyber model for privacy around the seven major principles in the existing international Privacy by Design (PbD) initiative** (Creator, Dr. Ann Cavoukian) also mapping these seven principles to the new 24 privacy controls in NIST 800-53a Appendix J.

Thus our “**Cyber Model for PbD** (C4P) will inherently address major privacy protection and control aspects, eventually encapsulating the data security attributes and making them relatively agnostic to the ongoing global privacy environment churn.

Current **PET methods are generally device centric and not integrated as part of an overall enterprise systems of systems (SoS) architecture foundation**. Hence current privacy products and services cannot work in multiple environments or scale – in a continuum from one end device to another, likely different, end device.

The essence of our **C4P approach is to develop an open privacy foundation (OPF) using a services-based “platform as a service” cloud construct applying data-centric security (DCS) methods which are integrated into an enterprise SoS environment** using existing commercial “off-the-shelf” products (COTs).

Our framework leverages, aligns with NIST’s Risk Management Framework (RMF) and Cybersecurity Framework (CSF). The overall C4P intent is to integrate these initial application’s abilities into an enterprise, end-to-end, privacy platform by **developing and documenting a common OPF within a privacy EA**; thus enabling integrated privacy capabilities to enhance usability, reuse, and innovation insertion into a trusted environment.
PbD 7 Principles & Cyber Harmonization

1. Proactive not Reactive; Preventative not Remedial
   Cyber – an overall cyber model which provides implementation guidance, specific methods – enabling privacy

2. Privacy as the Default Setting
   Cyber – Most IA / CND products come preset for the secure settings. Management must put security over convenience in configuring the cyber baseline and data protection levels (and still not encumber the users).

3. Privacy Embedded into Design
   Cyber – Long standing tenet to build security in, not bolt it on – using common standards, controls, and products.

4. Full Functionality – Positive-Sum, not Zero-Sum
   Cyber – a properly designed cyber model does this, keeps it simple, does not affect users, and saves resources.

5. End-to-End Security – Full Lifecycle Protection
   Cyber – IA/Security products can be well integrated and enablers of applications and data – end2end and lifecycle.

6. Visibility and Transparency – Keep it Open
   Cyber – Security by obscurity has limited utility, best to have common methods and products & trust but verify.

7. Respect for User Privacy – Keep it User-Centric
   Cyber – Security can be an enabler = educate users, manage expectations, and provide for easy state changes

PbD and Cyber have common goals = data-centric security (DCS)!
“FAIR” Information practices (FIP)
(These were used in US Privacy Act of 1974)

1. Openness and transparency - no secret recordings
2. Individual participation – subject has control over own data
3. Collection limitation – data collection proportional to purpose
4. Data Quality – relevant to the purpose and kept current
5. Use limitation - data used for specific purpose and by authorized personnel
6. Reasonable security – adequate security safeguards, according to sensitivity
7. Accountability – record keepers accountable for compliance with principles

.... We all need common PbD USE CASES to V&V any Cyber Model....

Long term, incorporate the EU / OECD guidelines - thus reduce trade barriers. And specifically accommodate the EU’s “Data Protection Directive 95/46/EC”.

Any PbD cyber model supports: PbD 7 principles, FIP, EU DPD (& Safe Harbor)
Hierarchy of Data Needs
Not all data / metadata is equal

**Modified from Maslow’s Hierarchy of Needs (original five-stage model)**

- **Physical and Logical**
  - requirement, availability, accessible, discoverable, etc.

- **Security**
  - ownership, privacy, secure, role, limits, stability, etc.

- **Operational**
  - completeness, understandable, usable, brevity, etc.

- **Value**
  - trusted, authoritative, accurate, relevant, responsive, timely, etc.

- **Semantic**
  - interoperable, meaning, M2M, etc

**Use Data Centric Architecture & Security (DCA / DCS)**

Privacy must be accounted for at **ALL levels**
AND eventually accommodate **NPEs (non-person entities)**
Meeting the PbD / DCS challenge

Smarter Data Sharing and Management

- Smart/optimized delivery of Enterprise data to the Sea Services (prioritized and deduplicated)
- Maritime Centers of Data
- Cache Tactical Data at Maritime Centers of Data that have the Resources to archive and serve the data for the entire Enterprise

Auto-processing and Analysis Tools

- NMIC/MOCs/TOCs
- Fused National Maritime Picture
- Afloat Units

- National Intel Data
- Inter-Agency Data
- Joint Data

- Application Integration Framework (AIF)
  - Tactical ISR Data
  - Combat Systems Data
  - Combat Support Data

Collaboration between ashore and afloat personnel

Leverage the Total Workforce

- Singles of specialists afloat
- Terabytes ($10^{12}$) of storage afloat

- Thousands of specialists ashore
- Exabytes ($10^{16}$) of storage ashore

Requirements, Budget, Acquisition Changes

- RDA Chief Engineer Enterprise Engineering Standards and Implementation Patterns Approval Board
  - S&T CE’s
  - SETA CE’s
  - POR CE’s
  - TA CE’s

- Technical Authority Enterprise Reference System
  - POR Engineers
  - SETA Engineers
  - S&T Engineers
  - Tech Auth Engineers

Privacy must be accounted for at all levels & types = Internet of ‘everything’
Exponential Data Growth = geometric privacy challenges!

**Theatre Data Stream (2006):**
~270 TB of NTM data / year

Max of **50 Mbps** per channel

Current single mode fiber carries **960 Gpbs**

Privacy will also need to account for ‘non-person-entity’ data!
Cyberspace Characteristics

All of the *warfighting* - and related *business* - domains intersect...

Cyberspace Domain is contained within and transcends the others

In relation to other mission areas... run by different *Communities Of Interest* (COI)

Cyberspace is a blend of exclusive and inclusive ties
Frequently the COI boundaries / MOAs are implicit
These Venn connections / COIs are pervasive

Numerous, dynamic “COIs” dominate relationships - *adding Complexity & Comms, & Control overhead* - causing “*cross domain / COI*” DATA sharing effects

Do NOT underestimate this aspect – affects CONTROLS needed for PbD!
Information Dominance: Comprehensive Data Strategy

Right Info, Right Time, Right Place

RAW --------------- REFINED --------------- RIGHT

Networks and Transport

Master Data and Metadata
- Data Definitions
- Auth Data Source
- Reference Data
- Data Valuation / Tagging
- Indexing
- Metadata Repositories
- Registration

Data Structure
- Taxonomy
- Data Models
- Process Workflows
- Data Lifecycle

Data Architecture
- Sizing
- Storage
- Processing
- Movement
- Retention and Deletion

Data Security
- IA
- Compliance
- Cross Domain
- PII
- Access Controls
- Releasability

Cyber for PbD must be E2E

PbD is enhanced with a DATA-centric architecture
IA / Cyber and **DATA** must be built 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.

And, people and processes too!

How does the DATA move and what are the privacy protections / controls at each layer?

---

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

Thus, the DATA, IA/cyber controls, interfaces and profiles in each element / boundary must be quantified / agreed to upfront!
“Notional” Data Centric Architecture (DCA)
iso the required privacy needs

IA / Security / cyber (e.g., defense in depth (DiD))

Supports quality / assured data (with a pedigree / provenance)

Data is either at rest, being processed OR in transit

Must account for the “four ‘Vs’”
Volume, Variety, Velocity and Veracity

A PbD Cyber Model accounts / translates the data 4V’s into privacy attributes and controls
DCA Cyber Model for *Data-Centric Security* (DCS)

Business Risk Management Approach is the core Tenet

End2end / lifecycle access control and encrypt everywhere

Open Architecture, modular capabilities, loose coupling

Common standards & specifications – focused on APLs (NIAP, etc)

SCM / SIEM, predictive analytics, & automated security policy

Cyber designed into an integration and interoperability (I&I) “EA”

**THESE are the factors *all PbD Cyber Models* will accommodate!**
Principles of Data-Centric Design

Data-centric design recognizes that the essential invariant is the *information exchange between systems or components*. It describes the exchange in terms of a "data model" and data producers and consumers of the data; and it relies on four basic principles:

• **Expose the data and metadata.** Data-centric design exposes the data and metadata as first-class citizens, and uses them as the primary means of interconnecting heterogeneous systems. "Data" is the primary means of describing the "world as it is," independent of any component-specific behavior. Metadata refers to information about the data's layout and structure. A data-centric interface is defined by the metadata, which must contain all of the information required to encode and decode the data in a given format.

• **Hide the behavior.** Data-centric design hides any behavior and direct references to operations or code of the component interfaces. A component interface cannot embed any component-specific state or behavior. Components implement behaviors that can change the data or respond to changes in data (the "world model").

• **Delegate data-handling to a data bus.** Separation of data handling and application logic is necessary for loosely coupled systems. The component application logic should focus on manipulating the interface data, not on its management and distribution. The responsibility of data handling is delegated to a data bus; and it is the authoritative source of the world model shared amongst the components.

• **Explicitly define data-handling contracts.** Data handling contracts should be explicitly specified by the application at design time, and enforced by the data bus at runtime. The delivery contracts specify the QoS attributes on the data produced and consumed by a component, including timing, reliability, durability, etc. The data bus examines these "contracts," and if compatible, establishes data flows. The data bus then enforces QoS contracts, thereby providing the application code clear, known expectations.

*Follow the data – secure the “four V’s” – at rest, in processing and in transit.*
Notional Data Centric Strategy Requirements

Understanding the Complexity

- On-demand Data Access
  - Understanding of anything associated with global domain
- Managing Uncertainty
  - Threat vs. Capability Based Response Plan
- Cross Agency & Community Integration
  - No established Core Data Structure (data or processes) to leverage

Situational Awareness (SA) is effective understanding of anything associated with the global maritime domain that could impact the security, safety, economy, or environment of the any business / organization...

SA tenets are:
- Big Data Analytics – analysis over large corpuses of data regardless of location
- Content Network Distribution – efficient data distribution over networks w/limited bandwidth to include C2
- Cloud Computing – surging of platform, software and infrastructure services
- Agile Development Operations – the rapid development and delivery of software to the operational environment

Privacy must be accounted for at all levels & types & places
Data Centric Approach

- Data-centric approach / middleware *maintains state*
- Infrastructure manages the support to the “4Vs”
- Developers write applications that read and update a virtual global data space

Popular standards: DDS API, wire spec

*Privacy must be accounted for at all levels & types & places*
Data and Information Architecture
(one more view of a DCA)

DATA GOALS & Objectives
1 (Ingest): Identify, Understand, Catalog & Publish Organizational Data at or as close to source as possible
2 (Analyze): Create & Publish algorithms & techniques for improved analysis & automation of information tasks
3 (Prioritize): Prioritize information so that different information flows are invoked with available bandwidth

DCA major elements

• Data-centric architecture (DCA) *decouples designs and simplifies communication* while increasing capability and easing system evolution... DCA can link “systems of systems” into a coherent whole, using an open standard — OMG DDS... Transports, operating systems, and other location details do not need to be known, and allowing adaptation to performance, scalability, and fault-tolerance requirements

• Define and modularize **DCA components** = create specifications (capabilities and profiles)
  - DCPS, DDSI, DataReader, DataWriter, Pub / Sub. Java, mobile code, widgets, storage SW, middleware, services, ESB, etc... these have cyber security aspects to assess

• Use **OMG / DSS** as a reference – AND - the *data schema / tagging* authoritative sources

**Data Centric Services**
... compression, capture, extract / transform, tagging, cleansing, format indexing, categorization, sanitization, quality, mining, record linking / association, metadata management, reference / authoritative sources, backup / recovery, storage / archiving, and record retirement / disposal ...

**Other data services** to accommodate
... Data Access, Information Mapping/Taxonomy, Mission Data Ingest, Information Tracking, Data Purging, and Data Governance ...

SECURE DCA services  =  **Data Centric Security (DCS)**
A PbD cyber model must map the data methods, controls, & services into privacy aspects.

+ Standard IA / CND / security suite = “IA devices” = Firewall, A/V, IDS/IPS, Crypto / Key Management, & VPN
+ Network infrastructure = “CCE” = common core computing / network environment - with ‘IA – enabled’ devices
Data centric services and cloud evolution

*PaaS objective* for combined / hybrid environments (with premise and cloud)

On-premises “Pre-cloud”

<table>
<thead>
<tr>
<th>You manage</th>
<th>Vendor managed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td></td>
</tr>
<tr>
<td>Data</td>
<td></td>
</tr>
<tr>
<td>Middleware</td>
<td></td>
</tr>
<tr>
<td>OS</td>
<td></td>
</tr>
<tr>
<td>Virtualization</td>
<td></td>
</tr>
<tr>
<td>CPU/Storage</td>
<td></td>
</tr>
<tr>
<td>Networking</td>
<td></td>
</tr>
</tbody>
</table>

Infrastructure as a service “Cloud v1”

<table>
<thead>
<tr>
<th>You manage</th>
<th>Vendor managed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td></td>
</tr>
<tr>
<td>Data</td>
<td></td>
</tr>
<tr>
<td>Middleware</td>
<td></td>
</tr>
<tr>
<td>OS</td>
<td></td>
</tr>
<tr>
<td>Virtualization</td>
<td></td>
</tr>
<tr>
<td>CPU/Storage</td>
<td></td>
</tr>
<tr>
<td>Networking</td>
<td></td>
</tr>
</tbody>
</table>

Platform as a Service “Cloud v2”

<table>
<thead>
<tr>
<th>You manage</th>
<th>Vendor managed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td></td>
</tr>
<tr>
<td>Data</td>
<td></td>
</tr>
<tr>
<td>Middleware</td>
<td></td>
</tr>
<tr>
<td>OS</td>
<td></td>
</tr>
<tr>
<td>Virtualization</td>
<td></td>
</tr>
<tr>
<td>CPU/Storage</td>
<td></td>
</tr>
<tr>
<td>Networking</td>
<td></td>
</tr>
</tbody>
</table>

Software as a service

<table>
<thead>
<tr>
<th>Vendor managed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
</tr>
<tr>
<td>Data</td>
</tr>
<tr>
<td>Middleware</td>
</tr>
<tr>
<td>OS</td>
</tr>
<tr>
<td>Virtualization</td>
</tr>
<tr>
<td>CPU/Storage</td>
</tr>
<tr>
<td>Networking</td>
</tr>
</tbody>
</table>

Securing the data and application layers *and inoculates them from lower layer risks*
Cyber Security is Complex from a Technical Perspective

**What factors must be addressed in PbD?**

**Which ones are inherent in the IA/CND/Cyber suite?**

(From an IBM security brief)
What matters in Cyber? Who says?
DoD Cyber Priorities Council - S&T Roadmap - Key Capability Areas “4+1”

Assuring Effective Missions
- Assess and control the cyber situation in mission context
- Support essential business success functions

Agile Operations
- Dynamically reshape cyber systems as conditions/goals change, to escape harm
- Autonomous responses and C3 Tools

Resilient Infrastructure
- Withstand cyber attacks, and sustain or recover critical functions
- Environment is robust and self-healing

Trust
- Establish known degree of assurance that devices, networks, and cyber-dependent functions perform as expected, despite attack or error
- Mixed trust levels in heterogeneous space

A PbD Cyber Model must also accommodate these key I&I needs
A cyber end-state stresses **encapsulation** using **secure communications**

( just like OOP )
SO just what are we trying to orchestrate?

An integrated “Cyber Defense in Depth / Breadth (DiD)” EcoSphere using dynamic lag and lead feedback, establish proactive, dynamic CND / IA Defense

Cyber “I&W”

“Virtual Storefront”

NMS / Security Management tools

IA & CND

Defensive assessments

Incident results

V&V / C&A

I&W / SCM

CERT / FBI

Red Teams

“SA” *****

(Sensors, CNA/E inputs, OpSec, Intel, etc…)

predictive feedback (leading indicators)

forensic feedback (lagging indicators)

“Virtual Storefront”

Users & CoC

Change “soft” settings (takes secs to mins)

Upgrades (developed & installed) (takes days to months)

With big data / predictive analytics / SIEM (near real-time!)

All “PbD” capabilities (including IoT) must be well integrated into the cyber ‘system’
Building a Trusted Cyber Infrastructure

“= an adequately assured, affordable, net-centric environment”
(built from disparate heterogeneous capabilities that we must integrate into a homogenous cyber ecosphere!)

Focus on a few core capabilities & devices
= PC, routers, IA suite, Servers, & SANS – all with access control

Standard IA/CND suite
FW, A/V, IDS/IPS, CDS, VPN, Crypto, Key Mgmt, Security Policy

HW / FW
Secure OS kernel
Secure Virtual Machine
Strict access / ZBAC
ALL OSes (MS, Mac, Unix)

Make IA / CND / security a commodity:
Use & enforce IA building blocks = APLs/PPLs -> “NIAP”
Interoperability and Compose-ability are built in upfront and help dramatically reduce complexity and ambiguity

Thus....establishing known risks & pedigrees:
Reduces attack surface, risks & TOC = baseline for PbD & IoT!
What will a cyber model provide?

<table>
<thead>
<tr>
<th>Driver</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interchangeability</td>
<td>To put each of (two things) in the place of the other, or to be used in place of each other.</td>
</tr>
<tr>
<td>Integratability</td>
<td>To form, coordinate, or blend into a functioning or unified whole. To incorporate into a larger, functioning or unified whole.</td>
</tr>
<tr>
<td>Replaceability</td>
<td>One thing or person taking the place of another especially as a substitute or successor.</td>
</tr>
<tr>
<td>Extensibility</td>
<td>The ability to add new components, subsystems, and capabilities to a system.</td>
</tr>
<tr>
<td>Interoperability</td>
<td>The ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces, and to use the services so exchanged to enable them to operate effectively together.</td>
</tr>
</tbody>
</table>

An Open Cyber Architecture requires Interoperability at a higher level than just Key Interfaces / Protocols and must address STATE.

**Data-Centric Security** provides an **Explicit Understanding of State**

**Within an overarching defense in depth/breath (DiD) cyber posture**

From 2012 RTI
Notional DiD Ref Arch

DiD has three main elements: **people** (train and enforce good behavior), **operations** (policy, management, C&A, COOP) and **technology** (IA criteria, evaluated products, risk assessment, layered defense), *we propose an OPF EA for the latter here*.

**Layered protections:** (1) Networks and Infrastructure, (2) Enclave boundaries, (3) Quantify security robustness for all components (aka – use NIAP), (4) use robust key management and PKI (IA&A), and use IDS/IPS (detection capabilities)
- *Using common cyber capabilities, with known pedigrees / assurance (APLs/VPLs -> NIAP)*

**OSI stack protections:** (1) restrict access, port security (2) VLANs, Static ARP, (3) VPNs, NIDS, content filtering, (4) Firewalls, ACLs (5) IAVA, crypto, authentication, (6) IDS, audits, (7) anti-virus, secure software (SDLC), patches... AND effective IA&A / access control methods...

**Manage / enforce IA controls at each layer / capability!**
Use existing IA controls management tools, like the below DISA link:

http://www.disa.mil/Services/Network-Services/Video/DVS-G/Becoming-a-Customer/VTF-DIACAP/Assigning-IA-Controls


Also the NSA’s Community Gold Standard. https://www.iad.gov/iad/CGS/cgs.cfm

+ As applied law the **NIST cyber security framework**. *This is a MUST DO reference guide!* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

**NOTE** - This is a *general requirements depiction of a DiD* - Using these general NIST and GIAC notional references


Essential DiD EA elements

Reduce complexity and unknowns:
Limit numbers, types and versions of IA capabilities (*drive to commodity state*)
Only use common cyber capacities with known pedigrees (& enforce APL/VPL = NIAP)

**DiD enterprise architecture (EA) based on layers / IA controls therein**
Define specifications for and modularize the below cyber building blocks (IDEA -> DFIA)
Include inheritance, interface controlling parameters, and required standards **AND profiles**
Map the DiD EA back to the organization’s risk management plan, key issues / risks therein

**CONOPS for notional DiD EA, including CM, governance, exceptions.**
Need to take a “mission assurance” perspective, with affordability / RoI
Integrate and Implement DoD / NSA common practices (SCAP, Risk, etc)
*Manage and enforce an effective, enforced Cyber CM/Hygiene posture and IA&A/IDAM!*

The basic cyber building blocks of security... a limited and controlled set of IA building blocks for a few main classes:
- **IA devices** (crypto, EKMS, PKI/CAC, A/V, VPN, Firewall, IDS/IPS, HBSS, HAP/TPM devices, reference monitor, etc)
- **IA enabled capabilities** (OS, web browsers, messaging systems, screening routers, etc)(and the IA/WSS standards!)
- **Services and Applications** (define a standard "security container" for each service, ideally a “class”)(see NSSI IA controls)

*DATA capabilities* _DCPS, DDSI, Pub / Sub, Java, mobile code, widgets, storage SW, middleware, services, ESB, etc_

-- **Critical HW/SW devices** (catch all for any special / unique IT/IA capabilities, these are generally low level aggregated devices / modules (e.g., “Tessel / IoT”), are a new “class” of IT/IA functions to standardize to) **AND actually use the “TPM”!**
- **PIT** (“Platform IT” – government designation of ‘unique’ capabilities that exempt them from more rigorous “C&A” V&V)

WE have what we NEED in cyber security – **now MANAGE it well**!
IBM’s Approach to Cyber Security
(As one reference model to compare to)

**Assurance**
Enable trust and confidence in IT through software and system assurance
- IBM Integrated Product Development Process
- System z Integrity Statement
- Trusted Foundry
- IBM High Assurance Platform
- Continuous Software Quality
- IBM Secure Blue

**Intelligence**
Stay ahead of the threat by monitoring the attack landscape and anticipating new threats
- IBM X-Force
- IBM Managed Security Services
- System S Event & Streaming System
- High Performance Computing
- Information Risk & Compliance
- Smart Surveillance

**Open Architecture**
Enable security and privacy with an open, standards-based architectural approach
- Open standards leadership in DMTF, IETF, OASIS, TCG, W3C, …
- SOA & Web Services Security
- IBM Security Blueprint
- IBM Trusted Identity
- Fine-grained Security
- Trusted Virtual Data Center
- UK/US ITA, IBM OCR, EU FP7 open research

**Process**
Provide visibility, control and automation through CoBIT and ITIL-based service management
- IBM Service Management Platform – asset management, problem & incident management, change & release management, etc.
- IBM Process Reference Model for IT (PRM-IT)
- IBM Rational Unified Process
- Patch management for virtual images

Any cyber model must be useable at the **implementation / execution level!**
What’s a user, operational centric cyber model look like?

Model may Include:
- Processes ...
- Policy ...
- IA/CND suite (= Firewall, A/V suite, IDS/IPS, Crypto, Key mgmt.) ...
- Mobile / wireless, ...
- Network (server, SANs, client, etc) ...
- Interfaces, protocols, specifications
- SCM. CDM, SIEM, & analytics etc.

How much “cyber” is enough?

Notional architecture view for one perspective....
+++ Cyber Model for PbD +++

Data Centric Security (DCS) enabling Privacy

- Data Encryption end2end – focused on services / applications (re: PaaS model)
- Enterprise access control – E2E multi-factor authentication (re: RAdAC objective)
- Security Policy management – Automated, serve multiple ‘avatar’ levels in PbD
- Application engineering - Common model for services, apps, phones, APIs, etc

*Added on top of the standard IA/CND/Security cyber suite*

**Monitoring, tracking, assessment** = SCM / SIEM, DLP / RBS, Predictive Analytics, etc

(With an integrated “AI/smart” correlation / POA&M tool complementing SIEM – mapped to cybersecurity framework steps)

**Standard IA / CND suite** = “IA devices” = Firewall, A/V, IDS/IPS, Crypto / Key Mgmt, & VPN

**Typical Network infrastructure** = “CCE” = common core computing environment

(with ‘IA – enabled’ devices - operating systems, database management, network management and web browsers)

Using existing capabilities in each “+” capability – develop an open privacy framework (OPF)
Cyber 4 PbD - Specifications

**DataSec** required capabilities for PbD (enterprise, end-to-end encryption, data-centric series and access control)

**User security:** PbD requires that only authenticated and authorized users have access to the privileged parts of their PbD enabled applications. To restrict access to other users, DataSec brings 5 factor authentication which cover location, time, biometrics and other sensor data from the user before allowing access to the more sensitive parts of a PbD enabled application.

**Security against data breaches:** Data breaches are now a routine occurrence and with the proliferation of cloud computing much of the sensitive data processed by PbD conscious applications is now resident in cloud datacenters. DataSec’s CipherDb and CipherStor products enable a PbD application to not only have data-in-transit and data-at-rest security at the back end but also allows the trust footprint to be smaller. This means that the database servers, file servers, the administrators, data center technicians or any intermediate equipment can all be untrusted. This dramatically reduces the chances of any accidental or malicious data breaches boosting the confidence of the PbD application and simultaneously simplifying compliance.

**Better operational awareness:** Security exceptions for both user security and data security are logged for audits and outlier events raise alerts to users and application owners.
Cyber 4 PbD - Specifications

**SecPolicy and SecSIEM** required features / overall capabilities for PbD:

- **Policy authoring:**
PbD needs an intuitive, user-centric privacy policy authoring feature for users to set their privacy policies (“informational self-determination”). Note that SecPolicy is by no means restricted to access control policies.

- **Policy enforcement:**
PbD needs a tool that maps these intuitive privacy policies into technical enforcement (access control, confidentiality etc.) across the information lifecycle and software development lifecycle, and configurable “privacy code libraries”. ABAC access controls and encryption are example mechanisms that can be configured to enforce the privacy policies.

- **Policy audit:**
PbD needs a user-centric tool that lets users verify (audit) that their policies are enforced correctly. SecPolicy & SecSIEM help audit “as-is” against the policies.

- **Complex data policies:**
PbD needs a user-centric tool that supports “data minimization” and “non-identifiable interactions”. PbD therefore needs to enforce complex, contextual, dynamic, fine-grained information flow policies to minimize access to data: “data minimization”; non-collection/-retention/-use; de-identification; redaction/filtering; strong default policies

- **Privacy-security policy mapping:**
PbD policies, while privacy policies at a high level, will often boil down to technical security rules (e.g. access control, filtering/redaction, encryption) when technically implemented – SecPolicy MDS (model driven security) bridges the gap.

- **Embedding privacy into systems/applications:**
MDS helps bake policies into the design and architecture of the systems in an effective, manageable, verifiable way.

- **Enforce full-lifecycle information flow control:**
PbD needs cradle-to-grave privacy policy information for information, which requires info flow control policies to be enforced (SecSIEM!).
Cyber 4 PbD - Specifications

**SW/AppSec** (Apps / Services & Phone/Mobile) required features / overall capabilities:

**Automated**: PbD dictates for the need of automated policy authoring, enforcement and auditing. If the security is based on manual processes, points of error, vulnerabilities, and noncompliance are likely to be created. Manual security processes also defeat the dynamic nature of the enterprise infrastructure.

**Ubiquitous**: Omnipresence; The same control and management implementation should be operable on any environment, regardless of physical location, operating system, virtualization platform, or deployment method used. Policies defined by PbD should govern all the entities (hardware and software) and their operation (message exchange, file storage, etc.) within the organization.

**Scalable**: The system should automatically grow and contract to meet the changing demands of applications and underlying infrastructure. PbD must automatically provision the appropriate security controls and maintain appropriate threat and compliance monitoring as infrastructure environments scale up or down.

**Multi-Layer Visibility**: Privacy challenges exist in both hardware and software level. SW/AppSec solution considers privacy as an integral part of security and hence provides comprehensive solutions at each operational hardware and software layer.
Open Privacy Framework (OPF) Foundation
(reference architecture implementation technical approach)

Interconnected Applications are Protected and Monitored

Full Privacy Information Lifecycle Management
C4P OPF functions and capabilities

**OPF-PM: - Policy Management** - PbD needs a manageable intuitive, user-centric privacy policy authoring feature for users to set their privacy policies ("informational self-determination") governing users, systems, applications, and interactions (information flows).

**OPF-PE: Automated Security Policy Enforcement & Alerting** - PbD needs a tool that enforces technical privacy rules and configurations generated by OPF-PM technically (access control, confidentiality etc.) across the IT landscape (multiple layers of the system/application/network/VM etc.), across the information lifecycle and software development lifecycle.

**OPF-CM: Compliance Management & Automation** - PbD needs a user-centric tool that lets users verify (audit) that their policies are enforced correctly.

**OPF-SD: System (of Systems) Discovery** - The system automatically generates a model of the enterprise networks, systems, applications, information flows, users etc. This “system description” plays a similar role as Common Criteria’s “Target of Evaluation”.

**OPF-IM - Incident Monitoring**: The solution needs to be able to watch network activity (including bandwidth usage), access control incidents, and more, by capturing automatically captures and analyzes anomalies detected in PbD appliances and/or locally installed Policy Enforcement Point (PEP) software proxies.

**OPF-PS - Presentation of (Current) Status**: - The solution displays the current privacy posture on a continuous basis in a consolidated fashion.

**OPF-SC - Security Administrator Collaboration**: The solution also includes a way for administrators to collaborate to resolve issues (e.g. a secure social network to facilitate collaboration between administrators).

**OPF-ER - Encryption for Data at Rest and Transit ("ET")**: The solution also needs to protect information at rest using encryption. The cryptography is configured and managed in a unified way together with the other policies in OPF-PM.

**OPF-AH: User/Machine Authentication**: The solution needs to also support the appropriate level of authentication. User Authentication should be based on 5 factors, namely the user memorized password or PIN, a cryptographically secure time-based one time password or token, successfully matched facial patterns of the user, location of user as well as time of request by user.

Cyber enabled PbD must be well integrated into your risk management portfolio!
The Integrated Business RM Approach
+ Making the Risk Management Plan (RMP) work! +

Company Vision
(business success factors)

Security Policy
(mobile, social media, etc)

C&A / V&V
(effective / automated)

Known Baseline
(security architecture)

Insider Threat
Company Intel
(open source, FB, etc)

CMMI / Sustainment
(SoPs / processes)

SCM / SIEM
(monitor / track / mitigate)

MSS / CISO
(3rd party IV&V support)

Privacy by Design
(manage PII, HIPAA, compliance)

Education / Training
(targeted, JIT, needs based)

Cyber insurance
(broker & legal council)

Common Business RMP model (RMF / COBIT & Risk IT)
AND IAW the NIST Cybersecurity Framework (CAR / ESA)
Cyber Security opportunities
(Cyber can both protect your business AND enhance the bottom line!)

IT / Cyber Global factors – user pull

World-wide B2B
Trust / cloud / sharing

IoT / M2M
Automation / Sensors

Consumerization of IT
Phones / wireless / apps

Privacy / Data
IP / PII / compliance

GAPS / Needs
(from the Federal cyber priority council S&T gaps)

TRUST
Distributed / MLS

resiliency
SW / apps / APIs / services

agile operations
BE the vanguard / integration

effective missions
Business success factors

Vulnerabilities / Threats
(Verizon BDR, Forbes, etc threat reports - what ails us most)

CM / Hygiene
patching / settings

Access control
Authentication is key

TOP security mitigations
Whitelist, patch, limit access

Risk Mgmt
Adhoc / not global

Future Opportunities

Effective Business Risk Management (BRM) = cybersecurity framework (CMMI / FAR)

Focus on reducing business risk...
Managed security services (MSS) & cyber insurance ...

SIEM / SCM
QA hygiene / sensors
“ESA” / simple tools!

Mobile Security
Poor apps / IOS weak
billions users = volume

Mitigate Obsolescence
Minimize patching, legacy vulnerabilities
OA / modularity / APIs & SCRM

Data Security
Predictive analytics
Privacy by design
“Overall Cyber Way Forward”
(given all the unknowns, variables... this is “one” approximately correct path...;-))

• **Company Vision** embedded in **Cyber Plans/RMP**...
  • support business success factors, know what the USER values

• **Risk Management Plan... RMP**
  – *Use NIST’s RMF! (or COBIT)* Have a dynamic, realistic RMP supporting your business units objectives... *as you ARE betting your livelihood on cyber!*

• **Effective, enforced Policy**...
  – Embedded in core business success factors, rules to enforce statutory, legal mandates, key processes, to enforce behavior (pos & neg incentives)

• **The Basics, basics, basics**...
  – New toys matter little, if your environment(s) are not managed (*SCM / SIEM!*)
  – *Poor hygiene / CM causes almost ALL security incidents* (80 - 95%)

  PbD must fit in ALL of these too!

SO... *Don’t just admire the “cyber problem / threat” --- DO something!*
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

DO the cyber BASICS well, for things, people AND processes
invest in select new capabilities, protect privacy and follow your RMP!!!
PbD links

ONE perceptive...

+++ and SOME other links too
http://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/
http://www.futureofprivacy.org/privacy-by-design/
http://itlaw.wikia.com/wiki/Privacy_by_design
https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=pbd-se


Useful numbers - https://www рискbasedsecurity.com/reports/2013-DataBreachQuickView.pdf
Integration, execution is everything
as if you can’t implement well, it costs you everywhere!!!

The quantitative benefits of systems integration and interoperability (I&I) 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

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...

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

Plan for “I&I” - then double it

The best capability means little, if it stays in the box
What is Cyber Hygiene?
(and the HUGE percentage of security incidents caused by lack of it)

National Security Agency (NSA) (80-85%)
NSA IAD director “Just improving the “IA Management” aspects of security (aka, hygiene factors) will reduce security incidents by over 80%

IA Management = CM, monitoring environment, follow SOPs

Verizon (2012 Data Breach Investigations Report) (up to 97%)
Report covered 855 incidents, 174 million compromised records
--- Breaches almost entirely avoidable through simple or intermediate controls
Threats: 98% from external agents, 81% from hacking... 69% used malware

Navy (our “red team” / NCDOC) (over 90%)
Poor “accountability” factors = willful misuse, lack of CM (& IAVA / patches), not having / following procedures, weak enforcement of policy, etc
They must spend all their time / resources fixing the “easy” vulnerabilities...

HYGIENE = Maintaining / monitoring your IA / Security / cyber equipment settings
As any incorrectly set cyber capabilities makes them much less effective!
Cyber Hygiene — the many faces of neglect

Our IA/CND/Security cyber suite is quite good – IF maintained!

- **Equipment settings**
  - (FW, A/V, IDS, etc)
  - Monitor / enforce

- **Social media**
  - Content & settings
  - Restrict sharing / privileges

- **Incident reporting**
  - No incident too small
  - Notify USCERT / FBI

- **Controlled Access**
  - Enforce least privilege
  - Separate / rotate duties

- **Security Awareness**
  - ALL levels – reinforce
  - Incentivize – good vs bad

- **Maintain Cyber Suite**
  - Patches, upgrades, etc
  - (compliance ≠ security)

- **Standard operating procedures (SOPs)**
  - USE / enforce them

- **Know your security baseline**
  - AND employ SCM / SIEM

- **Privacy and “PII”**
  - Enforce policy (note - “EU” is stricter)

Forbes top threats for 2013:

- “MOST” have “CM / hygiene” AND / or “access control “aspects
- Social Engineering; APTs; Internal Threats; BYOD / mobile malware;
- HTML5; Botnets; CLOUD infrastructure, & Precision Targeted Malware
Complexity of Enterprise IT Systems is Increasing
AND so is the associated Cyber Security – from sensor to cloud!

Key challenges in the problem space
- Network-centric, dynamic, very large-scale “systems of systems”
- Stringent simultaneous quality of service (QoS) demands
- Highly diverse & complex problem domains

So - what is ‘good enough’ security?

Key challenges in the solution space
- Enormous accidental & inherent complexities (& covert channels)
- Continuous evolution & change
- Highly heterogeneous platform, language, & tool environments

Mapping & integrating problem artifacts to solution artifacts is “wickedly” hard

Follow the DATA... where is it... who has it – how sure are you?
DoD CND (and “Cyber”) Defense in Depth

The “smart” integration and collaboration between MANY needed IO & IA functions

Secure Locally – Defend Globally

Cyber = “mostly” Life-cycle education and proactive, dynamic defense….

(From NCDOC briefs)
Capabilities Needed for “Information dominance”

Schema of maneuver (positioning for effect)
Assured C2 (OPCON / INFOCON)
Cyber (IA/CND protections & CNE/CNA (covert))
Kill / Effect Chains (maximize left side - ISR / I&W)

“ID” = Decision superiority

“Knowledge”
Quality / assured data = value, pedigree, provenance
Information environment (right data, to right folks at right time)
WAN/transport, network, cloud, data centers, cyber, governance...
Infrastructure / services / apps = trusted information systems

“IT / network”

Battlefield victory requires dominant position and maneuver
Which require best possible information, before the opposition can: (1) get his own information; (2) react to your movements or (3) infiltrate your environment...

The best possible info is ID:
A DiD with trusted information systems providing assured / quality data, facilitating all levels of command decision superiority
‘ONE’ Target Data Architecture view

Client Tier
- Web-based thin clients such as browsers or handheld devices
- Desktop based clients (Java, C/C++, .NET, COM) such as Analyst Workspace.

Middle Tier
- Data Access Layer (DAL)
- Business Components

Database Tier
- RDBMS
- Intelligence Databases
  - (such as GM, POINT, IMDB, DHDB, and ORDS)
- Support Databases
  - (such as ISHOPD and MIDB SUPPORT)
- Imagery Services (ITS)
- Track Manager (TMS Master)
- Message Services (UCP)
- Exchange Mail Services

Web Tier
- Java Server Pages (JSP)
- Web Services

Support Services
- XIS (FL, JMV, TMS, AFW, UCP, TMSV)
- JAF

COE Services
Sample DCA view... ONE of many... what DATA can be passed where & how???
Cloud Security Summary

Security in the cloud is **likely better than you have in-house**

* Security is the **SAME everywhere** – ‘WHO does which’ IA controls changes
* Don’t sell cloud – offer **security capabilities** instead – end2end services
* Few are “all in” the cloud @ 100% - Hence **TWO environments** to manage
* ALL must use the same **cloud security standards** (and QA in SLA)  
* Implement **SCM / SIEM** – **integrate cloud metrics / status** (& QA the SLAs)
* **Service Level Agreements (SLA)** not sufficient – trust but verify (*Orchestration SW ?*)
* **Encrypt** everywhere - Yes more key management, but risks greatly reduced
* **Data owners always accountable** for PII / privacy / compliance (& **location**)
* **Update Risk management Plan (RMP)** = Comms, COOP.... with **cloud R&R**  

For more details see paper: **Cloud Security – What really matters?**

At  [http://www.sciap.org/blog1/](http://www.sciap.org/blog1/) (under *Cyber Body of Knowledge*)
Mobile Security perspective

*Check Point’s* global survey of 768 IT professionals conducted in the United States, Canada, United Kingdom, Germany, and Japan. The survey gathered data about current mobile computing trends...

**Key Issue / Risk Findings:**

- **Extensive use of mobile devices connecting to corporate networks**
  - 89% have mobile devices such as smartphones or tablets connecting to corporate networks
  - Apple iOS is the most common mobile platform used to connect in corporate environments

- **Personal mobile devices that connect to corporate networks are extensive and growing**
  - 65% allow personal devices to connect to corporate networks
  - 78% have more than twice as many personal devices on corporate networks vs 2 years ago

- **Security risks are on the rise because of mobile devices**
  - 71% say mobile devices have contributed to increased security incidents
  - The Android mobile platform is considered to introduce the greatest security risks

- **Employee behavior impacts security of mobile data**
  - 47% report customer data is stored on mobile devices
  - Lack of employee awareness about security policies ranked as greatest impact on data security
  - 72% say careless employees are a greater security threat than hackers

- Contrast that 75%+ of users with personal devices with the percentage of employers who have a coordinated and comprehensive mobile security strategy in place (10%), and you see the problem...

*** NSA/CSS “Mobility Capability Package” = Architecture / Certification - a MUST DO ***

http://www.nsa.gov/ia/_files/MobilityCapability_Pkg_Vers_2_0.pdf

**Mobile / wireless are HUGE threat entry points!**