

# Privacy Pays

Privacy is a **GLOBAL** concern  
**AND**  
 and *business opportunity!*

*Mike Davis*

Risk Management / Cyber Security  
 Consultant, MSEE, CISSP (Retired USN)  
**Mike.Davis.SD@gmail.com**

**Bill Bonney**

Cyber Security | Internet of Things  
 Security | Identity Management  
**wqbonney@gmail.com**

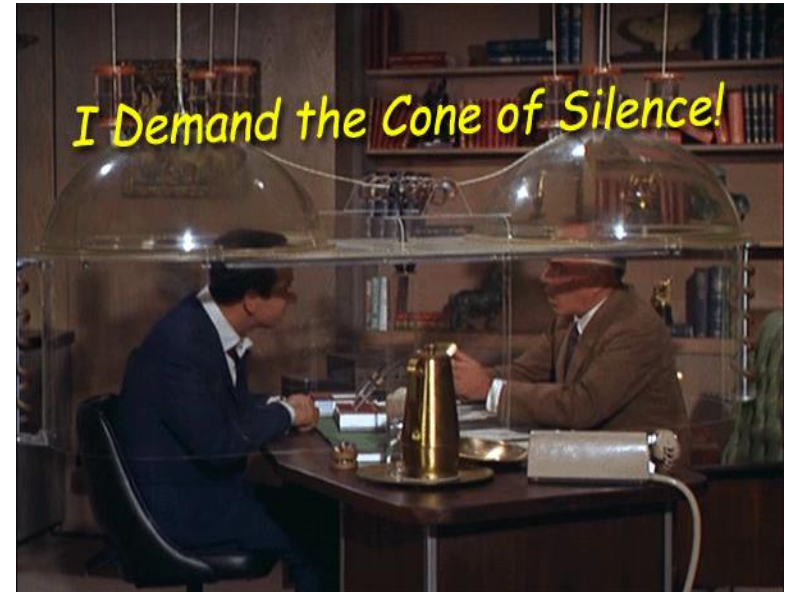


Detailed “Cyber Facilitated Privacy by Design” paper at:

<http://www.sciap.org/blog1/wp-content/uploads/Cyber-4-Privacy-Design-IEEE-CE-article.pdf>

# WHY do we need to care about Privacy?

- Over one **BILLION** records stolen in 2014 (just the ones we know about)...
  - Cost = ~\$200 / record
- “**Unconstrained**” third party liability and lawsuits – and heavy fines / damages
  - Coming anytime, from anyone, from anywhere
- **VALUE** is all about an organization’s enterprise risk management effectiveness
  - Using privacy as a lens captures many views, including compliance
- Get the **C-suite attention** better, and Directors & Officers / line managers
  - Directors & Officers can be held personally liable for lack of due diligence



”Privacy isn’t something I’m merely entitled to...*it’s an absolute prerequisite.*” – Marlon Brando

# HOW will Privacy PAY?

## 1 – **Reduce expenses and greatly decrease risks**

- A – Reduce insurance costs by SEVERAL factors and levels
- B – Minimize liability, especially 3<sup>rd</sup> party (data breaches, etc)
- C – Spend scare security dollars much more effectively

## 2 – **Minimize complexity, increase effectiveness**

- A – Too many ‘high priority’ needs – focus on the top few
- B – Too many moving parts, linkages (re: “*clarify the fog of cyber*”)
- C – Unclear integration and interoperability between factors

## 3 – **Better communicate, improve brand / market**

- A – Sell ‘security’ better using a privacy protection message
- B – Privacy, though itself is fuzzy, is a global concern and need
- C – Privacy protection processes integrates most cyber elements

# Data Breaches are expensive

**Cost Of A Data Breach Jumps every year - *average cost of an attack is now \$5.9M* \***

- More customers terminated their relationship with the company who had a breach
- Malicious or criminal attacks rather than negligence or system glitches were the main cause

**Target, Home Depot, Chase.. Just the visible big ones**

- National Archive and Records Administration, 2008: 76 million records
- Heartland Payment Systems, 2008-2009: 130 million records
- Sony online entertainment services, 2011: 102 million records
- Epsilon, 2011: 60 million to 250 million records
- Target, 2013: 110 million total records
- Home Depot, 2014: 56 million payment cards

**Target breach cost \$200M to reissue cards and \$100M to upgrade systems**

\* Source: <http://essextec.com/sites/default/files/2014%20Cost%20of%20Data%20Breach%20Study.PDF>

# Verizon Data Breach Investigations Report - DBIR (2014)

**10 years of data, 63,437 incidents, 1367 breaches, 95 countries**

WHAT - 92% incidents described by just nine patterns

Sectors - Top 3: Public (47, 479), Information (1132) and Finance (856)

Top 6 Threats (%)	POS intrusions	31	Web App Attacks	21
	Cyber espionage	15	Card Skimmers	14
	Insider misuse	8	Crimeware	4

Mitigations

Restrict remote access

Enforce password policies

Minimize “non” POS activity on those terminals

Deploy A/V (everywhere, POS too)

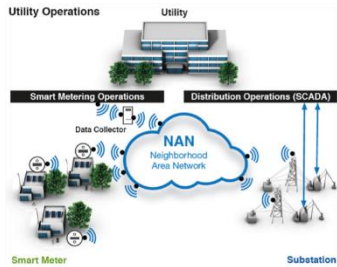
Evaluate threats to prioritize treatments

Look for suspicious network activity

Use two-factor authentication



# Strange and Risky New World



- Deloitte: There will be 1 **billion** new IoT devices deployed in 2015.
- Wearable and home automation devices = thousands of units, industrial devices = millions.
- 70% of top 10 home IoT devices vulnerable, 80% have privacy risks according to HP.
- The “*World Economic Forum Global Risks 2015*” report ranks "data fraud or theft" and "cyber attacks" as the number 9 and 10 (respectively) risks to the global economy in terms of likelihood.

## EDITORS' TOP PICKS

SEE ALL



Belkin WeMo Switch + Motion  
Starting at: **\$79.95**  
★★★★☆



Quirky Aros Smart Window Air Conditioner  
Starting at: **\$249.00**  
★★★★☆



SmartThings Know and Control Your Home Kit  
Starting at: **\$199.00**  
★★★★☆



Nest Learning Thermostat  
Starting at: **\$225.00**  
★★★★☆

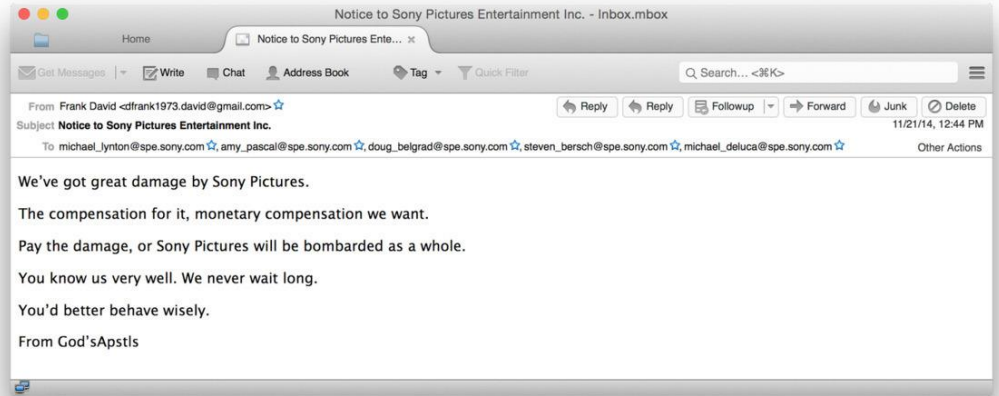


"There are more devices to secure against hackers, and bigger downsides from failure: hacking the location data on a car is merely an invasion of privacy, whereas hacking the control system of a car would be a threat to life." – World Economic Forum Global Risks 2015

# Doom & Gloom? IoT Extortion?



In 2013, McAfee, the security arm of Intel, collected more than 250,000 unique samples of ransomware.



We all watched in 2014 as "The Interview" debacle unfolded and \$100M in damage was done to Sony.

Cyber extortion of utilities dates back to at least 2008, according to Forbes and SANS, and 25% of utility executives reported in 2011 they had been victims of network-related extortion.



The fear and disruption that well publicized attacks can cause are too tempting a target to ignore.

# SO.... What is “*Privacy*”?

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!!!*

Practical 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.

*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.
- There are 100-1000s+ other attributes (from what you do, search) that can pinpoint you!

**One unified / executable solution is:**

A **cyber model enabling *Privacy by Design (PbD)***  
(e.g., specification based & relatively agnostic to the privacy requirements churn)



# ***WHY focus on Privacy? What's the problem to resolve?***

DATA is your greatest asset – is it well protected?

People are numb to the current “**FUD**” cyber approach  
(FUD = fear, uncertainty & doubt = security scare tactics)

Surveillance attacks our most primal notions of freedom

***Privacy LAWS*** are at the core of data breaches & fines

A **Cyber Enabled Privacy by Design** approach  
Can simplify and clarify the “*fog of privacy complexity*”

# It's The Law...

**Modern tort law** includes four categories of invasion of privacy:

- Intrusion of solitude: physical or electronic intrusion into one's private quarters
- Public disclosure of private facts: the dissemination of truthful private information which a reasonable person would find objectionable
- False light: the publication of facts which place a person in a false light, even though the facts themselves may not be defamatory
- Appropriation: the unauthorized use of a person's name or likeness to obtain some benefits

## **California Law** (representative sample)

- Article 1, § 1 of the California Constitution articulates privacy as an inalienable right.
- California Online Privacy Protection Act (includes Do Not Track protections)
- CA SB 1386 expands on privacy law and provides the first state data breach laws.
- California's "*Shine the Light*" law (SB 27, CA Civil Code § 1798.83), outlines specific rules regarding how and when a business must disclose use of a customer's personal information and imposes civil damages for violation of the law.

**Fourth Amendment** ensures that "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures"

Plus:

- Sarbanes-Oxley Act (**SOX**)
- The Payment Card Industry Data Security Standard (**PCI DSS**)
- The Health Information Portability and Accountability Act (**HIPAA**)
- The Federal Information Security Management Act of 2002 (**FISMA**)
- The Gramm-Leach-Bliley Act (**GLBA**)

## **Texas Law** (extreme notification)

- Due to a 2011 amendment to the Texas reporting law, if you "conduct business" in Texas, not only must you notify Texas any residents that their data has been breached, but you may also have to notify residents in states that have *no breach disclosure laws*, or face potential consequences from Texas.
- The *Texas reporting law theoretically includes all US residents!*

# Privacy Pays

## The Cost of Businesses Not Protecting Their Customer's Privacy

- **Sales Loses Due to Lack of Privacy**
  - Sales will migrate to companies that protect privacy
- **Lost International Opportunities**
  - International laws are in many cases more restrictive than US laws and can prohibit companies from offering certain services
- **Increased Legal Costs**
  - Breach notification, shareholder lawsuits, regulatory action, fines and sanctions
- **Investor Loses**
  - Brand Value impact, increased customer attrition, employee retention, shareholder lawsuits, regulatory action, fines and sanctions

## The Cost of Individuals Not Protecting Their Own Privacy

- **Higher Prices**
  - The cost of breaches and insurance will be a cost of doing business
- **More Junk Mail & Telemarketing**
  - Puts all users and all electronic commerce at greater risk for breaches
- **Increased Identity Theft**
  - It takes 6-8 additional months to collect a tax refund if a fraudulent return is filed under your social security number
- **The Dossier Society**
  - Surveillance inhibits free exchange

The S&P 500 is capitalized at \$12Trillion, 1/3 of that, or *\$4Trillion is directly attributed to the Enterprise Brand value*

# 7 Principles for Privacy by Design (PbD)

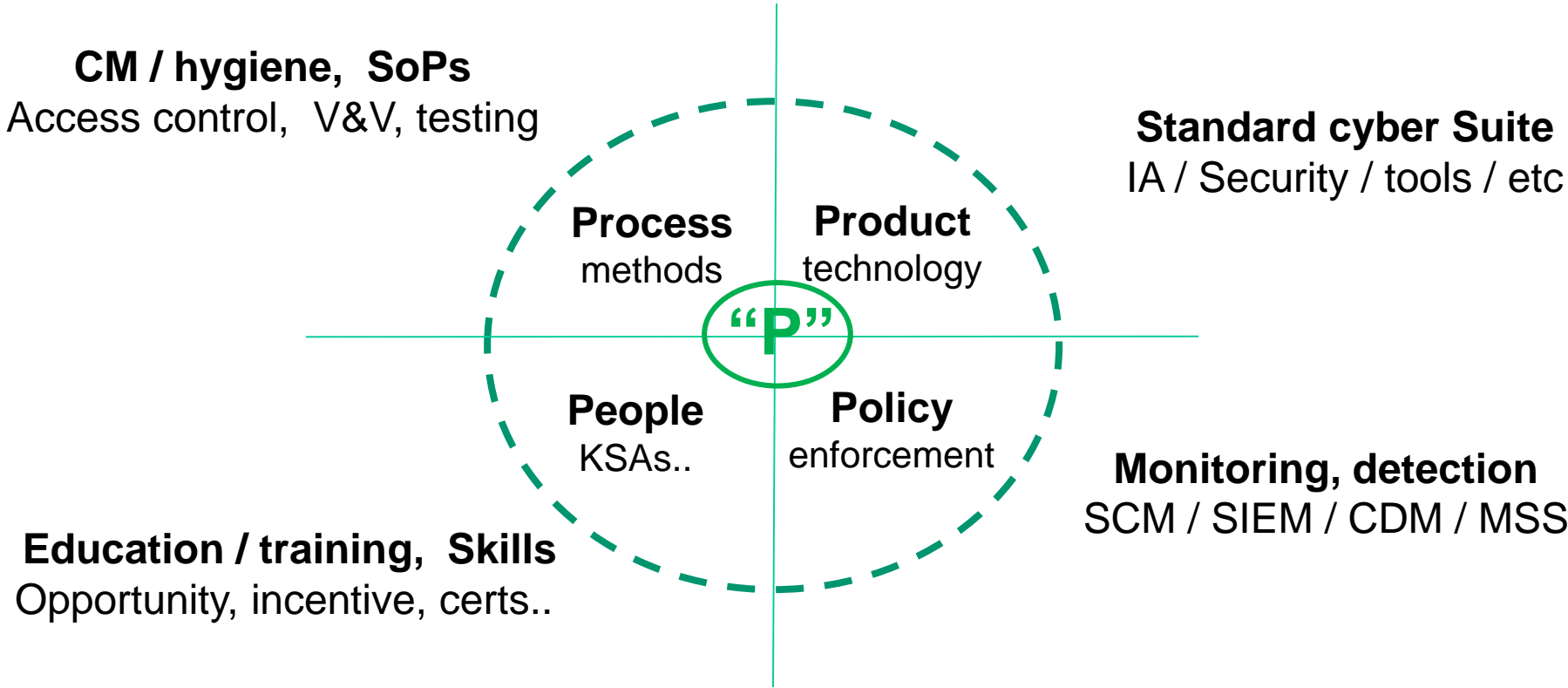
1. Proactive not Reactive; Preventative not Remedial
2. Privacy as the Default Setting
3. Privacy Embedded into Design
4. Full Functionality – Positive Sum, not Zero-Sum
5. End-to-End Security – Full Lifecycle Protection
6. Visibility and Transparency – Keep it Open
7. Respect for User Privacy – Keep it User-Centric

**Data Centric Security (DCS) maps directly to PbD**

# Privacy protection with the 4P's of Cyber

**Privacy protection is at the cyber intersection**

**ALL aspects must harmonize or data is not secure or controlled**

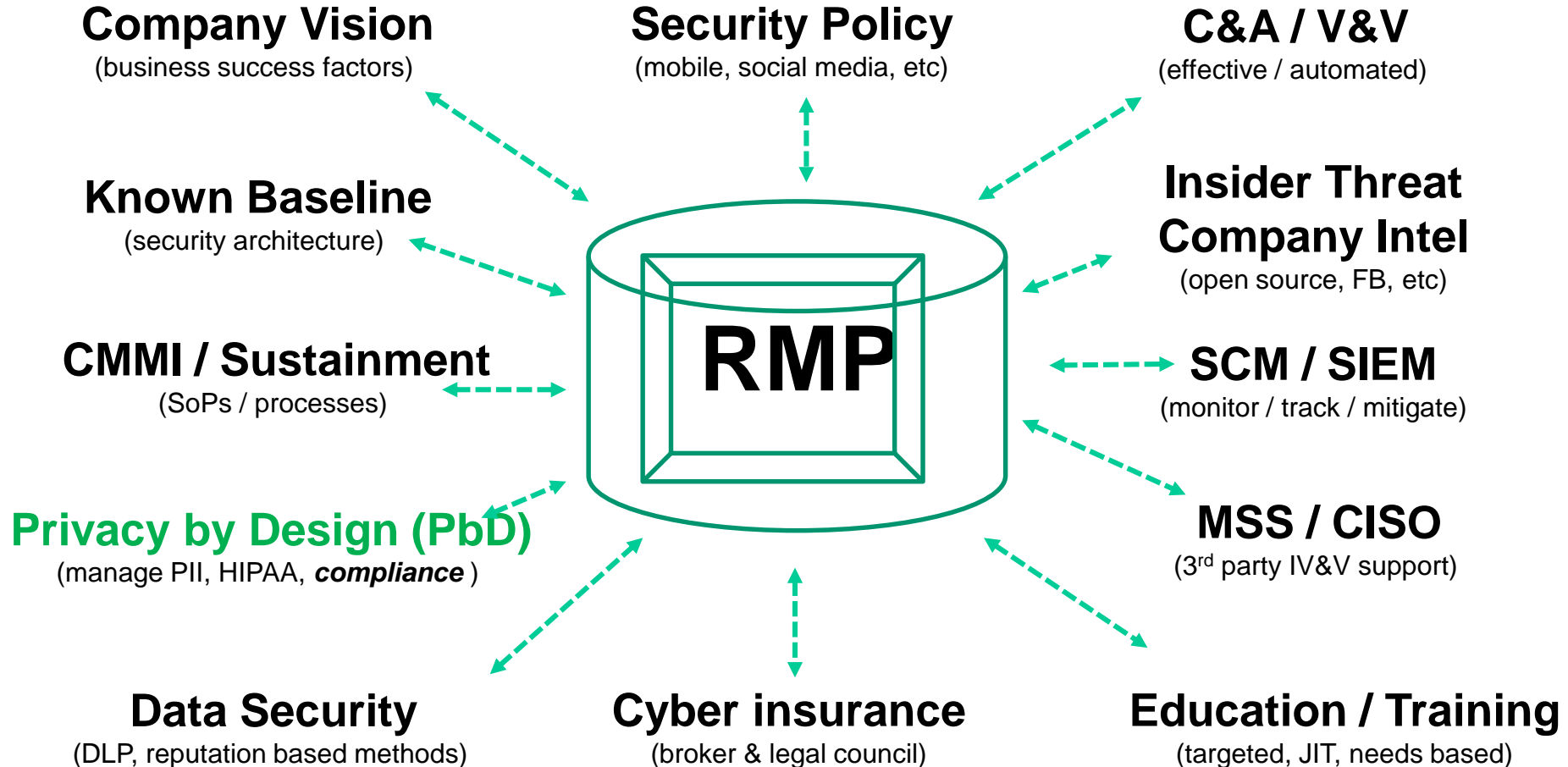


Our Cyber model enabling PbD integrates Product & Policy  
And interoperates with and works on top of the IA / CND / Cyber suite



# The Integrated **Business RISK** Approach

+ Making privacy protection a full organizational contact sport +



Must start with an enterprise risk management plan (RMP) / framework  
AND use the NIST Cybersecurity Framework

# Privacy Requirements are fuzzy... most are high level

(e.g., a “wicked” problem, hence specifications to build don’t exist)

## - Privacy by Design – *PbD* - seven principles

<http://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/>

## - Fair Information Principles (FIPs) Practices

<http://www.nist.gov/nstic/NSTIC-FIPPs.pdf>

## - OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

<http://www.oecd.org/sti/ieconomy/privacy.htm>

## - Data Protection Directive 95/46/EC

[http://en.wikipedia.org/wiki/Data\\_Protection\\_Directive](http://en.wikipedia.org/wiki/Data_Protection_Directive)

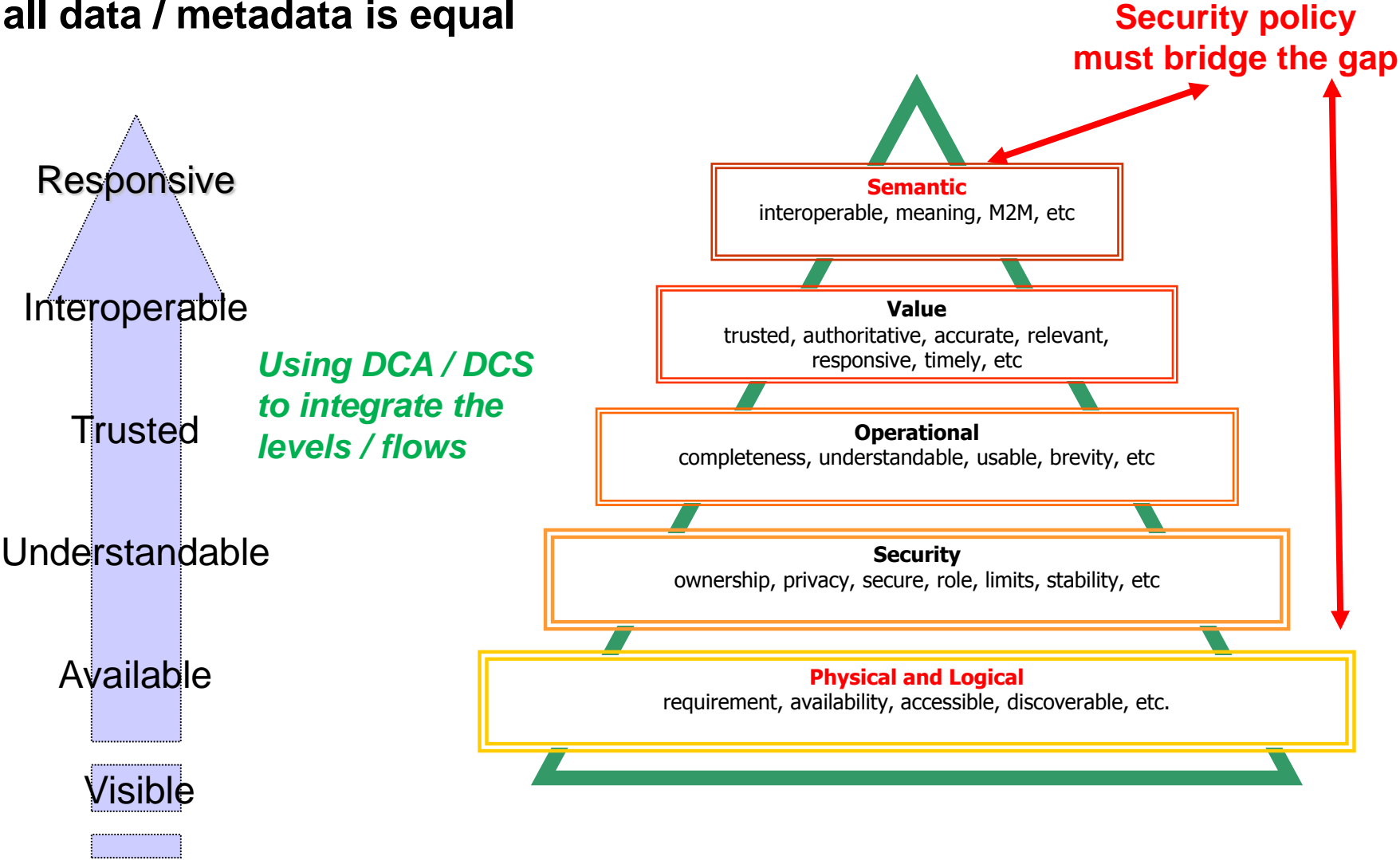
## - NIST 800-53Rev4 – Appendix “J” – 26 privacy controls

<http://dx.doi.org/10.6028/NIST.SP.800-53r4>

A Cyber model for PbD, provides useable, buildable specifications  
*That are relatively agnostic to the Requirements churn!*

# Hierarchy of Data Needs

Not all data / metadata is equal



Privacy must be accounted for at ALL levels  
AND eventually accommodate NPEs (non-person entities)

# Data Centric Architecture (DCA)

## Principles of Data-Centric Design

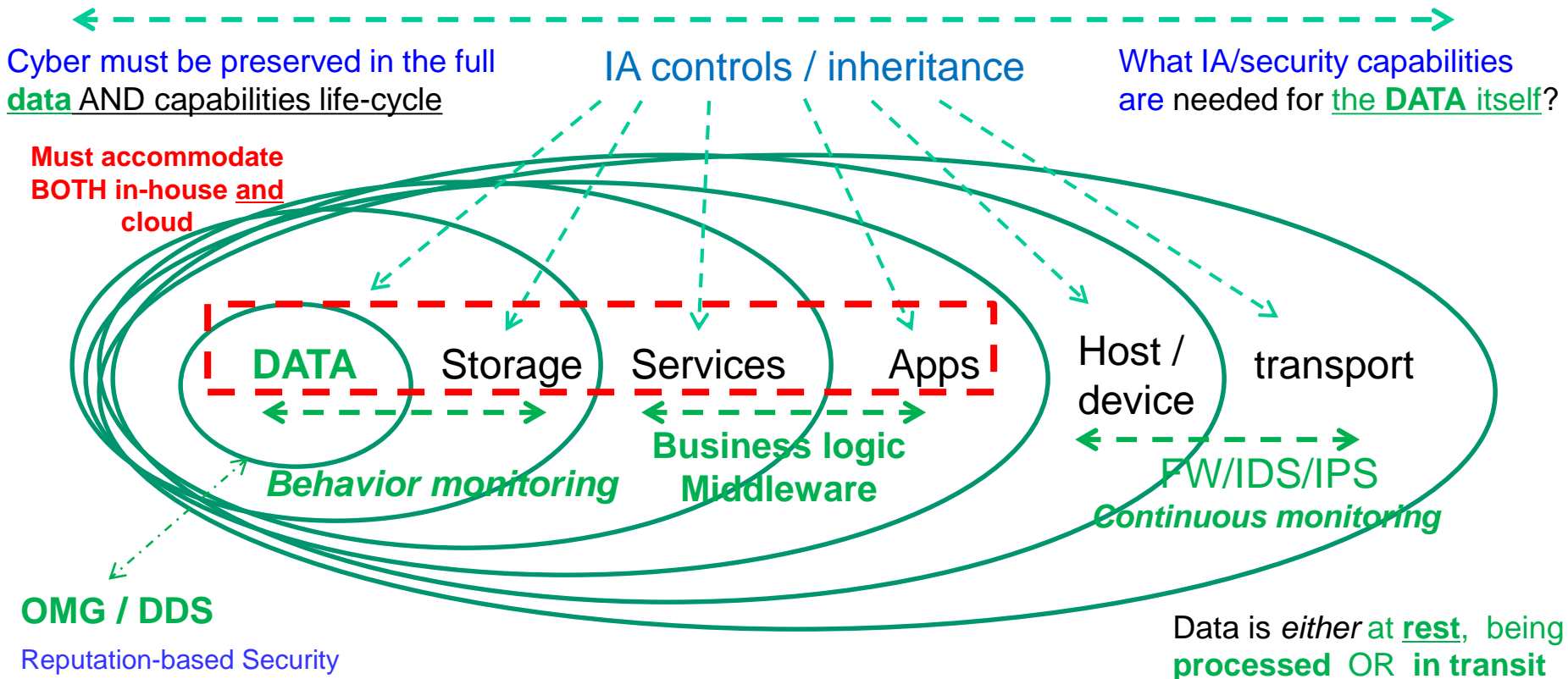
1. The main view is the **information exchange between systems** or components.
2. **DCA decouples designs and simplifies communication** linking “systems of systems” into a coherent whole, using an open standard – like Object Management Group (OMG) Data Distribution Service (DDS)
  - Expose the data and metadata
  - Hide the behavior
  - Delegate data-handling to a data bus
  - Explicitly define data-handling contracts
3. DCA Enables Data-Centric Services and Privacy
  - End2end / **lifecycle access control** and **encrypt everywhere**
  - Open Architecture, modular, APIs, loose coupling (e.g, “OOP”)
  - Common standards & specifications – focused on APLs (NIAP, etc)
  - “Infrastructure agnostic” – with DCS & “PaaS” = KISS

**DCA / DCS significantly simplifies the privacy problem**

# “Notional” DCA enterprise / end2end view

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

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



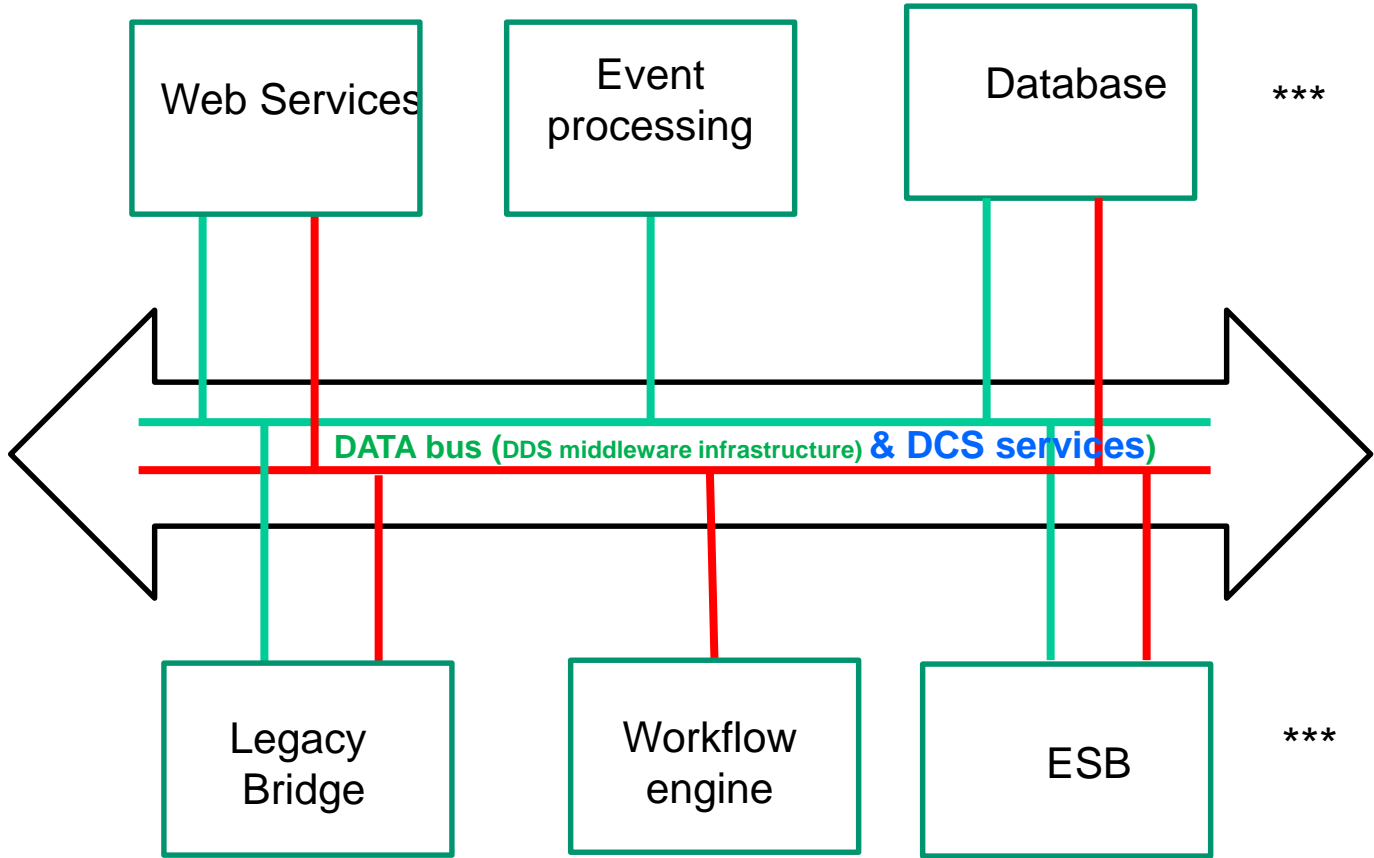
Must account for the “four ‘Vs’”

## Volume, Variety, Velocity and Veracity

A PbD Cyber Model accounts / translates the data 4V's into privacy attributes and controls



# Security Services Overall Construct

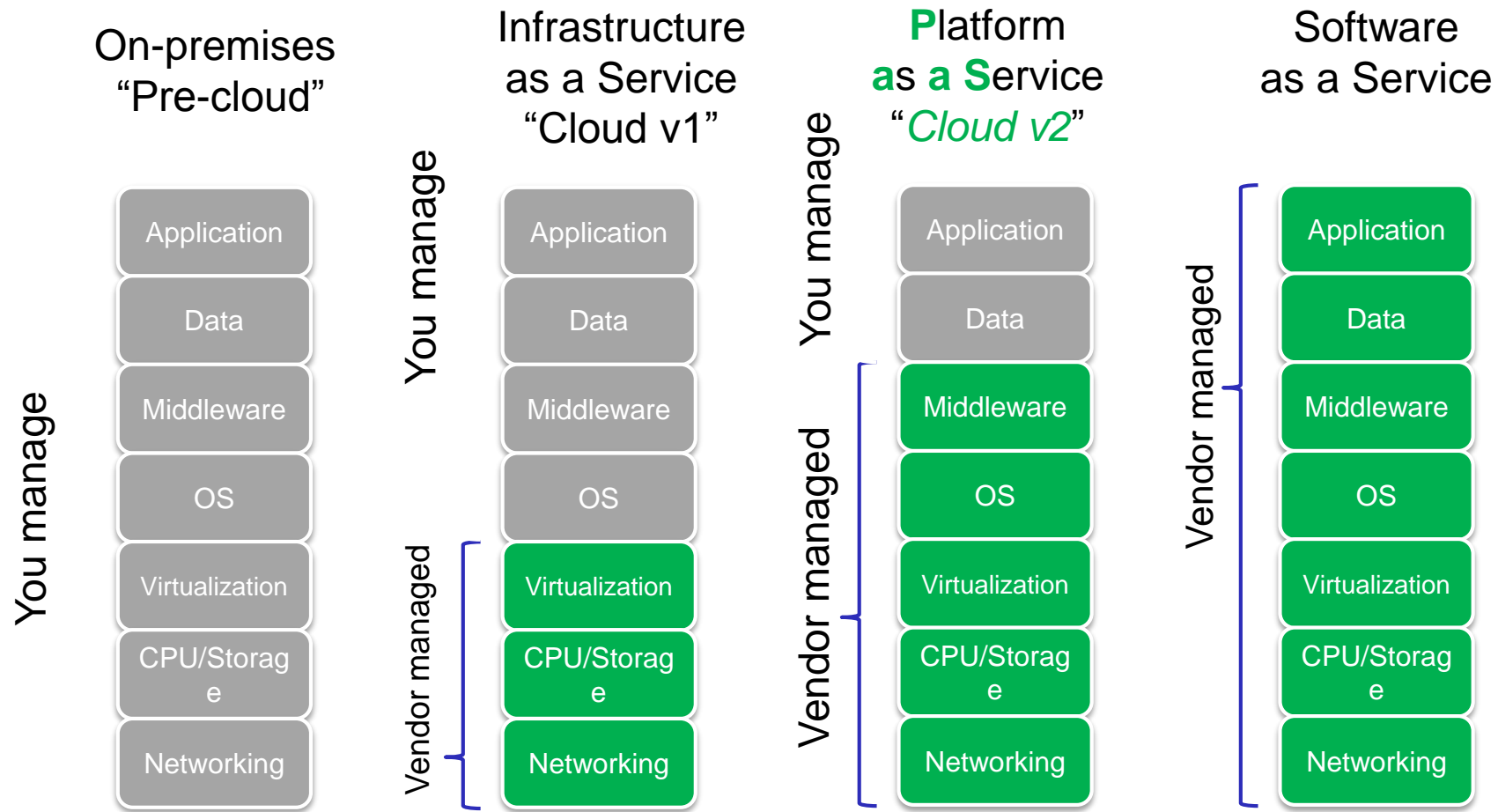


+ Standard IA / CND / security suite = "IA devices" = Firewall, AV, IDS/IPS, Crypto / Key Management, & VPN  
+ Network infrastructure = "CCE" = common core computing / network environment - with 'IA - enabled' devices

Our PbD cyber model *maps the data management, controls, & services into privacy aspects.*

# Data centric services, cloud ownership and security evolution

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



Securing the data and application layers *and inoculates them from lower layer risks*

# +++ Cyber Model for PbD +++

## *Privacy = data protection and security policy / controls*

- + 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, etc

-----

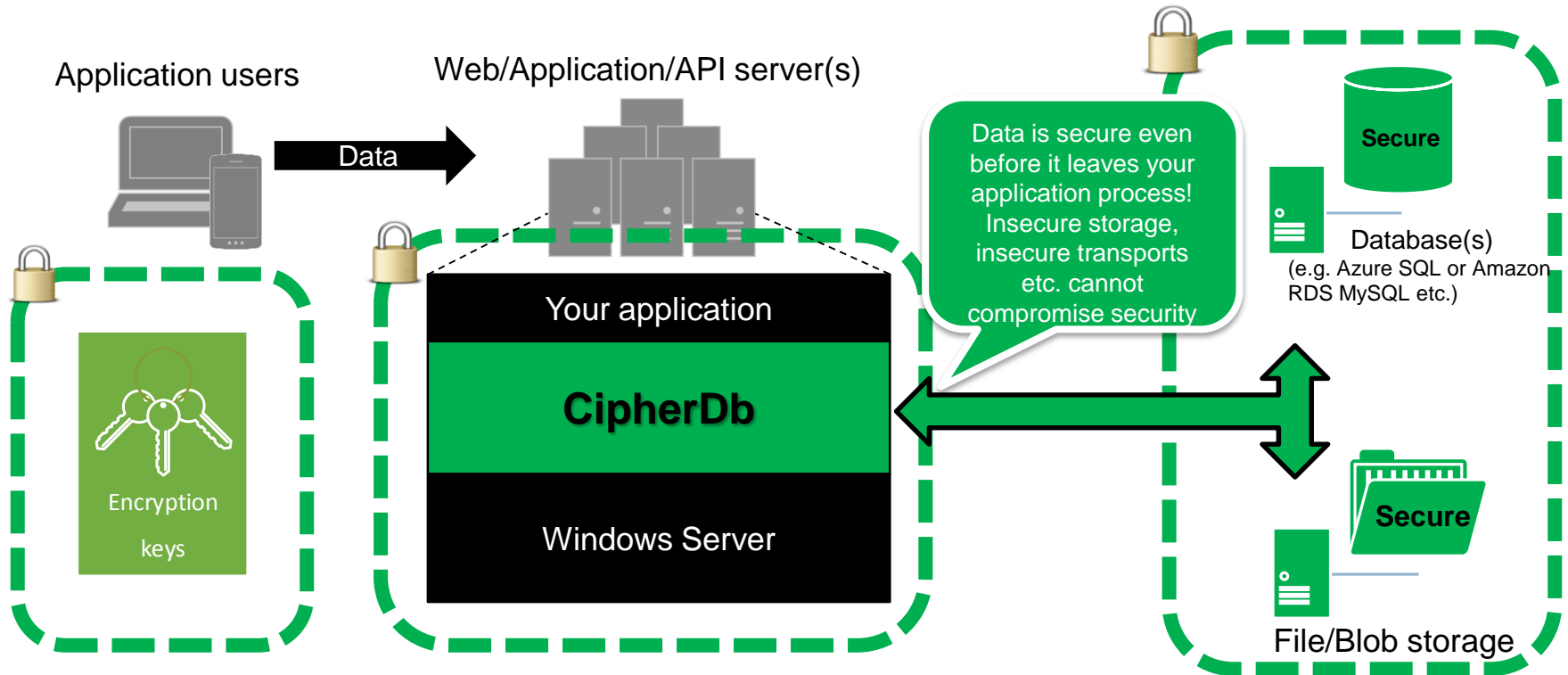
Standard **IA / CND suite** = “IA devices” = Firewall, A/V, IDS/IPS, Crypto / Key Mgmt, & VPN

-----

Typical **Network infrastructure** = common core computing environment

*Facilitate **Specifications** for an open privacy framework (OPF) for PbD*

# Cyber 4 PbD – Draft Specifications - DataSec



Multiple layers of encryption for sensitive applications

Keys never stored with database

Database hacks or even loss of SQL admin password means **no loss of data privacy or integrity**

Keys have multiple layers of encryption

**Complete** topological freedom over keys, compute and data for cloud, hybrid or on-premises

Creates an application layer, virtual private cloud between compute and data resources

# CipherDb – Secure data store to data store

Enterprise, end-to-end encryption, data-centric security and effective access control

User security: PbD requires that only authenticated and authorized users have access to the privileged parts of their PbD enabled applications.

Use 5 factor authentication = location, time, biometrics and other sensor data from user

## Database Security

- Turnkey solution for enterprise developers demanding strong data security in a connected environment
- Practical example: CipherDb enables compliance even in the public cloud!
- Data-centric security methods – *encrypt all sensitive data*
- Ultra fast encryption (<1ms) with column level granularity
- Focus on developer productivity and simplicity
  - Data encryption, decryption, access-audits, key-rollovers, tamper detection etc.
- Key management server that supports + 1 trillion keys (thus “IoT”)
- Data-at-rest as well as data-in-transit security
- Stack technologies ( .NET and Java enterprise stacks & works with any database )
- DoSCipher crypto-technology to protect APIs from DoS by forcing adversary to expend more CPU and memory (spend more on resources / LoE – *make attacks harder*)

<http://www.crypteron.com/products>  
(CipherDb, CipherStor, and TotalAuth)

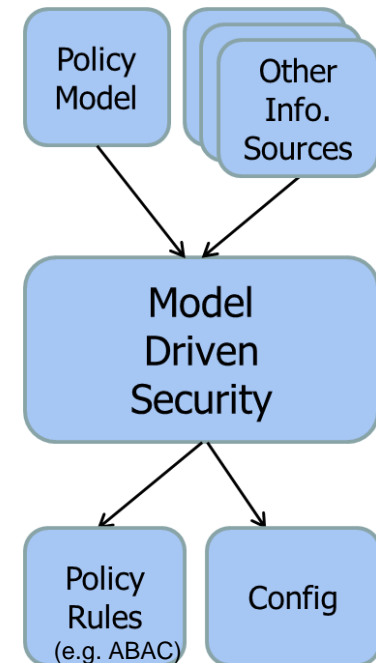


# Cyber 4 PbD – Draft Specifications - SecPolicy

- **Policy authoring:**

- intuitive, *user-centric* [privacy policy authoring](#) feature for admins (suitable mechanism “*model-driven security*”, **MDS**)
- *enable users to set their privacy policies* (“informational self-determination”, “intervenability”)
- automatic, configurable mapping to *matching* [security implementation machine code](#) (e.g. access rules, “privacy code libraries”) (suitable mechanism “*model-driven security*”)
- Must support complex, contextual, dynamic, fine-grained information flow policies; non-collection/-retention/-use; de-identification; redaction/filtering; strong default policies
- *advanced access control approaches* (e.g. PBAC, ZBAC, RAdAC, HBAC, ...)
- across information & software lifecycles (full-lifecycle information flow control “cradle to grave”)

MDS: Bridges the [semantics gap](#)



© ObjectSecurity LLC

- **Policy decisioning/enforcement:** Embedding privacy into systems & apps

- in an effective & manageable way (**PDPs/PEPs**)
- *preventive* (“*whitelisting*”) access decision-making
- enforcement at a fine granularity using PEPs, e.g. per data resource
- (suitable mechanism Attribute-Based Access Control (ABAC) & encryption)

- **Policy monitoring, auditing:**

- for the enterprise; but also:
- *user-centric tool that lets users verify (audit) that their policies are enforced correctly.*

<http://www.objectsecurity.com/en-products-openpmf.html>

# ObjectSecurity® OpenPMF™ - Overview



## OpenPMF™ Model-Driven Security Policy Automation

### Problem

#### Unmanageable Security Policies

Manually translating security policy & compliance requirements into effective technical implementation is difficult, expensive, and error-prone - esp. for interconnected, agile applications (e.g. SOA & cloud). Where does the policy come from? Who can write the matching technical policy rules? Who can maintain them despite dynamic changes? Who can verify policy correctness & compliance?

### Solution

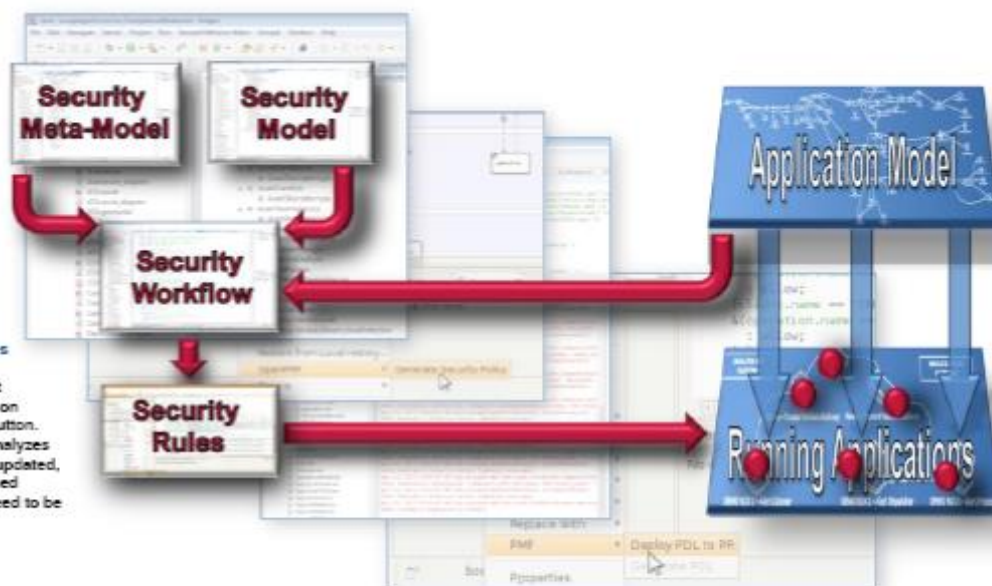
#### OpenPMF™ Model-Driven Security (MDS)

OpenPMF™ makes application security manageable through MDS automation. MDS automates the process of turning human-understandable security & compliance requirements (e.g. for attribute-based access control, ABAC, and monitoring) into the matching numerous and ever-changing technical security policy rules (whitelists) and configurations. MDS also distributes and proactively enforces those rules at the application layer, and also continuously monitors security. Unlike traditional manual authoring of rules, MDS automates technical policy generation and update from intuitive business security requirements models - including least privilege and workflow policies, which can protect against insider attacks. MDS helps automate policy management even for agile SOAs and cloud platforms. MDS forms a critical part of any authorization management, entitlement management and identity & access management (IAM) strategy. MDS also enables a secure application development lifecycle at development time right from the beginning - dealing with policy abstraction, externalization, authoring, automation, enforcement, audit monitoring/reporting, and verification.

*"Model-driven security is the tool supported process of modeling security requirements at a high level of abstraction, and using other information sources available about the system (produced by other stakeholders). These inputs, which are expressed in Domain Specific Languages (DSL), are then transformed into enforceable security rules with as little human intervention as possible. It also includes the run-time security management (e.g. entitlements / authorizations), i.e. run-time enforcement of the policy on the protected IT systems, dynamic policy updates and the monitoring of policy violations."*  
- Wikipedia

### 1 Configure

intuitive business security requirements policies  
Security professionals can configure or select generic application security requirements in a model-driven security tool, including access and monitoring policies. No need to be an application specialist.



### 2 Generate

matching technical security policies automatically  
Application developers can implement application specific technical application security policy rules at the click of a button. Model-driven security automatically analyzes your software as it is being written or updated, and generates the matching fine-grained access and monitoring policies. No need to be a security specialist.

### 3 Enforce

technical security policies automatically  
At runtime, local authorization management policy decision points and policy enforcement points (PDPs/PEPs) underneath all applications automatically intercept and check all information flows before they are forwarded to the application.

### 4 Monitor

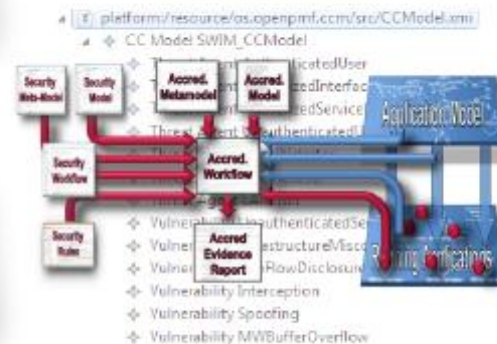
technical security policies automatically  
At runtime, policy monitoring points automatically collect information about security incidents for monitoring and auditing purposes. The collected information can be configured through generic monitoring policy models.

### 5 Update

technical security policies automatically  
Model-driven security uniquely updates technical security policies automatically when systems are reconfigured (e.g. SOA). No need to manually update technical security policies. This unique feature makes policy management and implementation manageable for today's rapidly evolving interconnected applications (e.g. agile SOA w. BPM and clouds).

### 6 Verify

compliance/accreditation automatically  
This MDS feature automatically produces supporting evidence that the enforced security rules match with accreditation/compliance policy models and security policy models. It helps shorten accreditation/re-accreditation time and reduce cost (esp. for agile IT landscapes such as SOAs)



References [objectsecurity.com/publist](http://objectsecurity.com/publist)

**Object Security**  
info@objectsecurity.com  
www.objectsecurity.com  
ObjectSecurity LLC Plug & Play Tech Center 530 University Ave #202  
Palo Alto CA 94301 USA Tel: 650-515-3391  
ObjectSecurity Ltd. St John's Innovation Centre Cowley Road  
Cambridge CB4 0WG England Tel: +44 (0) 1223 420 252

# Cyber 4 PbD – Draft Specifications - SecSIEM

- **Enterprise IT mapping:**
  - maintain a global map of network information flows, systems, applications, routing data and interactions on the network
  - used for visibility into incidents, and for SecPolicy MDS automation
- **Incident detection**
  - detect anomalies and policy violations to create an accurate situational picture of the cyber security posture
  - use signature/behavior/policy-based intrusion detection mechanisms
  - also use SecPolicy's ABAC enforcement incidents.
  - provide users access to their incident information (for “transparency”)
- **Compliance evidence & verification**
  - automatically provide real-time information about the level of compliance,
  - automatically generate compliance evidence reports.
  - provide users access to their compliance information (for “transparency”)
- **Forensics support**
  - Keep evidence and provide as needed

Monitors key architecture aspects critical for performance and assurance, feeds MDS.

[http://www.promia.com/products\\_and\\_tools/raven/RavenOverview.html](http://www.promia.com/products_and_tools/raven/RavenOverview.html)




# Military Grade Cyber Integration

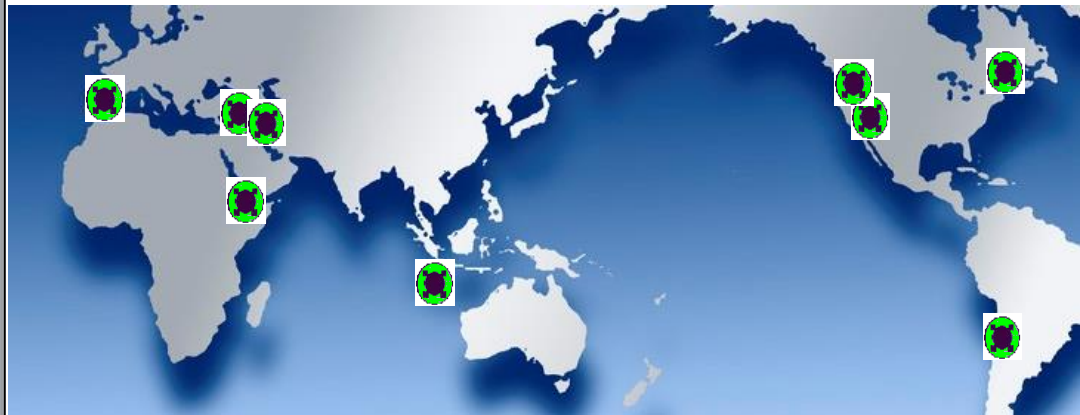
- Promia Raven support open standard interfaces including Web 2.0 RESTful APIs, and incorporates data from Arcsight, BIT9, McAfee ePO (HBSS) and other generic agents. Raven feeds DoD Clouds for OWF.
- Raven feeds other systems through secure XML, JSON, CVS APIs
- Common Criteria, DIACAP, FISMA, NERC CIP compliance
- **DoD TRL Level 9** – integrated with OpenPMF = “TrustWand”

Customers:

Defense, intelligence, finance, energy, smart city, healthcare

*Global Presence*

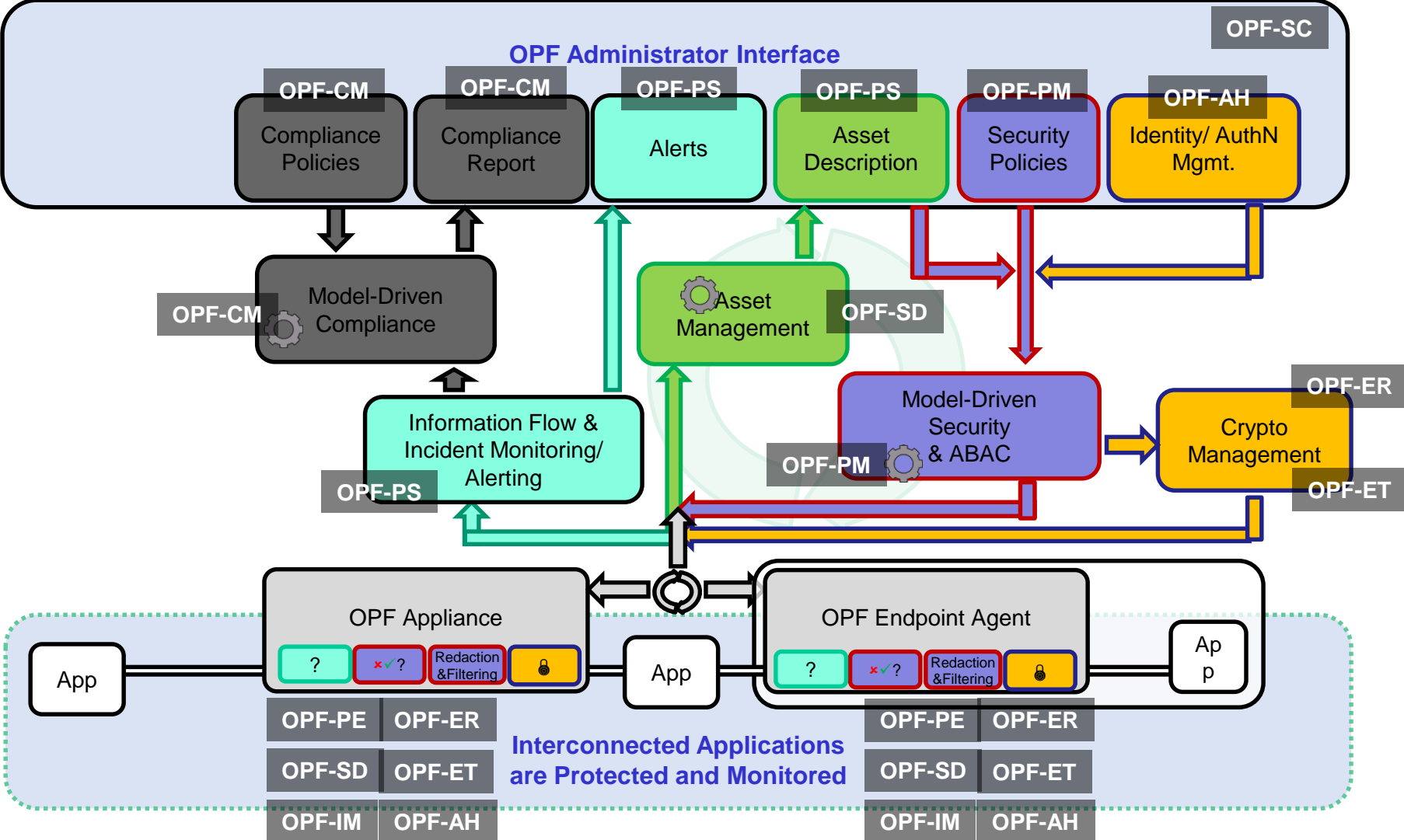
Promia Raven Family of Appliances	
<b>Required – Promia Raven 2100</b>  <small>Promia Raven</small>	Core hardened appliance <ul style="list-style-type: none"><li>• Local or as part of an enterprise grid</li><li>• Copper, Fiber, 1G; 10G</li></ul>
<b>Optional – Analytic Tool Unit</b> 	Extended Analysis & Trending <ul style="list-style-type: none"><li>• Remote forensics and security data analysis</li><li>• 24 thread dual XEON</li></ul>
<b>Optional – Analytic Storage Unit</b> 	Big Data Storage – All Traffic <ul style="list-style-type: none"><li>• Stores TBs of security data</li><li>• Unit Can Support 72 TB</li></ul>





# Open Privacy Framework (OPF) Foundation

(reference architecture implementation **technical approach AND specifications**)



## 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!

# What is the privacy market opportunity? “RoI”

## Value Proposition

Enhancing privacy protection can *payback in savings in under a year*  
The intangibles (brand, 3<sup>rd</sup> party liability, etc) will be many multiples of that

## Market Penetration

*Privacy laws, fines, etc applies to ALL organizations* – SMB typically not prepared  
Company's with sensitive data (PII, HIPPA) will spend more for higher confidence

## Risk versus Reward

Must be able to *prove* “at least” *DUE DILIGENCE in a legally defensible strategy*  
Measures that effectively ADD protection, confidence level to cyber suite do sell

## Emotional / buy-in aspect

Privacy is by its' nature is personal and emotional – add in personal liability  
*The IP, sensitive data loss downside can be larger than the company equity*

***Huge untapped market, timing is NOW, and it's the right thing to DO***

# “Cyber 4 PbD” – Privacy PAYS – OK, I’m lost..;-((

A focus on Privacy - *differentiates your business*, greatly reduces liabilities

A focus on Privacy - is a *wider appealing message*, easier sell than “FUD”

A focus on Privacy - building it in using PbD, *provides greater assurances*

A focus on Privacy - makes data security, compliance, etc. *a risk package*

Using “Cyber 4 PbD” (C4P) focuses on *your core business asset – DATA.*

C4P makes privacy protection *ubiquitous, agnostic to user, location*

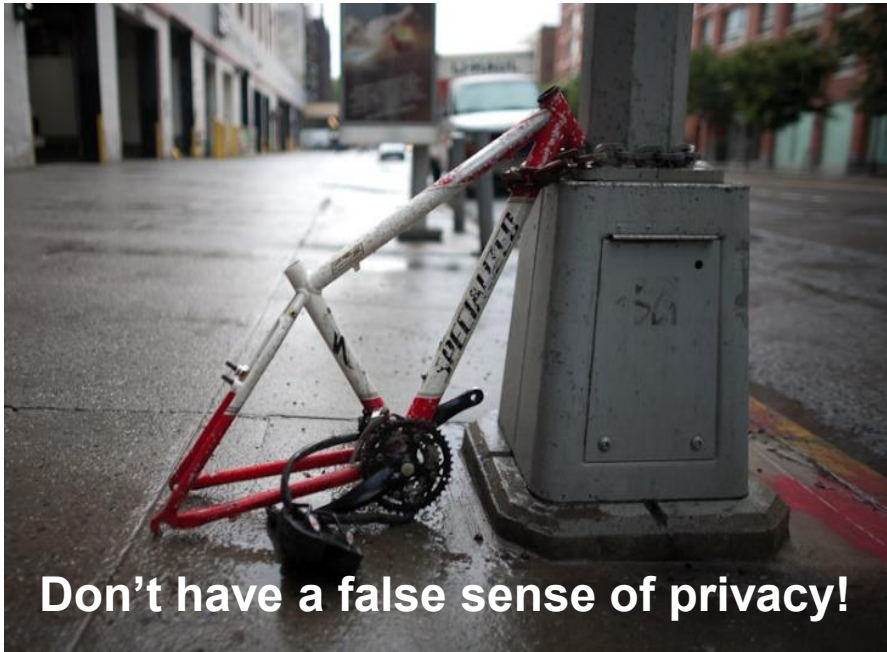
Using a specification based “OPF” *minimizes requirements churn impact*

**Build in Cyber 4 PbD into your risk management approach – privacy first.**  
**AND a lifecycle risk view = baselines, SCM / SIEM, MSS (SME), & Cyber Insurance**

# SUMMARY: SO.... What “really” matters in Cyber / privacy?

It's all about **TRUST** and **DATA (protection)**

( Identity, authentication, secure comms - -- provenance, quality, pedigree, assured (the 4 Vs))



Don't have a false sense of privacy!

## (1) Doing the cyber BASICS well:

- (a) enforced *cyber hygiene*,
- (b) effective *access control*,
- (c) *reduced complexity* in IA / cyber  
(use APLs / NIAP / approved products),
- (d) Cyber “SCM / CDM / SIEM”

## (2) Collaborating on Cyber 4 PbD:

- (a) Common *privacy specifications*,
- (b) *Privacy assessment tool*,
- (c) *Privacy monitoring capability*
- (d) **SD PbD / Data Security meetup**

It's the “services” that tie it all together!

**DO the cyber BASICS well**, for products, people and processes

Follow your RMP - Protect privacy, MSS/SME oversight, & cyber insurance...