Privacy Pays

1 - Offering both Business Opportunities and liability / risk reductions
2 – Sells cyber better than ‘just’ improved security benefits alone

Mike Davis
Mike.Davis.SD@gmail.com
Risk Management / Cyber Security Consultant & Enthusiast (...virtual CISO...)
ElectEngr / MSEE, CISSP & CISO, PM, SysEngr (Retired USN)

Privacy is a GLOBAL concern and business opportunity too!

Detailed “Cyber Facilitated Privacy by Design” paper at:
WHY do we need to care about Privacy?

Over one BILLION records stolen in 2014 (just the ones we know about)

the damage cost of the average record is around $200...

“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 D & O’s / line managers

D & O’s can be held personally liable for lack of due diligence

The following slides show WHY we need to care (pay for it) and
HOW we can take an affordable, enterprise privacy approach
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.

"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
What’s Wrong With This Security?
The issues / gaps therein are also prevalent in privacy protection!

When a capability is “invisible”, like IA, safety, reliability – and privacy - what you see is not the whole picture!

The gates were fully locked, properly configured and validated (C&A’d).
I could not get through them. But.... Thus Privacy can be an illusion…
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.
Focus on Privacy? WHY? SO what?

1 – **REDUCE expenses** and greatly decrease risks
   
   A – Reduce insurance costs by SEVERAL factors and levels  
   B – Minimize liability, especially 3\textsuperscript{rd} 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

**Improved privacy protection** PAYS in many ways!
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)**
(Specification based & relatively agnostic to the privacy requirements churn)
**WHY 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)

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

Surveillance attacks our most primal notions of freedom

A **Cyber Enabled Privacy by Design** approach
Can simplify and *clarify the “fog of cyber complexity”*
Yes, It really is ALL about the DATA*

Future Data Sources

Convergence

Embedded Computing

Location Based Services

Interactive 3D

Telematics

Internet of Things

Mobilization

“CBAD” = Cloud, Big Data, Analytics, Data Science

It’s a data-centric world; so use a data centric architecture (DCA)

By providing enterprise DCS for PbD

* and TRUST!
Some “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
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

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..... (= rate of cloud app use, mobile use, more data sharing)

Due diligence security environment required
and
Implement a privacy protection approach

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

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

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

Forbes list: Social Engineering; APTs; Internal Threats; BYOD; HTML5; Botnets; Targeted Malware & cloud

We have met the cyber enemy, and they are US(ers)
It’s the LAW!
(and you may not even know many of them)

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

- **Fourth Amendment** ensures that "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, ... needing probable cause (maybe)
- THEN there ALSO: 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), and the Gramm-Leach-Bliley Act (GLBA).

Office of Management and Budget (OMB) Circular A-130 (“PII”) and OMB memos: 07-16 and 10-22...

- **Federal Trade Commission** (FTC) regulates and oversees business privacy laws and policies that impact consumers. **Financial data, enforcing data security** and ID theft...

- **List of USA Privacy Laws**, Regulations, and more *(Privacy Act, etc)* (even your garbage)
  [http://www.informationshield.com/usprivacylaws.html](http://www.informationshield.com/usprivacylaws.html)
- **Privacy Journal** - Compilation of State and Federal Privacy Laws (750+) ($26 for PDF)
  [http://www.privacyjournal.net/_center_compilation_of_state_and_federal_privacy_laws__center__3077.htm](http://www.privacyjournal.net/_center_compilation_of_state_and_federal_privacy_laws__center__3077.htm)
THEN, It’s “CA”LAW!
California Online Privacy Protection Act also known as CalOPPA

Article 1, §1 of the California Constitution articulates privacy as an inalienable right.

In 2003, California established the landmark California Online Privacy Protection Act. In 2013, the Act was amended by Assembly Bill 370, which requires information on how the operator responds to Do Not Track signals or similar mechanisms.

CA SB 1386 expands on privacy law and provides the first state data breach laws. SB 24 amended the law, January 1, 2012, to require organizations issuing a security breach notification to more than 500 California residents. CA AG recent report on how the law was doing... recommendation no 1 – encrypt, encrypt, encrypt

California's "Shine the Light" law (SB 27, CA Civil Code § 1798.83), operative on January 1, 2005, 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.

Overall review of CA privacy law
http://moritzlaw.osu.edu/students/groups/is/files/2012/02/betzel.pdf

CA DoJ AG – Privacy laws for CA (& Federal) http://oag.ca.gov/privacy/privacy-laws
THEN it’s Texas Law too: Reaching Beyond the Boot

• Thanks to a 2011 amendment to the Texas reporting law, if you “conduct business” in Texas, not only must you notify Texas residents (if any) 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.

• That is, the Texas reporting law theoretically includes all US residents!

• This is but ONE example, where keeping track of all the cyber / digital / privacy laws is almost impossible...inside the USA, let alone international

Thus once again showing the criticality of effective cyber preparedness / proven due diligence level.... AND the need for proactive privacy protection! especially in 3rd party law suits – which can come from anywhere at anytime! And will get worse globally... hence ‘unconstrained’ 3rd party liability!
Privacy Pays

Business Opportunities (as well as risk reduction!)

Differentiate your organization – be a good business partner.

The added value of privacy is intrinsic – (like being “green”)

BRAND, competitive advantage and new products / services

RE: Brand value = 1/3 the value of $12Trillion capitalization of S&P 500

Provide a user-centric experience – enable consumers

Must make it simple and easy – embedded in services, automated

Data breeches are expensive -  D & O’s can be personally liable!

Privacy

Much more than just compliance or reduced liability & costs

Increased sales through an enhanced customer experience
The **Costs Businesses Incur** by *NOT* Protecting Privacy

Sales Losses Due to Lack of Privacy

One Retailer’s Loss Is Another Retailer’s Opportunity

Lost International Opportunities

Increased Legal Costs

Investor Losses

**Privacy**

Much more than just compliance or reduced costs

*Increased sales through an enhanced customer experience*

https://epic.org/reports/dmfprivacy.html
The Costs *Individuals* Incur by NOT Protecting Privacy

Higher Prices

MORE Junk Mail

MORE Telemarketing

Increased Identity Theft

MORE SPAM, software snooping, tacking, etc..

The Dossier Society – surveillance inhibits free exchange

**Privacy**

*Much more than just compliance or reduced costs*

*Increased sales through an enhanced customer experience*

[https://epic.org/reports/dmfprivacy.html](https://epic.org/reports/dmfprivacy.html)
What is the privacy market opportunity? “RoI”

Value Proposition
Enhancing privacy protection can payback in savings in under a year
The intangibles (brand, 3rd 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 that the company equity
Privacy Requirements are fuzzy... High level (e.g., a “wicked” problem, hence specifications to build don’t exist)

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

- **Fair Information Principles (FIPs) Practices**

- **OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**
  [http://www.oecd.org/sti/ieconomy/privacy.htm](http://www.oecd.org/sti/ieconomy/privacy.htm)

- **Data Protection Directive 95/46/EC**

- **NIST 800-53Rev4 – Appendix “J” – 26 privacy controls**
  [http://dx.doi.org/10.6028/NIST.SP.800-53r4](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!*
PbD 7 Principles (it has an international following)

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
The **4 P’s** of any effort – Privacy too

**People:**
Education is the fundamental core need. Must tie to other three P’s.

**Policy:**
Clear, championed from the top, monitored and enforcement built in.

**Process:**
Consistent execution & operations requires documented methods, SoPs.

**Product (technology):**
To build in data security / privacy, must have an integrated ecosphere.

One solution – a **cyber model for privacy by design (PbD)**
Proposed **specifications** account **Product & Policy**.
Privacy protection is at the cyber intersection
ALL aspects must harmonize or data is not secure or controlled

CM / hygiene, SoPs
Access control, V&V, testing

People
KSAs...

Process
methods

Product
technology

Policy
enforcement

“P”

Education / training, Skills
Opportunity, incentive, certs..

Standard cyber Suite
IA / Security / tools / etc

Monitoring, detection
SCM / SIEM / CDM / MSS

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 +

- 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 (PbD) (manage PII, HIPAA, compliance)
- Data Security (DLP, reputation based methods)
- Cyber insurance (broker & legal council)
- Education / Training (targeted, JIT, needs based)

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

Cyber for PbD uses DCA / DCS to simplify the privacy environment
Principles of Data-Centric Design

The essential invariant is the *information exchange between systems or components*.

*DCA decouples designs and simplifies communication* while increasing capability and easing system evolution linking “systems of systems” into a coherent whole, using an open standard — like OMG DDS.

- Expose the data and metadata.
- Hide the behavior.
- Delegate data-handling to a data bus.
- Explicitly define data-handling contracts.

*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)

Cyber must be preserved in the full data AND capabilities life-cycle
Must accommodate BOTH in-house and cloud

IA controls / inheritance

What IA/security capabilities are needed for the DATA itself?

DATA
Storage
Services
Apps

Host / device
transport

Behavior monitoring
Business logic
Middleware

FW/IDS/IPS
Continuous monitoring

OMG / DDS
Reputation-based Security

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
A PbD cyber model must *map the data management, controls, & services into privacy aspects.*
Data centric services and cloud evolution

**ownership and security**

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

<table>
<thead>
<tr>
<th>On-premises “Pre-cloud”</th>
<th>Infrastructure as a Service “Cloud v1”</th>
<th>Platform as a Service “Cloud v2”</th>
<th>Software as a Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Application</td>
<td>Application</td>
<td>Application</td>
</tr>
<tr>
<td>Data</td>
<td>Data</td>
<td>Data</td>
<td>Data</td>
</tr>
<tr>
<td>Middleware</td>
<td>Middleware</td>
<td>Middleware</td>
<td>Middleware</td>
</tr>
<tr>
<td>OS</td>
<td>OS</td>
<td>OS</td>
<td>OS</td>
</tr>
<tr>
<td>Virtualization</td>
<td>Virtualization</td>
<td>Virtualization</td>
<td>Virtualization</td>
</tr>
<tr>
<td>CPU/Storage</td>
<td>CPU/Storage</td>
<td>CPU/Storage</td>
<td>CPU/Storage</td>
</tr>
<tr>
<td>Networking</td>
<td>Networking</td>
<td>Networking</td>
<td>Networking</td>
</tr>
</tbody>
</table>

Vendor managed

Vendor managed

Vendor managed

Vendor managed

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

Develop Specifications for an open privacy framework (OPF) for PbD
Cyber 4 PbD – Draft Specifications - DataSec

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)
CipherDb — Secure data store to data store

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
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”)

- **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.

ObjectSecurity® OpenPMF™ - Overview

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 (whitepapers) 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.

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, 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/publish
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
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”

Promia Raven Family of Appliances

- Required – Promia Raven 2100
  - Core hardened appliance
  - Local or as part of an enterprise grid
  - Copper, Fiber, 1G; 10G

- Optional – Analytic Tool Unit
  - Extended Analysis & Trending
  - Remote forensics and security data analysis
  - 24 thread dual XEON

- Optional – Analytic Storage Unit
  - Big Data Storage – All Traffic
  - Stores TBs of security data
  - Unit Can Support 72 TB

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

Global Presence
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!
“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 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))

(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**

A false sense of privacy is worse then none!

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 oversight, & cyber insurance...