



pennsylvania
INSURANCE DEPARTMENT



pennsylvania
DEPARTMENT OF PUBLIC WELFARE



Cyber Security – Risks and Options for Improvement

Cyber security challenges and opportunities
Jim Weaver, CTO
August 15, 2011



- Lack of understanding and clarity in communication about the level of risk and business impacts to the business stakeholders.
- Addressing fraud, waste and abuse requires enhanced cyber security measures and information sharing of incidents among agencies.
- Budget lags behind similar private-sector enterprises – absence of information security budget or grants at HHS agency level.
- Shortage of highly skilled cyber security state workforce.
- Most of us have security standards, but the challenge is in execution.
- Increased use of business partners, third party providers and cloud computing; limited agency control and influence on how they protect agency data
- Increasing cyber threats and organized cybercrime.

DPW adapts to evolving Security and Privacy challenges



pennsylvania
DEPARTMENT OF PUBLIC WELFARE

Business Driver:

- Waste, Fraud, & Abuse
- Health care reform
- HITECH Act

Business Driver:

Web enablement
& self service

Business Driver:

Worker oriented
services

- Access Management

Technology Enabler:

- Mainframe security

- Web Access Management
- Delegated User Administration
- Citizen Self-service
- Business Partner Self registration

Technology Enabler:

- CA Site Minder
- CA Identity Manager

- SOA Security
- Virtual Servers
- Risk Framework
- Vulnerability Management
- Privacy and Data Protection
- Security Incident and Event Management (SIEM)

Technology Enabler:

- SOA Security Manager
- RSA enVision (SIEM)
- HP Web Inspect
- Imperva Firewall

- IT Risk and Compliance Management
- Third Party Security Management
- Information Asset Management
- Automated User Provision
- Data Loss Prevention (DLP)
- Enterprise self-registration service

Technology Enabler:

- Risk Management COTS
- Data Leakage Prevention COTS
- IBM Tivoli Identity Manager
- Electronic signatures

1990s

2000-2010

2010 and beyond

Program Support Requirements

Our first opportunity from system modernization and web enablement



pennsylvania

DEPARTMENT OF PUBLIC WELFARE

Enterprise Identity and Access Management



Challenge

- Multiple open applications stemming from ONE mainframe – leads to handling of multiple user credentials
- Administrators challenge in managing access of many credentials to many systems
- Inconsistent security developed independently for each system
- Citizen and business partner online service.

Opportunity

- “Keystone key” – seamless access to multi-agency applications
- Role based access control
- Centralized and Delegated user administration
- User self-service
- Automated user provisioning from the HR system
- SOA security

Benefits

- Reduced sign-on
- Consistent security implementation for custom applications
- Increased business partner and citizen usage
- Centralized user management
- Reduced overhead from delegated administration
- Shared user repository with other agencies
- User provisioning during onboarding

Evolving risks from web enablement of HHS systems – An opportunity to manage



pennsylvania
DEPARTMENT OF PUBLIC WELFARE

Business stakeholders understand security vulnerabilities



Challenge

- Increased threat on application layer
- Emerging risks from web enablement of HHS systems
- Rise in Web-based vulnerabilities
- Usage of SSL and perimeter defense is insufficient.

Opportunity

- Secure Development Life cycle with manual vulnerability testing
- Web Application Firewall
- Fine grained access controls
- Centralized audit log management and monitoring using Security Information & Events Monitoring (SIEM).

Benefits

- Protect the Application layer
- Gain citizen trust in DPW's online applicant services
- Develop secure citizen centric web solutions from early detection and mitigation of vulnerabilities
- Identify potential violations through log correlation using SIEM solution.

The need to mature security risk management



pennsylvania

DEPARTMENT OF PUBLIC WELFARE

Enterprise Risk Management



Challenge

- Need to better communicate and manage risk with the program managers
- Reactive risk management through external Federal/State audits
- De-centralized audit and risk management

Opportunity

- Security Risk Framework: Correlated more than 4000 requirements from more than 140 Federal and State regulations to less than 360 integrated requirements
- Operationalized and automated Security Risk Framework
- Risk Impact Scale helps determine impacts of security incidents.

Benefits

- Proactive identification and management of security risks
- Better prepared for external audits through periodic internal assessments
- Assess once, address multiple legal and regulatory requirements
- Effective prioritization of remediation initiatives, audit findings or security needs.

Shared Services – Shared security resources



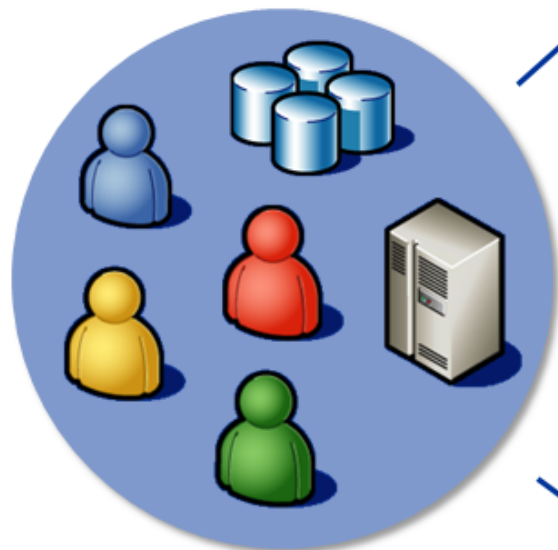
pennsylvania
DEPARTMENT OF PUBLIC WELFARE

Common Support

- Database Administrators
- Middleware
- Configuration Management Specialists
- Security Specialists
- Operations



THE COMPUTERWORLD
HONORS PROGRAM



Common Platform

- Configuration
- Database
- Middleware
- Security
- Knowledge Management



- **Reduce fraud, waste and abuse** - Implementing strong authentication controls such as Smart card and biometric solutions to deter fraud and increase accountability
- **Enterprise Data Loss Prevention** to establish continuous monitoring of flow of citizen personal identifiable information (PII) and prevent loss of citizen data
- **Embrace cloud computing** through proactive identification and mitigation of security/privacy risks