STATE OF INDIANA

Nominations for NASCIO's 2007 Recognition Awards for Outstanding Achievement in the Field of Information Technology, Business Continuity, & Disaster Recovery

Personal Information Identified & Protected. Period.

Information Security and Privacy

Between 2005 and today, the State of Indiana has completely revamped it approach to protecting personal information. Today, users are regularly trained on their responsibility to protect personal information retained by the State and system owners have been identified and trained to eliminate personal information that is not required to be maintained or to take multiple steps to ensure its security. And, in the event of a suspected breach, an Incident Response Team is ready to assist with technical, legal, and law enforcement resources to ensure the highest quality response.

Business Problem and Solution

An assessment in 2005 determined this simple conclusion about the State of protection of personal information in Indiana state government: Indiana has thousands of information systems that collect personal information, but no one knows how many, where they are stored, or who is responsible for them. You cannot protect what you do not know.

To combat this, the State inventoried all of its IT systems (and all manual processes that systematically collect personal information) in a searchable online application known as the Information Systems Inventory, established a new Information Resources Use Agreement (IRUA), trained all employees through an online (verifiable) training program on their responsibilities under IRUA and the repercussions for violating it, and established an Incident Response Team to act immediately when personal information is believed to have been disclosed beyond the State workforce. (The systems inventory is repeated each year and users are regularly retrained on their responsibilities to protect state data.) Additionally, the State has removed Social Security numbers from its public-facing online applications or, where they could not be removed, encrypted that data.

Significance of the Project to the Improvement of the Operation of Government

It does not take a genius to inventory all state IT systems, but it is a *fundamental* first step and one that must be regularly revisited, as IOT continues to do. The real work is the cultural shift, changing state IT professionals into *system owners* who are personally responsible for the applications they develop and maintain. Now, the State has owners for each system and those system owners understand that just because they have a contractor supporting the system (and though the contractor has responsibilities to protect the data) the system owner is personally responsible for the system.

Public Value of the Project

The value to the public is plain. The public rightfully expects that the State will keep personal informant secure.