

2009 NASCIO Recognition Awards Nomination

A. Title: Sensitive Data Protection with Endpoint Encryption

Category: Information Security and Privacy

State: Ohio

B. Executive Summary

Protecting the confidentiality of the information the State of Ohio collects about its citizens and businesses is a high priority.

In response to a major data-loss incident, which occurred in 2007, Ohio re-examined its approach to information security and strengthened its policy and organizational efforts for securing sensitive data. Extending those policy and organizational improvements down to the functional layer of government was key to strengthening security.

Therefore, Ohio began endpoint encryption, an immediate initiative to address and revamp its approach to endpoint data protection. This initiative was driven by the recognition that mobile devices present a high-risk threat for the loss of critical and confidential data.

To protect sensitive information that might be stored on laptop computers and other portable computing devices, Ohio acquired and implemented SafeBoot full disk encryption. Full disk encryption capability was acquired for more than 70,000 devices between August 2007 and September 2008.

The SafeBoot solution was selected and implemented through a collaborative process, which helped ensure that the solution met the needs of the state enterprise as well as the diverse needs of individual state governmental entities.

C. DESCRIPTION OF THE BUSINESS PROBLEM AND SOLUTION

Business Problem Description

Due to the quantity and potential value of the personal information that governmental entities collect and hold, they are prime targets for attempts by criminals to harvest sensitive information. The risk of data compromise due to the loss or theft of portable computing or data storage devices is especially high because of the inherent mobility and generally small form factor of those devices. They are typically lost or stolen more easily and more often than other computing devices. In addition, the number of such devices in use has been rapidly increasing, which makes incidents involving them more likely.

The distributed nature of Ohio's technical environment and IT governance structure served as a barrier to reducing Ohio's risk for data compromise due to lost or stolen portable devices. Varying management approaches, technical architectures and skill levels relevant to data protection existed among Ohio's state agencies. There was no strong enterprise view of data protection, and policies were at a baseline level with only limited requirements concerning protection of high-risk information.

Multiple studies have indicated that the largest single cause of data loss, which may lead to identity theft, is from lost or stolen portable computing or data storage devices. Unfortunately, Ohio experienced a major data loss of this type in June 2007, when a data storage device was stolen. The device contained sensitive information about nearly 1.2 million people and businesses, including Social Security numbers, federal tax IDs and banking information.

This highly publicized incident created a risk for the public and was costly for Ohio due to the loss of the public's trust and the time and money spent responding to the incident. Ohio notified potentially affected individuals and purchased one year of identity-theft protection services for those impacted by the incident. The estimated cost of this single incident was more than \$2 million.

Solution Description

In the aftermath of the data loss incident, Ohio began to turn around its approach to data protection through improved leadership and coordination efforts, an improved security policy stance, and applied shared solutions.

Leadership and Coordination - The role of the existing State Chief Privacy Officer position was expanded. A Data Privacy Point of Contact within each state agency was established. A multi-agency Data Protection Subcommittee was created. Later, the positions of State Chief Privacy Officer and State Chief Information Security Officer were established by law (see milestones below).

Improved Security Policy Stance – Sensitive data policies and an encryption standard were published (see milestones below). Existing state IT policies and standards were reviewed and revised to ensure they reflected the latest best practices and industry trends particularly with regard to enhanced risk management processes and security

controls. Updated policies covered topics such as security education and awareness, security notifications, data classification and intrusion prevention and detection. In addition, assurance materials were developed – white papers, frequently asked questions, fact sheets and audit checklists – for each statewide IT security policy.

Applied Shared Solutions – Solutions for endpoint encryption and IT asset tracking, SafeBoot and Computrace products respectively, were acquired and implemented (see below).

Endpoint Encryption: SafeBoot¹

To protect sensitive information that might be stored on laptop computers and other portable computing devices, Ohio acquired and implemented an endpoint encryption solution known as SafeBoot full disk encryption. The SafeBoot solution included software for a variety of end-user devices with a centralized management capability, as well as services for extended maintenance, installation, configuration and on-site training for administrators.

The acquisition and enterprise implementation of the SafeBoot solution by Ohio was accomplished with unprecedented speed through a highly collaborative process. By working together across all branches of state government, Ohio was able to implement the solution in less than a year in a manner flexible enough to meet the diverse needs of state entities and at the lowest available cost.

With leadership, coordination and most of the funding provided by the Ohio Department of Administrative Services (DAS), Office of Information Technology (OIT), Ohio acquired 70,369 SafeBoot licenses for \$1,113,342 between August 2007 and September 2008. Most agencies completed their laptop encryption efforts by July 2008, and many have implemented optional desktop encryption.

In addition to agency collaboration and OIT-coordinated purchases and funding, other keys to the success and speed of implementation of endpoint encryption are:

- a unified helpdesk within OIT to resolve issues between agencies and the vendor;
- a listserv for those agency staff implementing Safeboot; and
- published documentation on the program at <http://www.privacy.ohio.gov/government/>.

Finally, Ohio reached an agreement with the vendor to extend the negotiated pricing for the encryption product to Ohio's public universities and local governments through the state's cooperative purchasing program.

Major milestones included the following:

¹ SafeBoot was acquired by McAfee, and the SafeBoot product is now known as McAfee Endpoint Encryption.

June 2007 – Governor Strickland issued Executive Order 2007-13S, Improving State Agency Data Privacy and Security. Data Privacy Points of Contact were established in each agency.

July 2007 – Ohio IT Standard ITS-SEC-01, “Data Encryption and Cryptography,” which defines the minimum requirements for using encryption to secure sensitive data was issued. Ohio IT Bulletin ITB-2007.02, “Data Encryption and Securing Sensitive Data,” which requires encryption of sensitive data on portable devices in addition to other requirements was issued.

August 2007 – The Multi-Agency CIO Advisory Council, a group established to provide agency recommendations to the State Chief Information Officer, formed the Data Protection Subcommittee (DPSC) to address many facets of data protection including endpoint encryption. The DPSC, which represents 30 state agencies, was chartered to share cross-agency research and experience in information security practices.

September 2007 – OIT and the DPSC jointly formulated enterprise requirements for endpoint encryption. Since Ohio, like many other states, operates a highly federated computing environment, there was great diversity among hardware and operating systems in use. Participants had to pool and then prioritize their individual requirements to create a core set of requirements for the enterprise.

October 2007 – OIT issued a Request for Quotation for encryption vendors based on Gartner Magic Quadrant rankings. Seven of 12 vendors responded, and six qualified for consideration. SafeBoot scored highest in meeting requirements and had the best price at \$11.56 per license for quantity purchase.

November 2007 – A Master License Agreement was established with SafeBoot and Spectrum Systems, a reseller and GSA SmartBuy contract holder that also had an Ohio State Term Schedule contract. OIT purchased 61,019 SafeBoot licenses and the first two years of maintenance on behalf of all agencies, and authorized distribution of all but 37 licenses for \$813,858.

December 2007 – OIT coordinated agency SafeBoot license requests and began the license issuance process. OIT offered licenses to more than 100 state agencies, boards, commissions, offices of statewide elected officials, the Ohio House of Representatives, the Ohio Senate and the state judiciary. Most chose to participate; cabinet-level agencies are required to encrypt state-owned laptops.

January 2008 – OIT coordinated SafeBoot administrator training sessions, which served 167 people from 36 agencies; implementation began.

February 2008 – Many agencies completed laptop encryption. A major obstacle, which had to be overcome, was implementing decentralized administration. Most endpoint encryption products including SafeBoot use a single centralized administration model

for their enterprise installations. Ohio's federated model of IT governance and diverse computing environment meant that administration was carried out on a per-agency basis. This situation required essentially 40 to 50 separate customized setups for administration instead of one.

July 2008 – Most agencies completed laptop encryption and many agencies completed optional desktop encryption.

September 2008 – The Ohio Department of Job and Family Services, Ohio's largest agency, purchased an additional 9,350 SafeBoot licenses. The positions of chief privacy officer and chief information security officer are established by Ohio statute, and Ohio agencies are required by law to complete privacy impact assessments for new information systems.

IT Asset Tracking: Computrace

In addition to the SafeBoot implementation and with the endorsement of the DPSC, OIT made arrangements with Absolute Software for the purchase of Computrace for existing computers at a substantially reduced price in May and June 2008. The Computrace product provides the ability to track lost or stolen computers and to remotely delete sensitive information they may contain. Absolute extended the offer as well as a discounted price for installation on new computers through June 2010.

OIT purchased implementation training for 32 people from 14 agencies in July 2008 and provided ongoing support and online training sessions as needed through December 2008. As of December 2008, 18 agencies have implemented more than 16,000 Computrace licenses, mainly on laptops.

D. SIGNIFICANCE OF THE PROJECT

Protecting the confidentiality of the information Ohio collects about its citizens and businesses is a high priority. State of Ohio employees hold positions of trust both in preserving the confidentiality of constituent information and in safeguarding state information resources. Ohio's commitment to protecting citizen data is evidenced by legislation, management directives, executive orders signed by the governor and directives from the State Chief Privacy Officer and State Chief Information Officer.

The SafeBoot implementation not only improved the security of citizen information, but also improved compliance with state law and policy and provided alignment with statewide IT architecture. In addition, the SafeBoot solution was acquired at reduced cost compared to what agencies might have paid if they had acted individually. The implementation was accomplished through collaboration among state government entities and represents the first enterprise-wide implementation of a data protection solution in Ohio state government.

E. BENEFIT OF THE PROJECT

While implementing endpoint encryption cannot entirely eliminate the risk of data being compromised when a laptop is lost or stolen, it significantly reduces the risk. Lowering

the risk of data compromise lowers the potential impact when a laptop is lost or stolen, and can help avoid loss of constituent trust, negative publicity and costs associated with data loss notification.

The pricing on the SafeBoot Master License Agreement represented a discount of 91 to 94 percent from single-quantity pricing. By leveraging the state's coordinated buying power, Ohio is estimated to have avoided a cost of at least \$3.7 million compared to each state agency independently acquiring encryption solutions. Also, by law, state agencies are required to notify individuals of a data breach involving personal information unless such information is encrypted or redacted. In 2006, research by the Ponemon Institute revealed the average cost of a data breach per record compromised grew 30 percent, averaging a total of \$4.8 million per breach. State agencies using endpoint encryption can avoid the burdensome costs of notifying parties of a breach since such data is rendered inaccessible through cryptography.

Implementing an endpoint encryption solution aligns with the NASCIO 2009 state Chief Information Officer priorities of security, data protection and mobile workforce enablement. The SafeBoot full disk encryption implementation has provided a higher level of protection for constituent data and a greater level of control over unauthorized access to data when a laptop is lost or stolen. Prior to this implementation, there was little to no data protection provided when state laptops were lost or stolen.

Deployment of an enterprise solution for the protection of information security and privacy was dependant upon the enterprise research, selection and implementation of SafeBoot. The laptop encryption initiative was driven by an immediate business need and recognition of the high-risk threat potential present to loss of critical and confidential data through highly exposed mobile devices.

This initiative successfully delivered beneficial results in several critical areas:

- Risk assessment and active protection measures for mobile computing devices that may contain critical personal and confidential information;
- Delivery of an encryption security solution that would be successfully deployed and supported in a decentralized organizational structure;
- Joint state-level leadership and proactive support in creating a data security and privacy culture;
- Joint effort in organizing and implementing a statewide security solution to support the end-user mobile computing environment, which is flexible enough for the various client configurations;
- Protection for an external threat exposure to data on a lost or stolen laptops;
- Lower total cost of ownership through the use of common software and maximized use and increase in knowledge and skills across state agencies.

Through organizational leadership, policy setting and solution implementation, the State of Ohio improved its data privacy and security practices to safeguard the sensitive data entrusted to Ohio by its constituents.