

California Office of Privacy Protection

Protecting Privacy in State Government Training

NASCIO Recognition Awards 2009

Category: Information Security and Privacy



CALIFORNIA
**OFFICE OF
PRIVACY
PROTECTION**

Executive Summary

Organizations that collect and store sensitive information are responsible for keeping that information secure. California state government is no exception. Data breaches have the potential to expose California residents to the risk of identity theft and other forms of privacy invasions. In addition to the harm these privacy lapses can cause residents, data breaches also cost state governmental agencies, in both dollars and the loss of public confidence.

In 2003, California passed a landmark law requiring notification of individuals when their sensitive personal information had been compromised. The notification requirement forced executive management – often for the first time – to review their organization’s privacy policies. These initial examinations directed a spotlight on the negative effects, in both cost and operations, of poorly conceived and executed information privacy and security policies.

In September 2006, a statewide policy was issued that required all California state agencies to implement “ongoing education and training, at least annually, for all employees and contractors who handle personal, sensitive or confidential information.” Before this policy memo, training on how to handle confidential information was uneven or nonexistent.

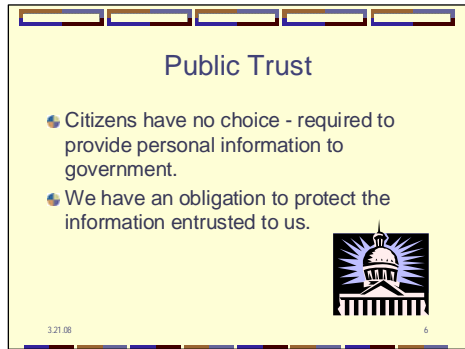
The California Office of Privacy Protection’s basic privacy training package focuses on best practices for interacting with personal and otherwise sensitive information, ensuring that state agencies are protecting individuals’ personal information and complying with California’s expansive privacy laws.

Protecting Privacy in State Government – COPP’s training program – does not use technical terms and contains practical advice on what to do and what not to do in handling sensitive information in typical work situations. While it does address legal requirements and the consequences of not meeting them, the focus of the training is on day-to-day operations.

There are two primary groups that benefited from the COPP’s basic privacy training program, California state agencies and California residents. California state agencies are better able to meet the rigors of California privacy law with focused professional training. The training has helped to bring an awareness of good privacy practices to those in government who are most in need of it – the employees whose information-handling practices can put people at risk.

Description of Problem

Organizations that collect and store sensitive information are responsible for keeping that information secure. California state government is no exception. Data breaches have the potential to expose California residents to the risk of identity theft and other forms of privacy invasions. In addition to the harm these privacy lapses can cause residents, data breaches also cost state governmental agencies, in both dollars and the loss of public confidence.



In 2003, California passed a landmark law requiring notification of individuals when their sensitive personal information had been compromised. The notification requirement forced executive management – often for the first time – to review their organization’s privacy policies. These initial examinations directed a spotlight on the negative effects, in both cost and operations, of poorly conceived and executed information privacy and security policies.

One of the most important lessons learned from data breaches is the critical role played by individual employees who are ignorant of or careless in following good data protection practices. In September 2006, a statewide policy was issued that required all California state agencies to implement “ongoing education and training, at least annually, for all employees and contractors who handle personal, sensitive or confidential information.”¹ Before this policy memo, training on how to handle confidential information was uneven or nonexistent. Some agencies provided information security training for just their IT staff, others provided specific training to selected staff, and still others provided no training at all. Without a statewide training program there would continue to exist a broad spectrum of employees whose work requires them to interact with sensitive information but who were provided no formal privacy training. To remedy this, the California Office of Privacy Protection (COPP) developed a basic privacy training practice.



¹ Management Memo 06-12: Protection of Information Assets, available online at http://www.documents.dgs.ca.gov/osp/sam/mmemos/MM06_12.pdf.

Solution

With data breaches becoming more costly and identity theft continuing to be an expansive problem, there was an impetus for California state government to provide annual information privacy training for any and all state employees and contractors who handle personal, confidential, or sensitive information. The urgency of this need to comply with the new statewide policy compelled COPP to write and deploy a basic privacy training that could be rolled out to the state's nearly 250,000 employees. The purpose of the privacy training was to provide California state agencies with the materials to train their employees to handle personal, sensitive, and confidential information in a manner consistent with California privacy laws, policies, and best practices. For the first iteration of this training, COPP would provide materials for classroom training and, as an alternative, self-training manuals.

The California Office of Privacy Protection's basic privacy training package focuses on best practices for interacting with personal and otherwise sensitive information, ensuring that state agencies are protecting individuals' personal information and complying with California's expansive privacy laws. As noted, the first form of training is a PowerPoint presentation with speaker notes and a self-training manual. These materials are available online at www.oispp.ca.gov/government/privacy/default.asp. In addition, to this training material, COPP is now developing a Web-based training module in order to increase the number of state agencies that can leverage COPP's expertise to meet the demands of protecting information in the modern workplace.

There were many barriers to achieving the desired outcome of better preparing California's workforce to properly handle sensitive information. For starters, the innovative first-in-the-nation California Office of Privacy Protection is a small (8.5 personnel per year) public-facing organization whose primary mission is to provide consumers with information and assistance on privacy issues and to recommend privacy practices to organizations.² As primarily an education and advocacy group, COPP wanted to develop a compelling training program and couple it with an aggressive outreach strategy. To meet this goal, COPP collaborated with the State Information Security Office to implement the basic privacy training for state employees in 2006.³ It also relied on departmental information security officers and training officers to deliver the training in their agencies.

² For more information on the California Office of Privacy Protection, see www.privacy.ca.gov.

³ In January 2008, the two offices were joined together in the Office of Information Security and Privacy Protection, with the dual mission of security state information and protecting consumer privacy. The Office of Privacy Protection retains its consumer focus within the new Office.

Costs and Project Implementation

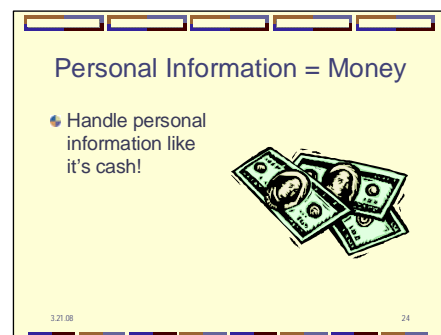
Between September and November 2006, COPP provided train-the-trainers instruction to departmental information security officers and training officers, enabling them to deliver the COPP-developed training throughout their agencies. This allows agencies the freedom to specialize their training to their workforce, but still ensures that a baseline of responsible information-handling practices is provided to all.

The costs to provide this statewide service were primarily staff time, with additional costs for photocopying and assembling the materials for training sessions and posting them on the web site. This resulted in a total cost of \$14,200.

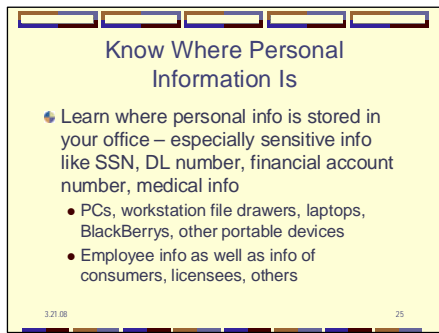
- 200 hours for research and development of training contents
- 80 hours for development and testing of PowerPoint presentation
- 24 hours for writing and testing of self-training manual
- 21 hours of train-the-trainers sessions
- Copying, assembling, Web posting, etc.

Significance

In developing the contents of the training, COPP reviewed both private and public sector privacy and security training programs. COPP found that the majority of these programs tended to be very legalistic, very technical, or both. A training regime that required the reader to master a glossary of terms in order to gain the intended value of the training was not going to fundamentally shift the way state workers operate with sensitive data on a day-to-day basis. While such programs may explain legal requirements, they are generally written at a theoretical level and do not speak to “the person in the cubicle.” Considering the audience of this training was not privacy or security experts, simply restating laws and policies were not seen as an effective way to make the message stick. The training’s goal was to make state employees understand at a fundamental level why protecting sensitive, personal, and otherwise confidential information was an absolute necessity. The extensive speaker notes provided with the slides were designed to enable non-technical persons, such as training officers, to deliver the training.

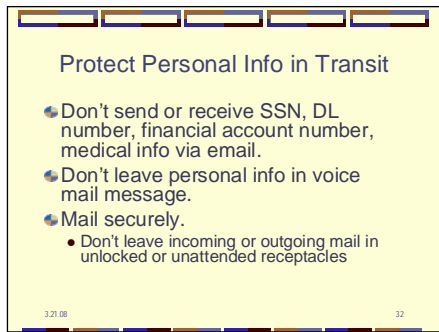


Protecting Privacy in State Government – COPP’s training program – does not use technical terms and contains practical advice on what to do and what not to do in



in unlocked recycling containers. The training also provides specific information on how to report a possible privacy breach or other information security incident.

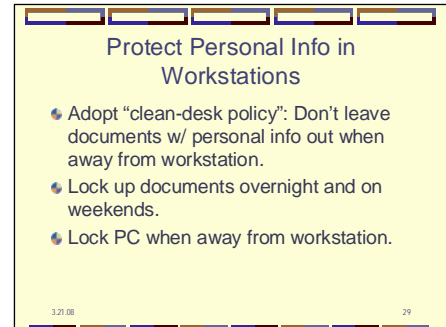
In addition to citing the legal and policy reasons for protecting privacy, the training specifically draws the connection between poor day-to-day privacy practices and identity theft. Making sure employees understand the connection to identity theft is one of the key ways to inspire those employees to care about privacy. Like the public in general, state employees are concerned about falling victim to identity theft – people understand inherently why adopting practices that minimize the risk for identity theft is something they should do. Making this link, between bad practices and the proliferation of identity theft, fundamentally changes how employees view privacy policy and



everyone's responsibility.

As COPP continues to improve upon the privacy training program, it plans to develop an interactive Web-based version, which will allow the addition of role-based modules.

handling sensitive information in typical work situations. While it does address legal requirements and the consequences of not meeting them, the focus of the training is on day-to-day operations. The practical tips include creating a strong memorable password by using a phrase, not sending Social Security numbers or other sensitive information in email, and not putting un-shredded records with



personal information

practices. It replaces the nebulous consequence of not following privacy policy with the very concrete consequence of subjecting a person to identity theft.

Also as a means of engaging employees, the word "privacy" is used more often than "security" in the training. This is because many employees view security as a technical matter that is the responsibility of a technical person, whereas privacy is seen as a personal concern that they care about. Privacy is

Benefits

There are two primary groups that benefited from the COPP's basic privacy training program, California state agencies and California residents. California state agencies are better able to meet the rigors of California privacy law with focused professional training. The training has helped to bring an awareness of good privacy practices to those in government who are most in need of it – the employees whose information-handling practices can put people at risk. The training is a critical component of California's comprehensive data privacy and security policies.

- The Management Memo requiring annual privacy training for state employees was issued on September 1, 2006.
- In seven two-hour sessions from September through November 2006, COPP staff trained 140 departmental information security officers and 45 training officers in how to deliver the training to employees in their departments.
- In 2007, 48 of 154 agencies (31%) reported having trained their employees.
- In 2008, 91 of 154, 59%, reported having trained employees – an increase of 59%.

The second group that benefits from COPP's basic privacy training is the people of California, whose personal, sensitive, and confidential information is collected, used, and stored by state government. The ongoing training of all state employees helps to merit a higher degree of public confidence in government's information stewardship.

Additional beneficiaries are other government agencies that have significantly relied on California's privacy training in developing training for their employees. Other jurisdictions are always welcome to use the California materials and adapt them to their situations. For example, the State of Ohio's training for their employees is based on California's, and the U.S. Department of Homeland Security also drew on the California materials in developing training for their employees.⁴

⁴ Available at www.privacy.ohio.gov/resources/Basic_Privacy-Security_Training.ppt.