



Agenda Item 8b

September 16, 2014

ITEM NAME: Information Security Update

PROGRAM: Enterprise

ITEM TYPE: Information

EXECUTIVE SUMMARY

Public and private sector organizations collect, process, and store a great deal of confidential information on computers and transmit that data across networks. With the growing volume and sophistication of cyber attacks, ongoing attention is required to protect sensitive business and personal information, as well as safeguard national security. During a Senate hearing in March 2013, the nation's top intelligence officials warned that cyber attacks are the top threat to national security, eclipsing terrorism.

In recognition of CalPERS highly sensitive financial, health, and investment data, this reporting item provides an overview of the current security environment and CalPERS information security measures designed to protect information assets with the most effective methods and technologies.

STRATEGIC PLAN

This agenda item supports Strategic Plan Goal B to "Cultivate a high-performing, risk-intelligent and innovative organization." CalPERS comprehensive information security measures provide a multi-tiered framework for risk reduction and increased privacy and protection of information assets.

BACKGROUND

CalPERS comprehensive information security program is a collaborative and integrated effort that ensures CalPERS technology and information remains secure against the constantly changing landscape of threats. It is focused on strengthening information security controls and implementing a proactive rather than a reactive approach to information security risk management. This program includes priorities, initiatives, and deliverables, with an eye on industry best practices and the latest preventative measures. CalPERS members, business partners, employees, Board and executives benefit through the reduction of risks and increased security of information assets.

ANALYSIS

All organizations, including CalPERS, are at financial and reputational risk as a consequence of inadvertent, unauthorized, or malicious disclosure of confidential and sensitive information. While cybersecurity threats continue to escalate, an

organization that continuously scans the environment, exercises ongoing vigilance, and implements a centralized approach to monitor, manage, and enhance the security framework increases their capabilities to protect and prevent the breach of critical information assets. The financial services industry had a notable increase in threat activity in the past year from 11% to 15%, as noted by the Mandiant 2014 Threat Report. CalPERS risk reporting through the Enterprise Risk Dashboard, the Top Risk Report, and the Quarterly Board Updates of the Security Roadmap Program demonstrate continual monitoring, tracking, prioritization, and responsiveness to potential threats and exposures. CalPERS engagement in numerous Security Taskforce Committees also affords visibility into regional and national threat activities for early detection and knowledge sharing of best practices.

BENEFITS/RISKS

CalPERS information security program upholds CalPERS commitment of acting ethically and helps protect public trust in CalPERS programs and systems by:

- Reducing the risk of inadvertent or malicious disclosure of confidential and sensitive information
- Complying with privacy laws and regulations (such as HIPAA and Civil Code 1798)
- Reducing risk of consequential damages including:
 - Reputational harm
 - Costly mandatory breach notifications
 - Loss of productivity due to system outages
 - Potential civil/criminal litigation

The benefits and features of CalPERS comprehensive information security program include:

- The advancement of financial and health security for all who participate in the CalPERS Pension and Health System
- A risk management philosophy that protects confidential member information and reduced risks in order to avoid significant security breaches with potentially serious financial and reputational ramifications
- An infrastructure that provides visibility to program areas to gauge compliance with all applicable laws, regulations, policies and best practices
- Program risk assessments and improved ability to conduct investigations, including deployment of tools to assist CalPERS divisions in identifying, monitoring and mitigating risks
- An oversight entity, comprised of various IT teams to ensure that patch management is carried out as a repeatable and effective process
- Streamlined processes to facilitate the production of evidence to support appropriate chain of custody for discoverable electronic mail
- Reduced complexity, time, and costs associated with responding to electronic discovery requests
- Improved IT resource efficiencies by automating security processes

CalPERS comprehensive information security program promotes a responsive risk intelligent environment with continual training on risk management and information security resulting in increased awareness and vigilance throughout the organization.

ATTACHMENTS

Attachment 1 – Information Security Update Presentation

KATHLEEN K. WEBB
Chief Risk and Compliance Officer
Office of Enterprise Risk Management

LIANA BAILEY-CRIMMINS
Chief Information Officer
Information Technology Services Branch

CHERYL EASON
Chief Financial Officer

DOUGLAS HOFFNER
Deputy Executive Officer
Operations and Technology