

Information Security Update

Finance and Administration Presentation

Liana Bailey-Crimmins, Chief Information Officer

Agenda Item 8b, Attachment 1
September 16, 2014

Agenda

- What is Cybersecurity
- Common Risks & Threats
- Industry Best Practices
- CalPERS Security Measures
- Current Initiatives & Benefits
- Next Steps

Cybersecurity Buzz

Mary Jo White, Chair of the Securities and Exchange Commission: "Cyber threats are first on the Division of Intelligence's list of global threats, surpassing terrorism."



2010 - 2015

The federal government has allotted over **\$13 billion** annually to Cybersecurity



The U.S. Army is recruiting cyber warriors for cyber command unit

Recent examples of costs for compromised security

House Intelligence Committee Chair, Mike Rogers - July 2013



\$100 million
lost in attack on a U.S. financial institution

\$2 trillion
lost in attacks from hackers outside the U.S.



3.3 million
Bank Account Numbers

5,000
Expired Credit Card Numbers

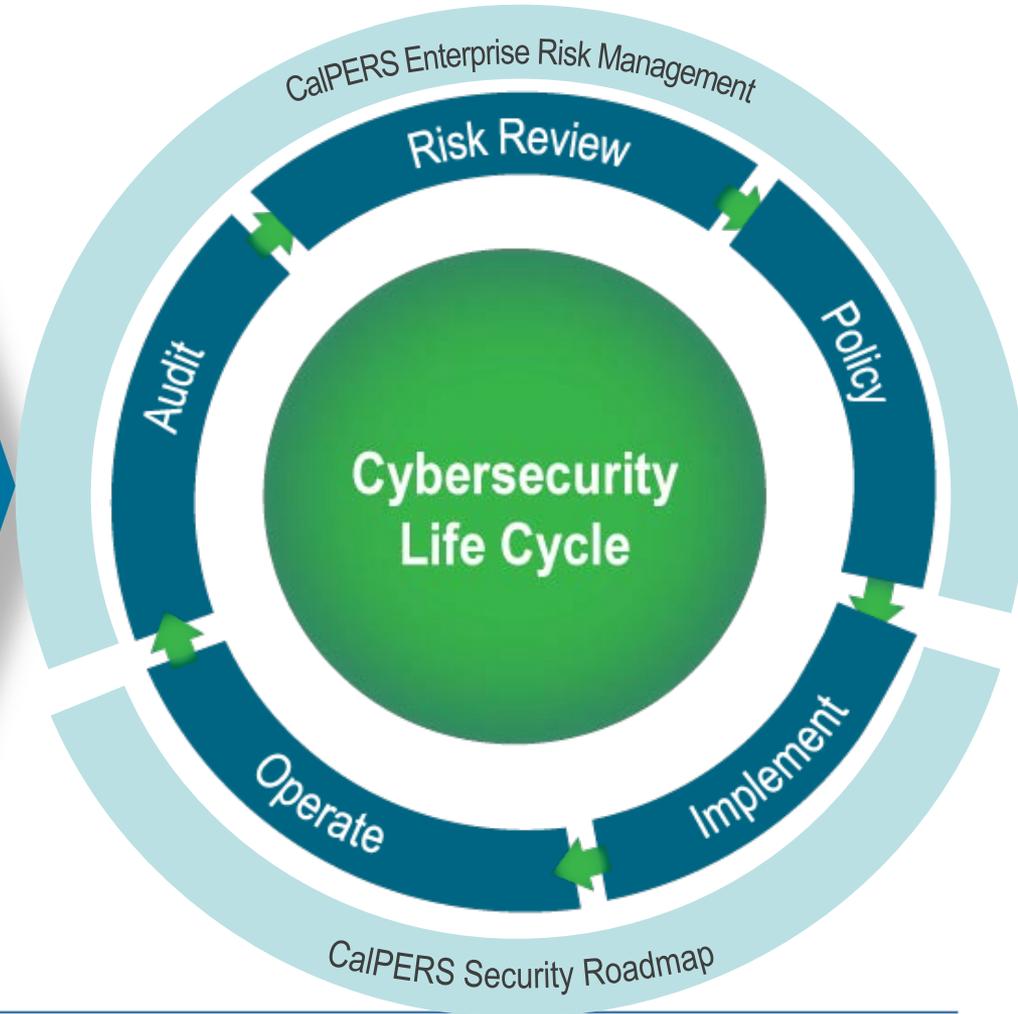
1.9 million
Dependents Information

\$12 million
in Identity Protection Services for Tax Payers

South Carolina Governor, Nikki Haley - Nov 2012

What is Cybersecurity

Cybersecurity, also known as information technology security, refers to preventative methods used to protect information on computers, networks, programs, and data from unauthorized access, change, or destruction.

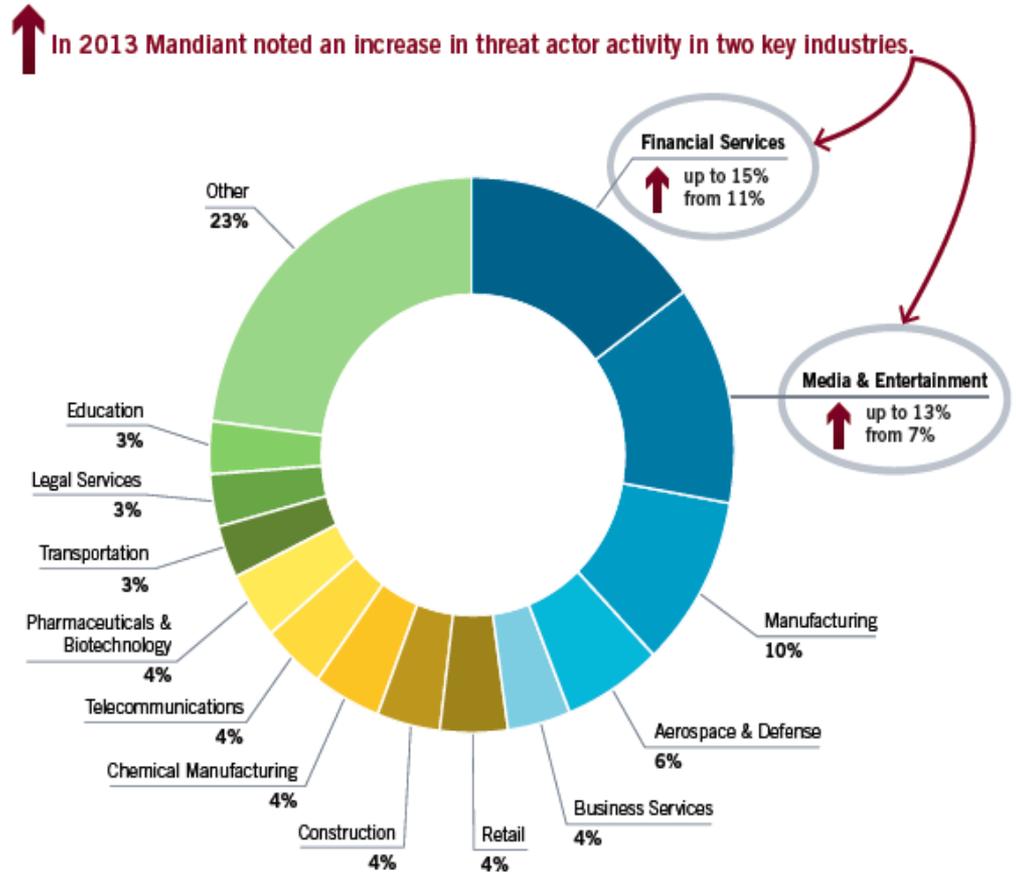


Cybersecurity | Not Just an IT Issue

“Cybersecurity has gone mainstream. It has gone from a niche IT issue to a consumer issue and boardroom priority. Everyone now knows what seasoned security professionals have long been aware of: **there is no such thing as perfect security.** Security breaches are inevitable, because determined threat actors will always find a way through the gap.”

Mandiant | 2014 Threat Report

Industries Targeted by Cyber Threat Actors



Cybersecurity Risks

CalPERS Highly Sensitive Data



Financial

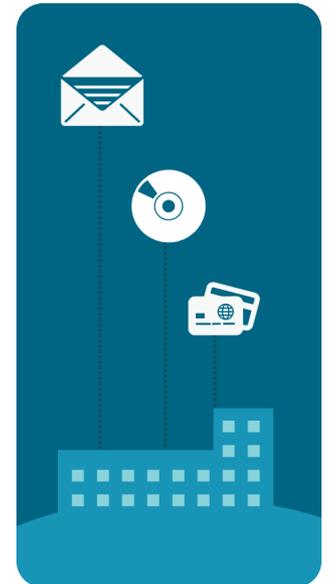


Health



Investments

- Financial and reputational risk is a consequence of inadvertent, unauthorized, or malicious disclosure of confidential and/or sensitive information
- There are numerous ways data can leave the enterprise: email, webmail, file transfers, CD and DVD drives, external storage devices such as USB drives, cloud storage, etc.



Industry Best Practices

IBM Best Practices White Paper



View Security as Risk Management

- Security is a key operational domain. Since services depend on the reliability and credibility of data and systems, cybersecurity becomes an essential risk management function.



Create a Fully Integrated Security Enterprise

- The best way to improve visibility and gain operational control is to integrate previously disparate, disconnected business processes and take a centralized approach to managing security where program and IT work together.



Use Business-Oriented Security Metrics

- In order to run cybersecurity as a true enterprise function, management needs a framework with which to establish a baseline for current security programs, understand the context and critical interdependencies, and set priorities accordingly.

National Institute of Standards and Technology

Executive Order 13636 Improving Critical Infrastructure Cybersecurity

- Step 1: Prioritize and Scope
- Step 2: Orient
- Step 3: Create a Current Profile
- Step 4: Conduct a Risk Assessment
- Step 5: Create a Target Profile
- Step 6: Determine, Analyze, and Prioritize Gaps
- Step 7: Implement Action Plan

CalPERS Comprehensive Security Program

Operations



- Risk assessments
- Environmental scans
- Policy development
- Education for staff, members, employers, partners, and Board
- Incident management
- Collaboration with government & vendor partners
- Different approaches for insider threats vs outsider threats

Initiatives



Security Roadmap & Framework

- Joint effort between program and technology
- Create an ongoing Security Program with the initial focus on implementing the latest preventative measures through 25+ projects
- Quarterly reports to the Board
- Manage, measure, test, and track known information security vulnerabilities
- Conduct yearly risk assessment to reevaluate security environment and priorities



Infrastructure

- Sophisticated technology for effective integration & enhanced intelligence

Risk Reporting

- Enterprise Risk Dashboard
- Top Risk Report
- Quarterly Board Updates

Top Risk Report: Information Security				
Risk Category: Operational	May-13	Oct-13	May-14	Current Trend
Risk Domain Rating	▲	▲	▲	▼
Rating Comments: There is no change to the risk rating in this reporting period.				
Risk Statement				
This domain identifies risks that may impact information security that protects access to employer and member personal health and financial data, and prevents loss of information assets. Includes compliance with CalPERS information security policies and state requirements.				
Designated Executive Owner:		DEO, Operations & Technology Chief Financial Officer		
Sub Risks				
<ul style="list-style-type: none"> • Large Scale Data Breach • Targeted Information Disclosure • Compromised System Operation and Integrity • Detection of Malicious Activity • Severe Denial of Service Attack 				
Management's Risk Response Strategies: Accomplished Risk Response				
<ul style="list-style-type: none"> • Provided information security awareness training • Created information security policy for data protection [ERMD/ISMS] • Identified and classified business data (ERMD/ISMS) • Required authorization for business data leaving CalPERS (ERMD/ISMS) • Implemented technical controls on CDs, DVDs, and USB storage devices • Implemented security configurations for desktops in compliance with rigorous US Government standards • Applied technical controls that include firewalls, intrusion detection and prevention systems, and malicious code protection systems • Performed security assessment for remote access systems • Implemented limited myCalPERS security reports 				
Management's Risk Response Strategies: Ongoing Risk Response				
<ul style="list-style-type: none"> • Locate and secure data using Data Loss Prevention technology • Implement and manage security patches for CalPERS information systems • Provide technical staff training • Apply antivirus protection and remediation tools • Monitor sensitive data leaving CalPERS via our network 				
Management's Risk Response Strategies: Planned Risk Response				
<ul style="list-style-type: none"> • Implement Security Incident and Event Monitoring • Implement protection for non-CalPERS web based email and storage • Implement Network Access Control systems to improve controls over access to our network 				

Benefits to CalPERS Stakeholders

Members	<ul style="list-style-type: none">• Increased privacy and protection for personally identifiable information (PII) and protected health information (PHI)• Increased trust in CalPERS programs and services• Minimized risk of a disruption to services
Business Partners	<ul style="list-style-type: none">• Increased privacy and protection for business partner managed data• Increased trust in CalPERS programs and services• Increased protection for data transfers• Reduced risks associated with information disclosures and disruption to services
Employees	<ul style="list-style-type: none">• Enhanced information security awareness & education• Increased risk awareness through technical security training for IT and Risk Management Staff• Increased privacy and protection for employee data• Increased trust in CalPERS programs and services
Board and Executives	<ul style="list-style-type: none">• Increased trust in CalPERS programs and services• Reduced risks associated with unauthorized information disclosures• Reduced liabilities in the event of a large scale information security incident• Increased compliance with regulatory requirements

Next Steps

Cyber threats are continuously evolving and becoming more sophisticated.

Security is never 'done'.
– Gartner

CalPERS is committed to:



Ongoing Vigilance



Engagement in Security Taskforce Committees, such as:



Continuous Assessment of Risk



Re-Prioritization Based on Assessment



CA Technology Agency



Cal OES
OFFICE OF
EMERGENCY SERVICES



CA Cybersecurity
Task Force



HTCIA
HIGH TECHNOLOGY CRIME
INVESTIGATION ASSOCIATION



MS-ISAC
MULTI-STATE
Information Sharing
& Analysis Center



NIST
National Institute
of Standards
and Technology