University of California
2019 Ethics, Compliance and Audit Symposium

REACHING NEW HEIGHTS

The Third Line of Defense in Cybersecurity Internal Audit and the UC Cybersecurity Audit Team

Greg Loge – Systemwide Cybersecurity Audit Director

Tye Stallard – Systemwide Cybersecurity Audit Specialist

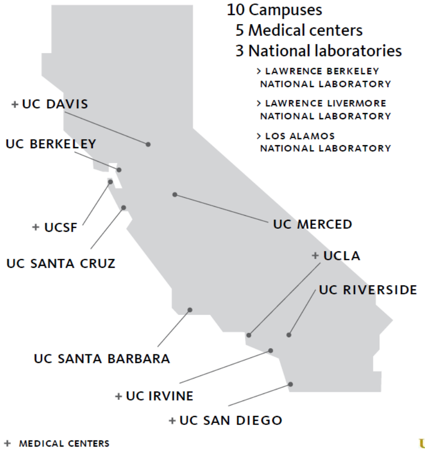
UNIVERSITY OF CALIFORNIA Ethics, Compliance & Audit Symposium
REACHING NEW HEIGHTS

Overview

1. University of California and Internal Audit
2. Establishing the Cybersecurity Audit Team (CAT)
3. CAT Structure
4. Projects
5. Engaging the Board

The University of California at a Glance

The University of California improves the lives of people in California and around the world through world-class educational opportunities, groundbreaking research, top-rated health care and agricultural expertise. We are driven by values of public service in all we do.



10 Campuses
5 Medical centers
3 National laboratories

- › LAWRENCE BERKELEY NATIONAL LABORATORY
- › LAWRENCE LIVERMORE NATIONAL LABORATORY
- › LOS ALAMOS NATIONAL LABORATORY

EDUCATION	
Total enrollment	280,380
Undergraduate students	222,493
Graduate students	57,887
Alumni	2.0 M
More than 160 academic disciplines	
More than 800 degree programs	

UC HAS SET A GOAL OF PRODUCING 1.2M GRADUATES BY 2030.

FACULTY AND STAFF	
Faculty	23,300
Other academic (postdocs, etc)	47,000
Staff	157,400
Represented employees	59%

UC IS THE STATE'S THIRD LARGEST EMPLOYER.

RESEARCH IMPACT	
Inventions per day (avg.)	5
Inventions (FY2017)	1,716
Startups founded on UC patents (TO DATE)	1,125
Active inventions (FY2017)	12,528

MANY OF THE CALIFORNIA'S LEADING INDUSTRIES GREW FROM UC RESEARCH, INCLUDING BIOTECHNOLOGY, COMPUTING, SEMICONDUCTORS, TELECOMMUNICATIONS AND AGRICULTURE.

MEDICAL CENTERS AND CLINICS	
Outpatient visits	4.7 M
Emergency room visits	375,104
Inpatient days by payer	174,839
Medicare patients Medi-Cal patients	31% 36%

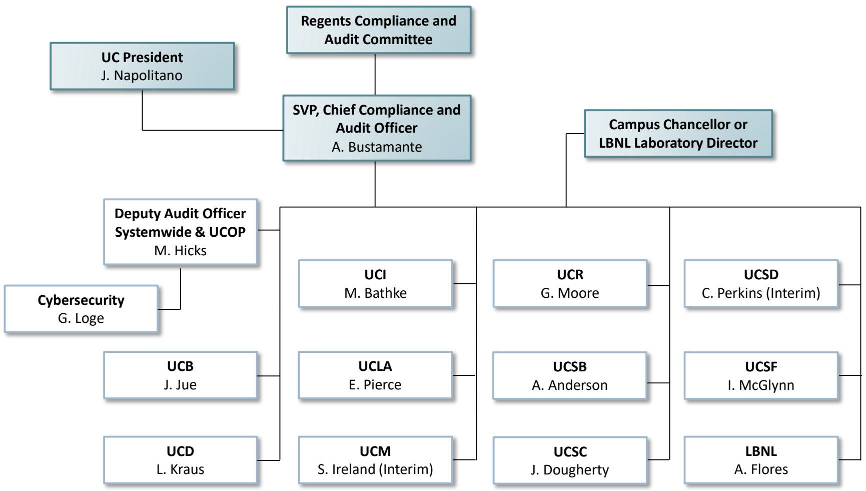
UC MEDICAL CENTERS PERFORM HUNDREDS OF CLINICAL TRIALS EACH YEAR, RESULTING IN NEW DRUGS AND DISEASE TREATMENTS.

All data as of April 2017 unless otherwise stated. See: http://universityofcalifornia.edu/infocenter for more information.

Internal Audit at UC

- Over 100 auditors in total across the system
- Audit departments at each location
  - 10 Campuses, National Laboratory, Office of the President
- Systemwide office reports to independent board and oversees the audit function
- Dual reporting at the systemwide and location level
- IT auditors and healthcare auditors based at locations

UC Internal Audit Organization Chart



Regents Compliance and Audit Committee

UC President
J. Napolitano

SVP, Chief Compliance and Audit Officer
A. Bustamante

Campus Chancellor or LBNL Laboratory Director

Deputy Audit Officer Systemwide & UCOP
M. Hicks

Cybersecurity
G. Loge

UCI
M. Bathke

UCR
G. Moore

UCSD
C. Perkins (Interim)

UCB
J. Jue

UCLA
E. Pierce

UCSB
A. Anderson

UCSF
I. McGlynn

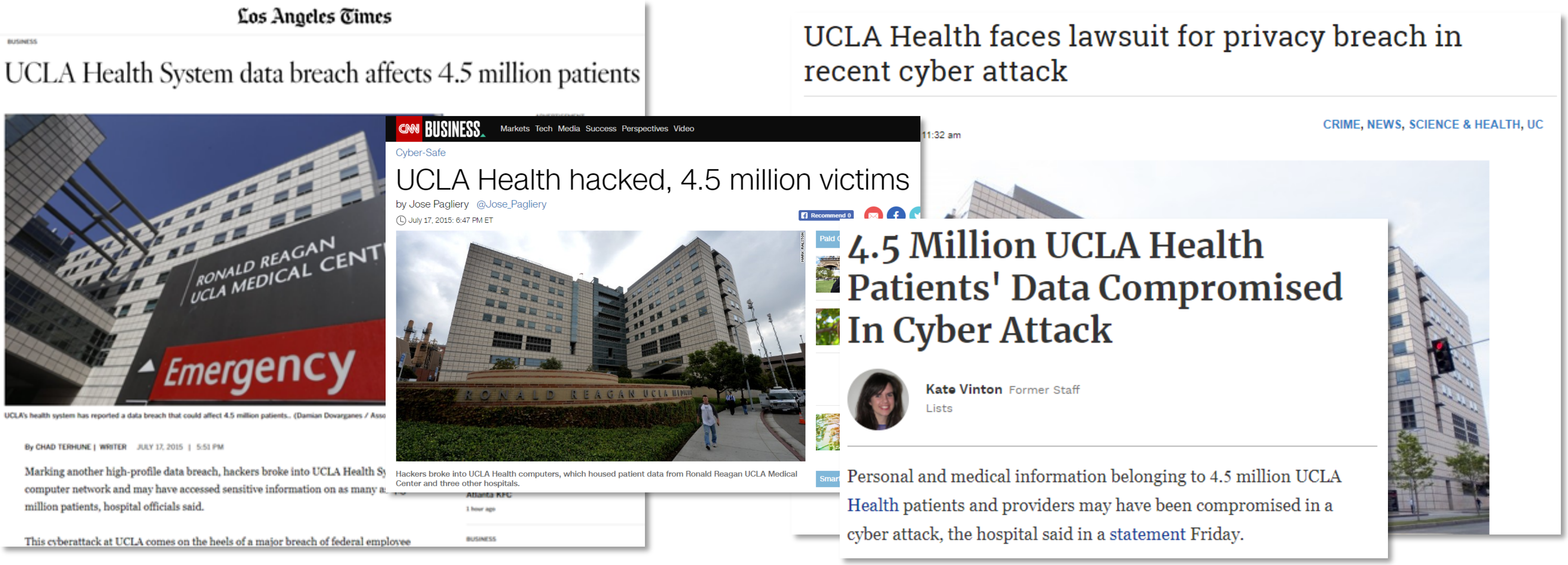
UCD
L. Kraus

UCM
S. Ireland (Interim)

UCSC
J. Dougherty

LBNL
A. Flores

Cyber Attack: Catalyst for Change



Los Angeles Times

BUSINESS

UCLA Health System data breach affects 4.5 million patients

UCLA's health system has reported a data breach that could affect 4.5 million patients.. (Damian Dovarganes / Asso

By CHAD TERHUNE | WRITER JULY 17, 2015 | 5:51 PM

Marking another high-profile data breach, hackers broke into UCLA Health Sy computer network and may have accessed sensitive information on as many a million patients, hospital officials said.

This cyberattack at UCLA comes on the heels of a major breach of federal employee

CNN BUSINESS Markets Tech Media Success Perspectives Video

Cyber-Safe

UCLA Health hacked, 4.5 million victims

by Jose Pagliery @Jose_Pagliery

July 17, 2015: 6:47 PM ET

Hackers broke into UCLA Health computers, which housed patient data from Ronald Reagan UCLA Medical Center and three other hospitals.

UCLA Health faces lawsuit for privacy breach in recent cyber attack

CRIME, NEWS, SCIENCE & HEALTH, UC

11:32 am

4.5 Million UCLA Health Patients' Data Compromised In Cyber Attack

Kate Vinton Former Staff

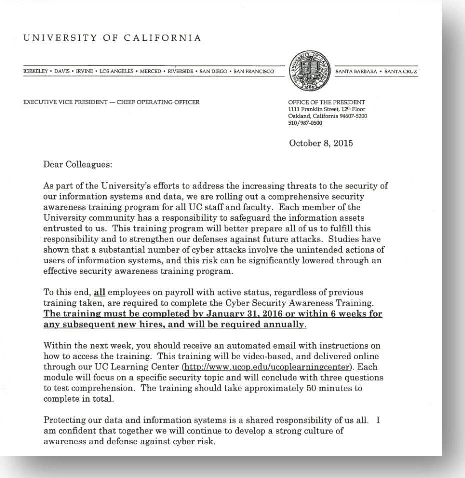
Lists

Personal and medical information belonging to 4.5 million UCLA Health patients and providers may have been compromised in a cyber attack, the hospital said in a statement Friday.

UNIVERSITY OF CALIFORNIA Ethics, Compliance & Audit Symposium REACHING NEW HEIGHTS

The University's Response

- A leading cybersecurity firm engaged to assist in analyzing network activity at all UC locations to **detect and respond to any advanced persistent threat** activity
- Every UC location submitted a **120-day cybersecurity action plan** to harden systems and improve administrative and physical safeguards
- A **Cyber-Risk Governance Committee** (CRGC) was established to oversee and guide system-wide strategies and plans related to cybersecurity
- A system-wide **incident escalation protocol** was developed to ensure that the appropriate governing authorities are informed in a timely way of major incidents
- **Mandatory cybersecurity training** was rolled out to all UC employees



UNIVERSITY OF CALIFORNIA

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO SANTA BARBARA • SANTA CRUZ

EXECUTIVE VICE PRESIDENT — CHIEF OPERATING OFFICER

OFFICE OF THE PRESIDENT
1111 Franklin Street, 12th Floor
Oakland, California 94607-5200
510/987-0500

October 8, 2015

Dear Colleagues:

As part of the University's efforts to address the increasing threats to the security of our information systems and data, we are rolling out a comprehensive security awareness training program for all UC staff and faculty. Each member of the University community has a responsibility to safeguard the information assets entrusted to us. This training program will better prepare all of us to fulfill this responsibility and to strengthen our defenses against future attacks. Studies have shown that a substantial number of cyber attacks involve the unintended actions of users of information systems, and this risk can be significantly lowered through an effective security awareness training program.

To this end, all employees on payroll with active status, regardless of previous training taken, are required to complete the Cyber Security Awareness Training. **The training must be completed by January 31, 2016 or within 6 weeks for any subsequent new hires, and will be required annually.**

Within the next week, you should receive an automated email with instructions on how to access the training. This training will be video-based, and delivered online through our UC Learning Center (http://www.ucop.edu/ucoplearningcenter). Each module will focus on a specific security topic and will conclude with three questions to test comprehension. The training should take approximately 50 minutes to complete in total.

Protecting our data and information systems is a shared responsibility of us all. I am confident that together we will continue to develop a strong culture of awareness and defense against cyber risk.

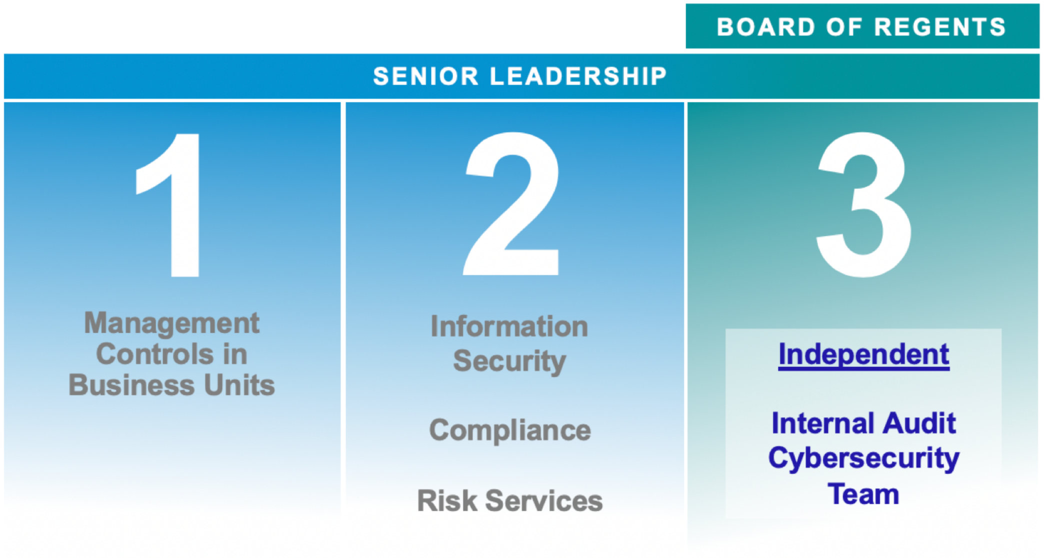
Establishing the Cybersecurity Audit Team (CAT)

- Need for greater cybersecurity expertise in internal audit across UC locations
- Evolving UC IT environment – More systemwide IT initiatives not tied to a single campus
- Cyber-risks increasing in complexity and significance and affecting multiple locations

Cybersecurity Audit Team

- Formed in fall of 2017
- Cybersecurity-focused
- Systemwide internal audit resource - All UC Health and UC campuses
  - Support UC location internal audit offices
  - Perform cyber-risk focused audits across UC system

Third line of defense in cybersecurity



BOARD OF REGENTS

SENIOR LEADERSHIP

1

Management Controls in Business Units

2

Information Security

Compliance

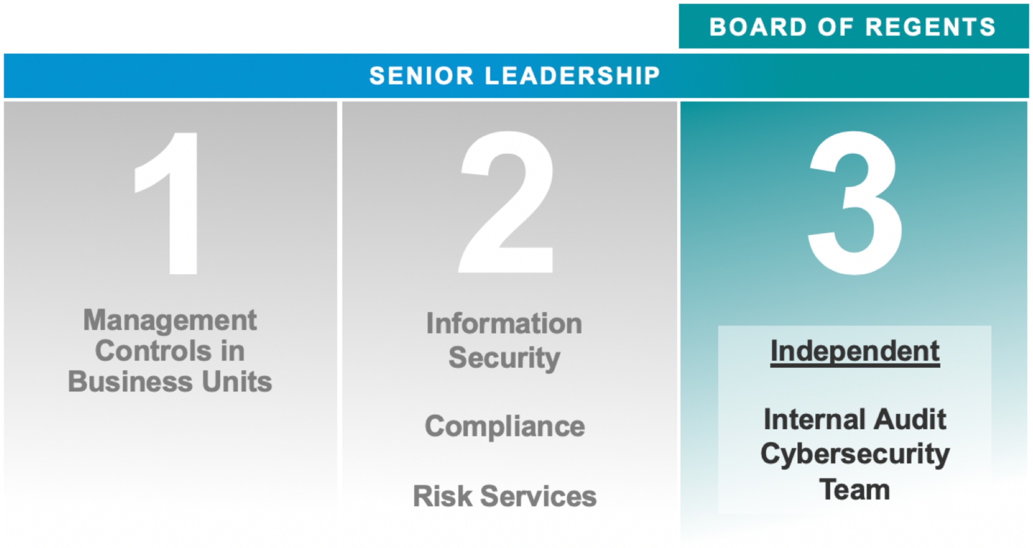
Risk Services

3

Independent

Internal Audit Cybersecurity Team

Third line of defense in cybersecurity



BOARD OF REGENTS

SENIOR LEADERSHIP

1

Management Controls in Business Units

2

Information Security

Compliance

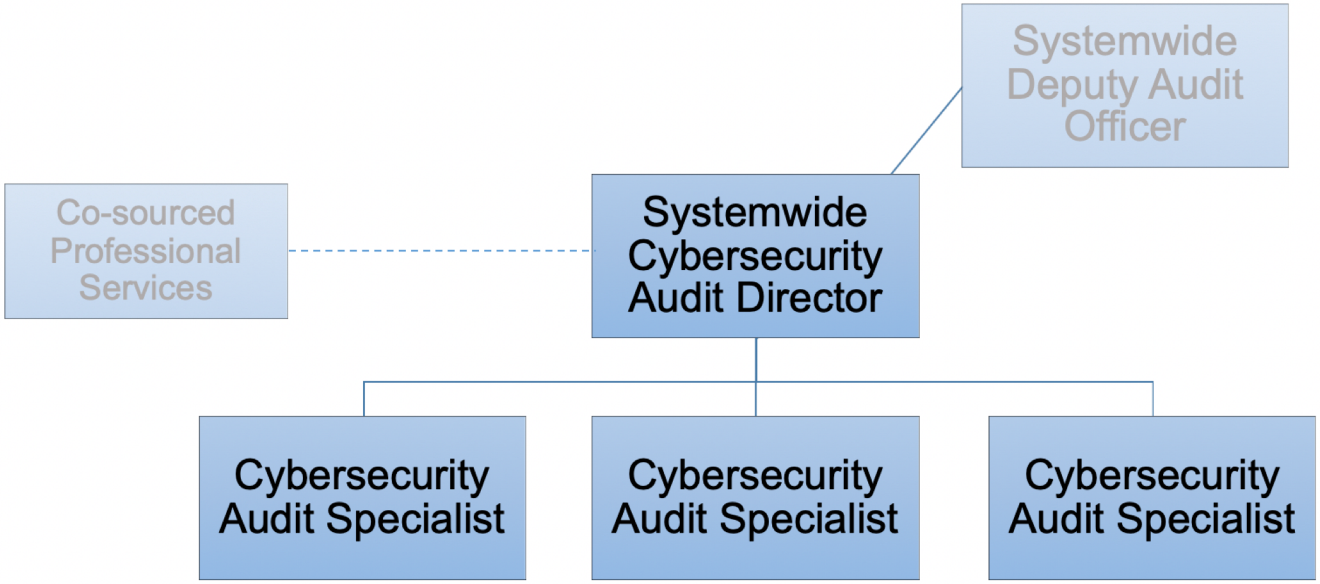
Risk Services

3

Independent

Internal Audit Cybersecurity Team

CAT Structure



Systemwide Deputy Audit Officer

Co-sourced Professional Services

Systemwide Cybersecurity Audit Director

Cybersecurity Audit Specialist

Cybersecurity Audit Specialist

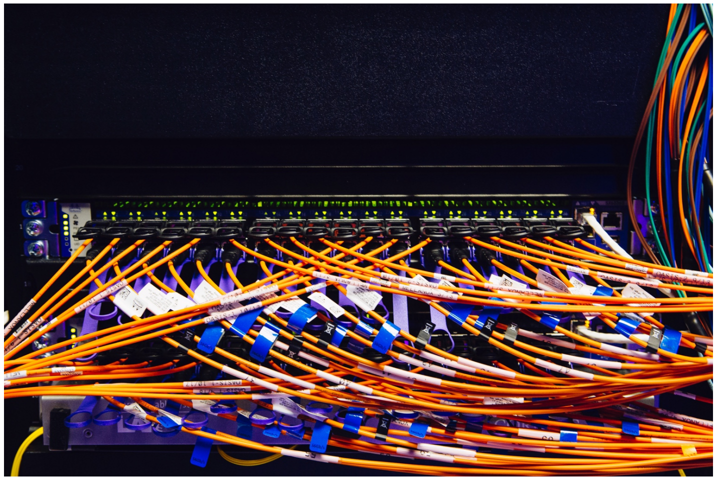
Cybersecurity Audit Specialist

CAT Structure

- Cybersecurity Audit Specialists
  - Backgrounds in IT and cybersecurity
  - Internal audit experience
  - Regular professional development opportunities

- Co-sourced professional services
  - Specialized skills
    - Penetration testing analysts

  - Staffing augmentation
    - Recruitment challenges



Federal and Industry Partnerships

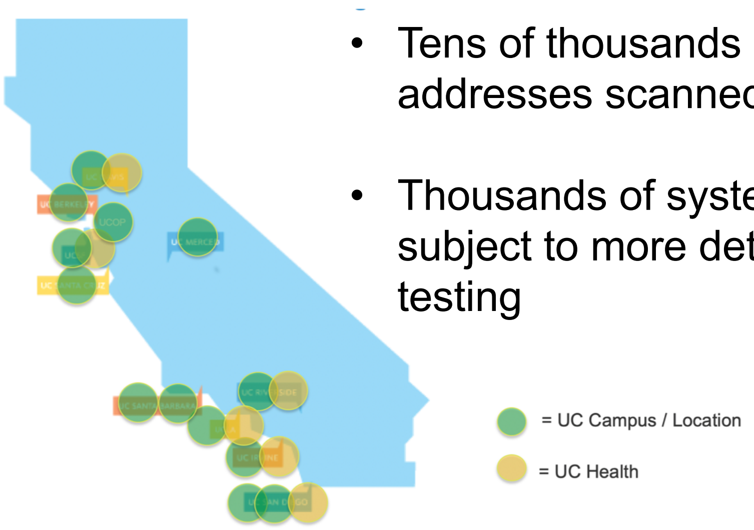
- Federal partners
  - Briefings
  - Collaboration

- National Guard

- Industry Partnerships
  - Industry expertise
  - Specialized skills

Penetration Testing Audits

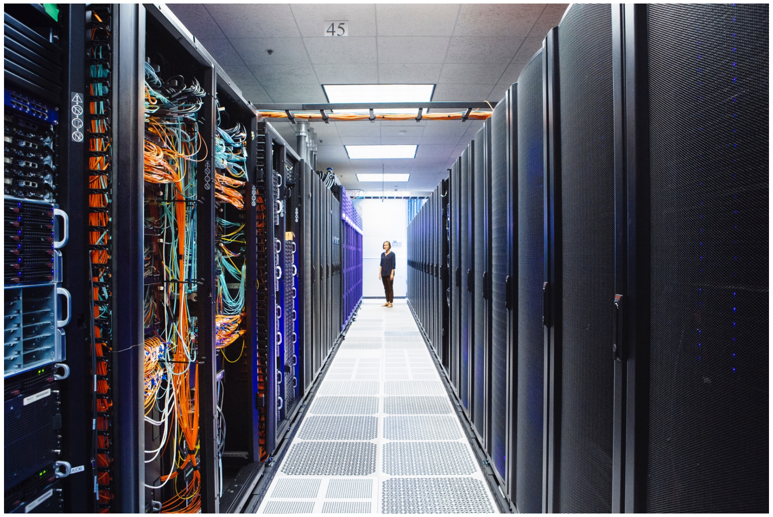
- Coverage:
  - All UC Campuses
  - All UC Health Locations
  - UCOP
  - Other small units



- Tens of thousands of addresses scanned
- Thousands of systems subject to more detailed testing

Penetration Testing Audits

- Work closely with risk partners in cybersecurity:
  - Cyber-Risk Responsible Executives (CRE)
  - Chief Information Officers (CIO)
  - Chief Information Security Officers (CISO)
  - Unit leadership
- Work with professional services firm for penetration testing analysts
- Three years – Scope targets high risk areas across all of UC

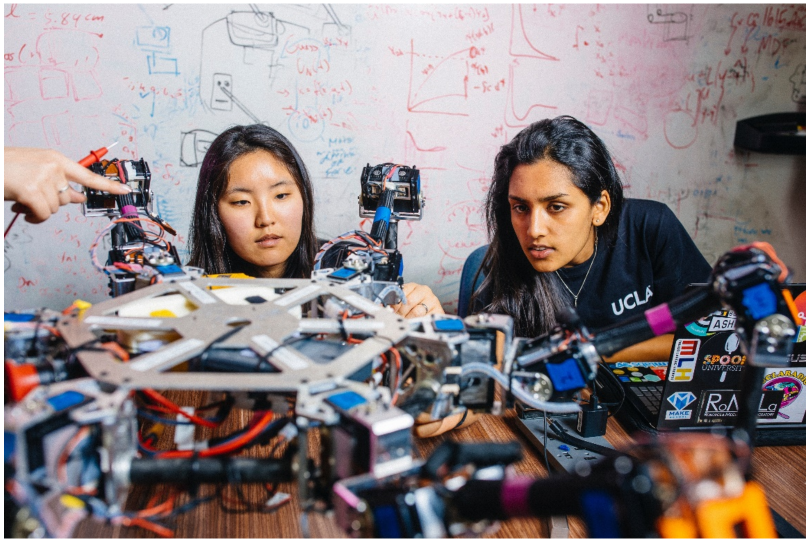


Penetration Testing Audits

- Objectives:
  - Identifying weaknesses in high risks systems for improvement
  - Evaluating the overall vulnerability management programs across high risk areas of UC and make improvements as necessary
- Scope:
  - 1000/1000 internal and external IP addresses scanned
  - 100/50 internal and external IP addresses selected for more detailed penetration testing
  - 2 web application penetration tests

Penetration Testing Audits

- Management corrective actions – Closure criteria:
  - Address the vulnerabilities identified
    - Remediation
    - Mitigation/compensating controls
    - Risk acceptance
  - Improvement to vulnerability management program
    - Consistent/periodic scanning
    - Tracking of vulnerabilities
    - Management reporting – Oversight and accountability



Current Projects

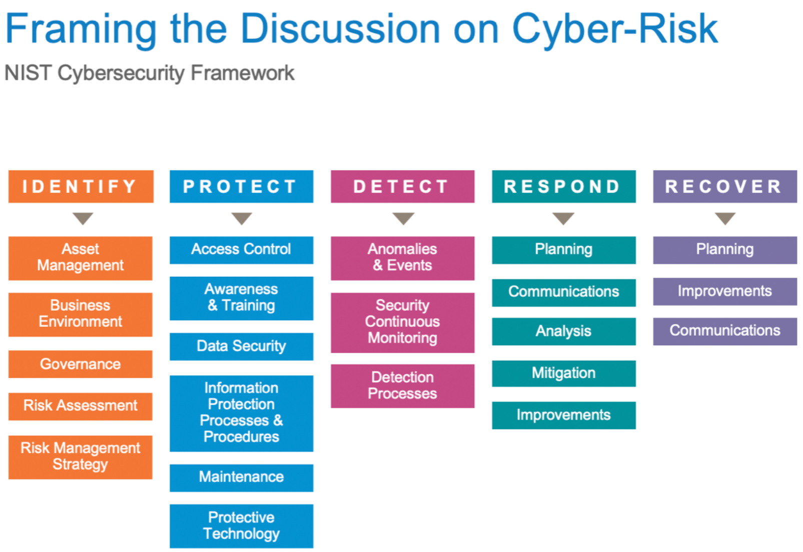
- Systemwide Audit of Implementation of Threat Detection and Information
- Systemwide Vulnerability Assessment and Penetration Testing – Research Focus
- UC Path Cybersecurity
- UC Health Data Warehouse

Engaging the Board

- Compliance and Audit Committee Briefings
  - Results from audits and management's actions
  - Emerging risk areas
  - Federal and industry partnerships
  - Education on cyber-risk frameworks and how we can use them in communicating our results
  - Supporting the board's oversight role for cyber-risk

NIST Cybersecurity Framework

- Federal government and widely adopted industry framework for addressing cybersecurity
  - Used by UC operations
  - Leveraged in our audits to communicate results
  - Common language
  - 5 Functions
    - 23 Categories



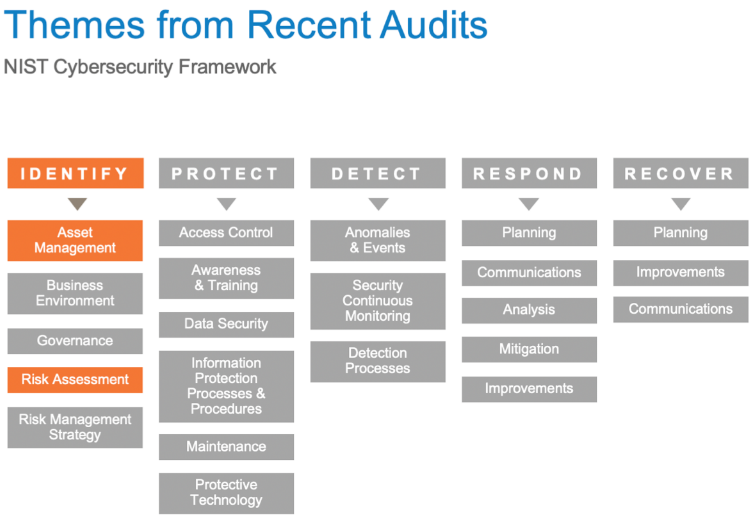
Framing the Discussion on Cyber-Risk

NIST Cybersecurity Framework

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Asset Management	Access Control	Anomalies & Events	Planning	Planning
Business Environment	Awareness & Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Information Protection Processes & Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

NIST Cybersecurity Framework

- Communicating audit results
- Identifying themes across projects



Themes from Recent Audits

NIST Cybersecurity Framework

IDENTIFY
- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy

PROTECT
- Access Control
- Awareness & Training
- Data Security
- Information Protection Processes & Procedures
- Maintenance
- Protective Technology

DETECT
- Anomalies & Events
- Security Continuous Monitoring
- Detection Processes

RESPOND
- Planning
- Communications
- Analysis
- Mitigation
- Improvements

RECOVER
- Planning
- Improvements
- Communications