CYBERSECURITY BOULEVARD – WHERE RISK, INFORMATION TECHNOLOGY, GENERAL COUNSEL, PRIVACY, AND COMPLIANCE MUST MEET AND NOT COLLIDE!

Cheryl Lloyd
Associate Vice President &
Chief Risk Officer

Tom Andriola
Vice President &
Chief Risk Information Officer

University of California
UC Overview

What is the cyber footprint?
### INFLUENTIAL SCALE

<table>
<thead>
<tr>
<th>Category</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Campuses</td>
<td>10</td>
</tr>
<tr>
<td>Medical Centers</td>
<td>5</td>
</tr>
<tr>
<td>National Laboratories</td>
<td>3</td>
</tr>
<tr>
<td>FTE Students</td>
<td>252,000</td>
</tr>
<tr>
<td>Full-time Faculty and Staff</td>
<td>146,000</td>
</tr>
<tr>
<td>Living Alumni</td>
<td>1,700,000</td>
</tr>
</tbody>
</table>

### 5 ACADEMIC MEDICAL CENTERS

<table>
<thead>
<tr>
<th>Category</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Licensed Beds</td>
<td>3,666</td>
</tr>
<tr>
<td>Outpatient Clinic Visits Annually</td>
<td>4,500,000</td>
</tr>
<tr>
<td>Inpatient Days Annually</td>
<td>972,000</td>
</tr>
<tr>
<td>Major trauma centers</td>
<td>5</td>
</tr>
</tbody>
</table>

### HONORS & AWARDS

<table>
<thead>
<tr>
<th>Category</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nobel Prizes – most of any public university</td>
<td>61</td>
</tr>
<tr>
<td>National Medals of Science</td>
<td>67</td>
</tr>
<tr>
<td>MacArthur Fellows</td>
<td>85</td>
</tr>
<tr>
<td>Fulbright Award Recipients</td>
<td>264</td>
</tr>
<tr>
<td>Pulitzer Prize Winners</td>
<td>16</td>
</tr>
</tbody>
</table>

### STRONG GOVERNANCE AND INDEPENDENCE FROM THE STATE

President Janet Napolitano directly oversees the 10 campus chancellors and the director of the Lawrence Berkeley National Lab.

UC remains constitutionally autonomous and is governed by a 26-member Board of Regents.

---

2. UC operates and manages Lawrence Berkeley National Laboratory under a contract directly with the Department of Energy (DOE). The University is a member in two separate joint ventures that operate and manage two other DOE laboratories, Los Alamos National Laboratory and Lawrence Livermore National Laboratory.
3. As of October 31, 2015
UC IS COMMITTED TO ITS THREE PILLARS OF EXCELLENCE

Quality
 UC provides top quality instruction to students at all levels and conducts research with some of the world’s brightest minds

Access
 UC is committed to enrolling a diverse student body and supporting access for students from low-income families

Affordability
 UC seeks to ensure that finances are not an obstacle to qualifying students through a generous, progressive financial aid program
UC IS ONE OF THE LEADING ACADEMIC RESEARCH ENTERPRISES GLOBALLY

- UC produces 8% of the nation’s PhDs (4,000 degrees), more than any other university system.¹
- UC performs nearly one-tenth of all academic research and development in the United States.² Research expenditures average over $4.3 B annually, demonstrating UC’s continued importance as a source of innovation and economic growth.³

1. Source: UC Graduate Research Fact Sheet (April, 2015)
3. Over the last 5 years (FY 2010-11 through FY2014-15), adjusted for inflation. Source: UC Information Center
CYBERSECURITY
The challenge: Securing an open environment
THE AWAKENING

- In 2015, UC (like many other organizations) was targeted by hackers
- The challenge/opportunity: developing a comprehensive plan to detect and report intrusions and taking a systemwide view of our cyber profile
- President Napolitano put into place a new security plan
PRESIDENT’S CYBERSECURITY PLAN

- Governance
- Enhanced risk management
- Modern technology
- Security environment
- Systemwide culture change
GOVERNANCE

- Responsible Cyber Executive at each location – reports to Chancellor
- Cyber Risk Governance Committee
- Cyber Risk Advisory Board
GOVERNANCE STRUCTURE

UC Cyber-Risk Governance Structure

Board of Regents

Office of the President

Council of Chancellors (COC)

Cyber-Risk Governance Committee (CRGC)

Academic Computing Committee (UCACC)

Cyber Coordination Center (CCC)

Cyber-Risk Advisory Board

* 6 members – 3 internal, 3 external
* Meet with CREs 2 times per year

Cyber Risk Executives (CRE)
* 10 locations + ANR + Lab Mgmt. + OP functions
* Up to 3 Academic Senate Reps (chosen by Senate)

CRGC Meetings
* Meet as a group four times per year

Faculty Members

UCOP Staff
ENHANCED RISK MANAGEMENT

- Utilize National Institute of Standards and Technology (NIST) cybersecurity framework as risk management standard
- Comprehensive risk assessments at all locations
- Senior management/executive reporting
MODERN TECHNOLOGY

- Enhance/support capabilities to identify, protect, detect, respond and recover
- Governance and Advisory Committee oversight and direction
- Create consistency and leverage investments
SECURITY ENVIRONMENT

- Cyber Risk Coordination Center – Office of the President
- 24/7 threat monitoring
- Systemwide dashboards
- Intercampus knowledge sharing/transfer
SYSTEMWIDE CULTURE CHANGE

- Mandatory training for all employees
- Systemwide escalation protocols
- Cybersecurity Summit—February 2016
- Engaging and educating students
- Communication and awareness programs
INSURING CYBERSECURITY

Where to begin?
HISTORICAL PERSPECTIVE

- UC presents a complex risk exposure to the insurance market
- First attempts to purchase insurance presented challenges
- To access the market, UC adopted the “reverse underwriting” approach
  - Underwrite standard vs. actual conditions
  - Conditions Precedent
- Continuously worked with market
  - Gradually increased limits
  - Altered Conditions Precedent to a standards-based and more favorable approach
- New policy
  - No Conditions Precedent
  - Increased limits
HISTORICAL PERSPECTIVE – INSURANCE LIMITS 2010-2017

Conditions Precedent

No Conditions Precedent

- 2010-11: $2M
- 2011-12: $10M
- 2012-13: $20M
- 2013-14: $20M
- 2014-15: $45M
- 2015-16: $40M
- 2016-17: $80M
HOW WE GOT FROM THERE TO HERE

- Risk had a good story to tell
- Underwriters recognize systemwide efforts and changes post UCLA
  - Elevation of cyber risk – Cyber Risk Responsible Executive (CRE) and Cyber-Risk Governance Committee (CRCG) model
  - Adoption of National Institute of Standards and Technology (NIST) Cybersecurity Framework as risk management standard
  - Mandatory training – receiving a credit for training
  - Escalation process
  - Investment in technology – Fidelis and Fire Eye
  - Risk assessments
- Info provided by Chief Information Security Officers (CISOs)
- UC is taking a larger portion of the risk
- Relationship with the market
QUESTIONS?

Discussion