UCLA Campus
Cybersecurity Plans

UCLA Board on Privacy and Data Protection
March 30, 2016
UCLA Cybersecurity

- Program Objectives and Initiatives
- Multi-Factor Authentication (MFA)
- Threat Detection and Identification (TDI) –
The complex, constantly changing cybersecurity landscape is a serious challenge ...

### Unique Challenges of Higher Education

- A data-rich “soft target” (e.g., research, intellectual property, personally identifiable information (PII), protected health information (PHI), etc.)
- Open by design with a focus on global collaboration, academic freedom, privacy, and transparency
- Constantly changing users (e.g. new students) and a large number of devices with significant amounts of data
- Highly decentralized (hundreds of autonomous units) and few enforcement mechanisms
- One of the most heavily regulated industries in the U.S.
- Low level of Information Security awareness and literacy generally

### Education Breaches Cost More

**Breach Cost per Capita*, 2014**

- **Direct Costs**:
  - $294
- **Indirect Costs**:
  - $197
  - $97
  - $201

**Source**: The Advisory Board, 2015
... and addressing this challenge will involve change

• UCOP cybersecurity mandates
• UC Cybersecurity Risk Governance (CRE)
• Coordinated UCLA Campus and Health System governance
• Campus-wide information security risk assessment and risk management plan
• Minimum security standards and a modified approach to ensure compliance
• New and expanded scope of security solutions, services, and support for the campus
• Changes in how we architect, manage, and protect the campus network and IT infrastructure
• Increased emphasis on cybersecurity awareness, compliance and accountability
Enhanced Cybersecurity Program

**Goal – Upgrade our cybersecurity strategy and improve our ability to identify, protect, detect, respond, and recover from cybersecurity threats**

- Improve information security governance, funding, and our ability to plan for the future
- Coordinate security activities across UCOP, Health System, campus, and campus units
- Ensure prevention controls are differentiated and appropriately matched to our research, academic and administrative needs
- Evolve our security practices to address emerging complexities (e.g., mobile, social media, cloud adoption, process digitization, big data, internet of things, changing regulatory landscape, etc.)
- Mitigate risks, reduce incidents, and avoid breach associated costs; optimizing security investments across campus organizational units in a cost-effective way

**Plan – Programmatically improve security practices and deploy advanced cybersecurity technologies**

- Expand the scope of security services and support that are available to the campus
- Improve the maturity of our security processes and practices
- Provide the expertise and skills necessary to support a next-generation security strategy
- Update the sophistication of our security tools and technologies
- Redefine and enhance our relationship with campus stakeholders and collaboration with departmental IT staff
- Promote measured but effective spend for long-term continuous improvement
UCLA Program Initiatives

Immediate / Near Term

• Remediation of known vulnerabilities (web sites, applications, data stores, and IT infrastructure) - Campus
• Information security risk assessment (ISRA) and risk management – Campus
• Multi-factor authentication (MFA) - Campus
• Dedicated HIPAA data environment and research infrastructure – Campus and IDRE / SOM
• Threat detection and identification (TDI) – Campus and Health System
• Next generation firewalls (NGFW) and privileged access management (PAM) – Data Center
• Cybersecurity awareness and training – Campus Staff, Faculty, and Students

Longer Term

• IT security reference architecture and minimum standards
• Vulnerability scanning, penetration testing, patch management, and system hardening improvements
• Encryption enhancements (laptops, disk drives, and mobile devices)
• Advanced endpoint protection and policy enforcement
• Automated data discovery / classification and data loss prevention (DLP)
• Website monitoring and web application firewalls (WAF)
Multi-Factor Authentication (MFA)

- MFA is authentication requiring more than one type of assurance
- Common assurance factors:
  - Something you know, e.g., password
  - Something you have, e.g., smart card, cell phone, token
  - Something you are, e.g., biometric such as fingerprint
About the UCLA MFA Project

- Mitigates risk associated with weak passwords, compromised credentials / accounts, and phishing attacks
- Managed by the IT Security Office with multi-pronged / phased deployment

<table>
<thead>
<tr>
<th>UCLA Logon</th>
<th>Campus at Large</th>
<th>IT Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Shibboleth</td>
<td>• Interested campus department with local account space</td>
<td>• IT Services VPN</td>
</tr>
<tr>
<td>(Sensitive -&gt; All Applications)</td>
<td>• Active Directory, local systems, etc.</td>
<td>• Application Development and Management Tools</td>
</tr>
<tr>
<td>• Campus VPN</td>
<td>• Integration with Health Systems Active Directory</td>
<td>• Privileged Access Management</td>
</tr>
<tr>
<td>• Campus Wi-Fi</td>
<td></td>
<td>• Data Center</td>
</tr>
<tr>
<td>(UCLA Wi-Fi and eduroam)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

GOAL: All employee access through UCLA Logon will require MFA
Duo Security Enterprise

(Partner with InCommon and Internet2)

• Allows both user pre-registration and Just In Time (JIT) account and device registration

• Support for Smart Phone Apps (iOS and Android), SMS and Voice (at cost), and hardware tokens
As Simple as 1... 2... 3
### Who Uses MFA with UCLA Logon?

<table>
<thead>
<tr>
<th>Proposed</th>
<th>Phase I May 2016</th>
<th>Phase II Fall 2016</th>
<th>Phase III Spring 2017</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Users with Sensitive Access</strong></td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
</tr>
<tr>
<td><strong>Employee</strong> (UCLA faculty and staff)</td>
<td>Opt-In</td>
<td>Opt-In</td>
<td>Required</td>
</tr>
<tr>
<td><strong>Student</strong> (currently enrolled student)</td>
<td>Opt-In</td>
<td>Opt-In</td>
<td>Opt-Out</td>
</tr>
<tr>
<td><strong>Affiliate</strong> (parents, contractors, etc.)</td>
<td>Opt-In</td>
<td>Opt-In</td>
<td>Opt-Out</td>
</tr>
</tbody>
</table>

*Proposed Future State: MFA will generally be required (phased deployment) for UCLA Logon with (limited / TBD) Opt-Out exceptions*
Threat Detection and Identification (TDI)

Fidelis

• UCOP is rebooting the Fidelis systemwide threat detection services that were implemented after the UCLA Health cyberattack
• The scope of Fidelis network monitoring has been adjusted from the specific UCLA Health attack pattern to the analysis of “network traffic at UC for potentially malicious or unauthorized activity, including malware signatures and network anomalies”
• Privacy protections that Fidelis has agreed to:
  ▪ Adhere to the UC Electronic Communications Policy (ECP)
  ▪ Limit processing or observing of content to “least invasive” and “least perusal”
  ▪ Follow agreed “implementation procedures” and train their employees / subcontractors on those procedures
  ▪ Avoid analysis or reporting of network activity for an individual user except as a last resort

• Objective is to be able to correlate activity, alert, and report trends across seventeen sites
• Fidelis gear at each location will store network meta-data for a limited period
• If there is an indicator of compromise (IOC), short intervals of packets are captured before and after the alert to support investigation
• Inbound and Outbound email is not specifically monitored
• Fidelis master command post can view data and an analyst will monitor UC activity 16 hours / day x 365 days / year
• Fidelis will be looking for ”high-value” activity and provide real-time alerts but no blocking (i.e., monitoring device is passive)
• Fidelis services are temporary until campuses are ready to move to a permanent solution (i.e., FireEye)
FireEye (preliminary)

- FireEye provides broader and more integrated capabilities for attack detection and response
  [https://www.fireeye.com/](https://www.fireeye.com/)
- The FireEye systemwide TDI baseline includes:
  - Network Security (NX) to detect known and unknown attacks and prioritize alert response
  - Dynamic Threat Intelligence (DTI) subscription to a global cloud network for advanced threat detection and prevention
  - Threat Analytics Platform (TAP) to combine location event monitoring with FireEye threat intelligence
  - FireEye as a Service (FaaS) for around-the-clock Security Operations Center (SOC) monitoring and investigation

---

- Campus will / may add additional solutions for:
  - Cloud Email Threat Prevention (ETPC) for O365
  - Endpoint Threat Prevention (HX) for data center and other high-value / high-risk endpoints
  - Network Forensics (PX) for network event capture and investigation
  - Central Management (CM) to consolidate management of FireEye and other security solutions

- We will work with the Campus Information Security Coordinators (ITCC) / CSG regarding technical review
- We will work with the UCLA Privacy Board, IT Planning Board (ITPB), and the Academic Senate to assess alignment with UC Privacy Principles and the UC Electronic Communications Policy (ECP)
Threat Detection and Identification (TDI)

FireEye

- UCOP’s response to privacy concerns and questions [http://security.ucop.edu/index.html](http://security.ucop.edu/index.html)
- Location TDI baseline is mandatory and the costs will be covered by the system
- The Fidelis statement of work (SOW) has been reviewed with the UC Academic Senate and adheres to the UC Electronic Communications Policy (ECP) requirements
- The FireEye Agreement and baseline statement of work (SOW) are also being reviewed with the UC Academic Senate
- Information has been / is being provided to the CREs, CIOs, and CISOs; UCOP is not planning any additional communication

UCLA Deployment of FireEye

A task force be created to review the FireEye components that will be deployed, how they work, what data is collected / stored / retained, how various components are accessed and managed by whom, what oversite and controls will be in place to ensure alignment with Privacy Principles and ECP

- Privacy Board – Dana Cuff and Christine Borgman
- ITPB – John Mamer and Kathleen Bawn
- Academic Senate – Leo Estrada and Susan Cochran
- Administration – Andrew Wissmiller and Kent Wada