Introductions
Leo Howell, CISSP CISA

Professional

- **Mission**: empower the good guys, stop the bad guys
- **Security approach**: build secure things and secure things
- **Experience**: formerly AD of Internal Audit; formerly technical

Personal - proud husband and dad!

NC State by the Numbers

- R1, Land Grant
- $1.5B budget
- 34,000 students
- 9,000 faculty & staff
- $6.5B State economic impact; ~90K jobs
- Distributed IT
- Value public/private partnerships
Javier Torner, Ph.D.

Javier Torner is the Information Security Officer at California State University San Bernardino and director of the Information Security and Emerging Technology Office.

Javier coordinates and oversees the implementation of enterprise information security initiatives for the university’s information systems, including the development and adoption of information security policies and standards.

The information Security and Emerging Technologies Office provides among others support to university entities in conducting risk and vulnerability assessments for information assets, manages the intrusion detection and incident response, conducts digital forensic investigations, and manages the information security compliance program for the campus.

Javier has a CISM, CGEIT, and CRISC professional certifications from ISACA and is currently the President for the Information System Security Association Inland Empire Chapter. Javier is a Professor of Physics with over thirty years of teaching and working experience with data communication networks and computer systems.
Digital Capabilities in Higher Education

WICKED PROBLEMS

Deliberately un-deliberate

a meditation on methods

Unlike others

seek something really new

like solutions, not problems

complex, ambiguous

definition, itself is wicked problem

Can’t write a check

2. IDEO

20% evaluation

New facts, new people

Idea, concept, design thinking

WICKED PROBLEMS

Closed mode

Time bound

Stressed

Open mode

Relaxed

Curious

Why all same?

In constraint - we do what we know

Efficiency 

In box idea

1. EXERCISE

Draw a sound so sec.

John cheese creativity

Malcolm Brown EU

EDUCUSE LEARNING INITIATIVE

500 years
Digital Capabilities for Higher Education

<table>
<thead>
<tr>
<th>Research</th>
<th>E-learning</th>
<th>Student success</th>
<th>Culture of innovation</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT risk management</td>
<td>IT governance</td>
<td>Analytics</td>
<td>Information security</td>
</tr>
</tbody>
</table>

Mission differentiating capabilities

IT management capabilities

Foundational IT capabilities

http://er.educause.edu/articles/2016/12/the-digitization-of-higher-education-charting-the-course
The diagram illustrates the various dimensions of IT capabilities, including Research computing, E-learning, Student success, and Culture of innovation. Each dimension is further divided into subcategories, such as Leadership, Information security, and Mission differentiating capabilities. The diagram visually represents the correlations and dependencies among these different aspects, emphasizing the interconnectedness of IT management and how they collectively contribute to overall institutional success.
Digital Capabilities for Higher Education

http://er.educause.edu/articles/2016/12/the-digitization-of-higher-education-charting-the-course

http://er.educause.edu/articles/2015/11/2015-EDUCAUSE-Core-Data-Service
Tools for Better Decision Making

Campus leaders use EDUCAUSE assessment and benchmarking services to plan for and manage IT service delivery, financials, security and risk, technology-supported learning, and digital initiatives.

EDUCAUSE SERVICES

**ASSESSMENT**
- Learning Space Rating System
  - Measure how classroom design supports and enables active learning.
- Information Security Program Assessment Tool
  - Evaluate the maturity of your information security program.
- IT Risk Register
  - Identify common risks to support your strategic IT risk-management program.

**BENCHMARKING**
- Technology Research in the Academic Community
  - Track student and faculty technology needs and experiences.
- Core Data Service
  - Compare peer and aspirant data for IT financials, staffing, and services.
- Benchmarking Service
  - Measure technical and cultural capability for digital initiatives like student success.

Digital Capabilities for Higher Education

- Research
- E-learning
- Student success
- Culture of innovation

- IT governance, risk, and compliance
- IT risk management
- IT governance

- IT workforce
- IT agility
- IT service management

- Analytics
- Information security

Mission differentiating capabilities
IT management capabilities
Foundational IT capabilities
Information Security Maturity
(All Non-specialized US Institutions)

- Identity management: 3.0
- Business continuity: 2.8
- Policies: 3.3
- Systems review: 3.1
- Security services and operations: 3.4
- Asset protection: 3.8

Composite: 3.2

2016 EDUCAUSE Core Data Service

Information Security Maturity Index

www.educause.edu/benchmarking
Information Security Maturity
(All Non-specialized US Institutions)

- Identity management: 3.0
- Business continuity: 2.8
- Policies: 3.3
- Systems review: 3.1
- Security services and operations: 3.4
- Asset protection: 3.8

Policies

- Encryption policies: 3.8
- Identify critical assets: 3.7
- Electronic record life cycle: 3.6
- Cyberliability insurance: 3.5
- Mobile computing guidance: 3.4
- Sensitive data standards: 3.4
- Paper record life cycle: 3.0
- Classify data: 2.7

Categories:
5. Optimized
4. Established
3. Developing
2. Initial
1. Absent
Why keep it simple...

- Complicated beginnings
- Room for down-size
- Duplicate people
- Lots of meetings
- Slow Policy rollout
- Conflicts of opinions
- Professional objectors

Policy
- Broad principles
- University-wide
- Board of Trustee approval

Regulations
- General procedures
- Mostly university-wide
- Executive approval

Rules
- Detailed standards & procedures
- University- or division-wide
- Vice chancellor approval
Recent Changes in Policy & Governance Framework

**Rules**
- Approved by CIO
- Resembles standards
- Accompanying guidelines
- Increased agility

**Governance Framework**
- Undergoing simplification and right-sizing
- Dozens of repeals and consolidation
- Strategic shift toward unified compliance (IT)

---

Adoption... *It’s not about IT, it’s about leadership*

**Development approach**
- Drafted by Security team
- Reviewed by initial small group of SMEs
- Reviewed by OIT leaders

**Approvals**
- Reviewed by multiple governance groups
- Endorsed by top level governance
- Reviewed by IT Leadership Committee (CIO, CFO, Provost)
- Approved by CIO, Executive Committee, or Board of Trustees

**Leadership challenge**
- New requirements adds burden to overworked personnel
- Shift ownership to business leaders
  - Data Trustees
  - Data Stewards
  - Data Custodians
- Co-develop requirements with disparate players
### Major Policies, Regulations, Rules

<table>
<thead>
<tr>
<th>Policies &amp; Regulations</th>
<th>In the Works</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Computer Use Policy</td>
<td>• Incident Response Procedure</td>
</tr>
<tr>
<td>• Computer Use Regulation</td>
<td>• Endpoint Security Standard</td>
</tr>
<tr>
<td>• Data Management Procedures</td>
<td>• Secure Software Development Standard</td>
</tr>
<tr>
<td></td>
<td>• Vulnerability Scanning Standard</td>
</tr>
<tr>
<td></td>
<td>• Electronic Signature Standard</td>
</tr>
<tr>
<td>Rules (Standards)</td>
<td></td>
</tr>
<tr>
<td>• Network Printer Security</td>
<td></td>
</tr>
<tr>
<td>Standard</td>
<td></td>
</tr>
<tr>
<td>• System and Software Patching</td>
<td></td>
</tr>
<tr>
<td>Standard</td>
<td></td>
</tr>
<tr>
<td>• Security Standard for Sensitive</td>
<td></td>
</tr>
<tr>
<td>Systems and Data</td>
<td></td>
</tr>
<tr>
<td>• Password Security Standard</td>
<td></td>
</tr>
</tbody>
</table>

### Lessons Learned & Recommendations

- Think leadership
- Think “unified compliance”
- Policies and standards should not just document current state
- Co-develop with disparate players
- Engage the true owners (business leaders)
- Remove red tape to increase agility and flexibility
- Endpoint protection is a hot button issue
Information Security Policies and Standards

• CSU Information Security Policies and Standards
  – Based mainly on ISO-27001 and ISO-27002:2013
  – CSU Standards provide campuses flexibility for implementation
  – Information security policies and standards are developed by a system wide advisory committee of ISO’s
  – Currently 27 policies!

Information Security Policies and Standards

• CSU San Bernardino
  – established an IT Governance structure
  – standards are developed and review by a university subcommittee (currently 18 standards!)
  – standards are aligned with CSU standards
  – Standards are implemented through the adoption of processes and procedures
  – Metrics on processes are used to track adherence to standards
Continuous Assessment and Monitoring Program

- Program objectives:
  - to assess the maturity of the campus information security program
    - Maturity can only be assessed once processes are incorporated across campus entities
  - to monitor adherence to campus standards
    - Information security standards are implemented through the adoption of processes and procedures
    - Relevant benchmarks and metrics (quantitative) are selected and tracked on university information security processes
Continuous Assessment and Monitoring Program

• Operational standards (quantitative metrics!)
  – Access Control Standards
  – Network Security Management Standards
  – Vulnerability Management Standards
    – Patch Management
    – Server vulnerability
  – Log Management Standard
  – more in progress..

Discussion Questions: Policy Adoption

- What is the **obstacle** keeping you from the next maturity level for this dimension?

- Besides time or money, what can help overcome the obstacles? Where you have had **success** in this dimension? What were the keys to that success? What helped you get there?
15 minute break

Information Security Maturity
(All Non-specialized US Institutions)

- Identity management: 3.0
- Business continuity: 2.8
- Security services and operations: 3.4
- Asset protection: 3.8
- Policies: 3.3
- Systems review: 3.1

2016 EDUCAUSE Core Data Service
Identity Management

- Multifactor authentication: 3.3
- Identity mgmt. policy: 2.9
- Eduroam network access: 2.8
- Risk assessment: 2.7

2000 - 2010: Innovation & DIY
- Multiple Active Directories
- Kerberos, LDAP authN
- Manual and Semi-automated provisioning and deprovisioning
- Ad hoc governance, lack of policies, strategic direction
- Search for enlightenment

2005 - 2015 Automation & Adoption
- Sun Identity Manager (Customized)
- Official University Active Directory
- BPA, requirements documentation
- Shibboleth, Incommon, local federations

2010 - 2020 Integration, Security & Compliance, Phase I
- Emerging governance with functional and service owners
- Oracle Identity Manager Implementation
- Emergence of IAM as key component of security compliance

2010 - 2020 Integration, Security & Compliance, Phase II
- Grouping and role-base mgmt
- “Guest & Affiliate” mgmt
- AuthN, AuthZ and certification mgmt

NC STATE

IdM Long-Game
Oracle Identity Manager Rollout
- Official System of Record for Identity Data
- Replace existing home-grown solution
- Active Directory & LDAP Integration
- ERP Integration
- Self-service password resets
- Semi-provisioning/deprovisioning for AD, Kerberos, Google

Related “Nearby” Initiatives
- Cybersecurity Strategic Plan/Roadmap
- 2FA Authentication rollout for employees
- NIST 800-171, PCI DSS, HIPAA, GLBA
- Electronic Research Administration (eRA) system

Expected Outcomes

Key Activities
- Nightly data in-feeds
- Self-service password resets
- Nightly data out-feeds
- Password change synchronization
- Monitoring
Lessons Learned

- Business Process Analysis and Defined Requirements are critical
- Succession Planning key component of strategy
- Governance with empowered functional and service owners
- Data integration management
- Partnership trumps going it alone
- Project management & continuous cost-benefit management
- It’s a long-game, strategize accordingly

CSUSB Identity Management Program

- Beginning of the Century Challenges
  - Many domains, user accounts and “password standards”
  - Inconsistent provisioning of services – email, administrative accounts, computer labs, etc
  - No mechanism for de-provisioning
  - Decentralized IT - Security chaos!!
CSUSB Identity Management Program

• Started in 2004
  – Strategic direction - create identity group and consolidate to Single Sign On
• 2006 - First IdMS deployed on campus
  – Conducted first Identity and Access Management campus assessment
  – Implemented provisioning of email, wireless, campus AD, OpenLDAP
• 2007 - Deployed CAS/Shib
  – Campus standard for all Web applications authentication
• 2009 - Join InCommon Federation
• 2014 - Established a new IT Governance

CSUSB Identity Management Program

• Fall 2016
  – Student population: 20,767 (FTES 18,070)
  – Active accounts
    • Faculty/Auxiliaries/Staff: 2515
    • Students 65,353
    • Affiliates: 340
  – Email
    • Students – Gmail
    • Employees – Microsoft Office365
  – Campus portal + over 15 SSO applications
CSUSB Identity Management Program

- Identity Management system
  - Sun Systems - Production 2006
    - Provisioning and self-service
  - Migrated to Aegis -2014
    - Provisioning, deprovisioning, improved self-service
  - Authentication Systems
    - Microsoft AD and ADFS
    - CAS/Shib - OpenLDAP
      - Migrated Production to AWS - Summer 2015
      - Backup system - on campus
    - Implemented MFA (DUO) on CAS - Summer-2016
      - Critical System - System Administrators, IT staff, HIPAA, PCI, etc
      - Security Administrators/ Employees with access to Level 1 - in progress

California State University, San Bernardino
CSUSB Identity Management Program

- ONE Authoritative Source of Identity Information: ERP (CMS PeopleSoft)
- IdMS Provide provisioning, de-provisioning and authentication services
- Some metrics:
  - Time for provisioning of account and services: 24 hours
  - Time for de-activation of account: 24 hours
  - Time for De-provisioning of services
    • varies depending on affiliation - work in progress

Discussion Questions: Identity Management

- What is the obstacle keeping you from the next maturity level for this dimension?

- Besides time or money, what can help overcome the obstacles? Where you have had success in this dimension? What were the keys to that success? What helped you get there?
Information Security Maturity
(All Non-specialized US Institutions)

1. Absent
2. Initial
3. Developing
4. Established
5. Optimized

Business continuity
3.2

Identity management
3.0

Security services and operations
3.4

Asset protection
3.8

Policies
3.3

Systems review
3.1

Business Continuity

Business continuity plan
3.2

Business continuity tested
2.6

2016 EDUCAUSE Core Data Service

5. Optimized
4. Established
3. Developing
2. Initial
1. Absent

2016 EDUCAUSE Core Data Service
## ITDR & BCP Organization

<table>
<thead>
<tr>
<th>OIT</th>
<th>Environmental Health &amp; Public Safety</th>
<th>Everyone Else</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITDR, Enterprise Systems</td>
<td>BCP, ACP University-wide</td>
<td>ITDR Maturing BCP, ACP</td>
</tr>
</tbody>
</table>

## ITDR Timeline

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>- Critical Business Unit Planning</td>
<td>- Budget cuts</td>
<td>- Catastrophic event plan</td>
</tr>
<tr>
<td>- Annual cold-site test</td>
<td>- Coordination &amp; Guidance</td>
<td>- Diminishing A in CIA</td>
</tr>
<tr>
<td>- Tabletop Exercises</td>
<td>- Unit responsibility</td>
<td>- Unlimited Google Storage</td>
</tr>
<tr>
<td>- MTTR, RPO/RTO defined</td>
<td>- IR &amp; Lessons Learned</td>
<td>- Cloud-backups</td>
</tr>
<tr>
<td>- Offsite backup</td>
<td>- Generator tests</td>
<td>- Payroll test</td>
</tr>
<tr>
<td>- Audit Interest/FIN</td>
<td>- Payroll tabletop</td>
<td>- Service Planning</td>
</tr>
<tr>
<td></td>
<td>- ITDR</td>
<td>- Audit Interest/FIN</td>
</tr>
</tbody>
</table>

---

### ITDR Timeline Details

- **2008 - 2012 ITDR**
  - Budget cuts
  - Coordination & Guidance
  - Unit responsibility
  - IR & Lessons Learned
  - Generator tests
  - Payroll tabletop
  - Audit Interest/FIN

- **2012++ ITDR, DIY**
  - Catastrophic event plan
  - Diminishing A in CIA
  - Unlimited Google Storage
  - Cloud-backups
  - Payroll test
  - Service Planning
  - Audit Interest/FIN
Business Continuity Planning

- Aligned within EH&PS
- Policy and governance structure
- Current initiative for NIMS alignment
- Ongoing tabletops and simulations:
  - Active Shooter
  - Train derailment
  - Major cybersecurity event
- External evaluators
- Established EOC & EOG

Central BCP System & Processes (LDRPS)

- BCPs storage
- Planning templates
- Call trees
- Periodic update requirement

Lessons Learned & Recommendations

- Key personnel makes the difference
- Confidentiality and Integrity trumps Availability
- Integrate ITDR throughout system/service lifecycle
- Consider Cloud backup alternatives
- Provide leadership and guidance that outlast you
- Integrated ITDR and BCP to avoid false assumptions
- Evolve from ITDR to Service Continuity Planning (SCP)
Continuity Planning Program

Introduction

- Business Continuity Planning Program
  - 2 year program
  - Kick-off Letter from the President - September 2012
- Objectives
  - Implement a Sustainable and Effective University Business Continuity Program
  - Provide Continuity Planning Information and Training
  - Provide Continuity Planning Tools
Continuity Planning Program Overview

• Governance
  – Program Group
    • Risk Management, Information Security
  – Leadership Group
    • one member from each College/Department

• Training
  – Impact Assessment (IA)
  – Continuity Plan Building
  – Plan Testing (TBD)

• Resources
  – Impact Assessment Questionnaire (IAQ)
  – Coyote Ready
  – Website
  – Continuity Planning Program Coordinator

Leadership Group Activities

• Leadership Group Training
• Conduct Periodic Meetings
• Address Unit Questions
• Participate in Program Changes
• Assist with Review Process
• Troubleshoot Issues
Information Flow

Campus Continuity Plan

Divisions

Departments
Operational Units Continuity Plan

Continuity Plan Process

Step 1
Impact Assessments
• Tool: Questionnaire

Step 2
Continuity Plan
• Tool: Coyote Ready Program

Step 3
Sign-Off Process
• Supervisor
• Continuity Planning Group

Step 4
Plan Maintenance
• Review
• Testing
Continuity Plan Annual Cycle

1. Department/Office will have implemented a continuity plan
2. Department/Office Continuity Plans will provide the basis for the implementation of the University Continuity Plan
3. Increase university readiness to deal with unexpected situations
4. Meet compliance requirements
CP Program Milestones

• June, 2013
  – Continuity Planning Sign-off completed for all critical units

• August, 2013
  – All CSUSB units begun the Continuity Planning process

• September, 2014
  – All CSUSB units completed the Continuity Planning Process
  – Program managed by Risk Management

Metrics

The progress of continuity planning efforts were measured by 5 key performance indicators (KPI):

– Plan Count
  • Typically one plan represents one unit, however, in some cases 2 or more units are included in one plan.

– Unique Coyote Ready Users accessing the plan
  • Almost all units have more than one person with access to their plan

– Number of functions
  • Each unit should have at least one.
  • Most of Academic Affairs’ units will be under teaching and or research.

– Number of documents
  • Indicators of documentation supporting unit functions.

– Number of action items
  • action items are gaps in continuity plans.
Business Continuity Program Progress Report

CHALLENGE
Continuity Planning Engagement and Sustainability

Next Phase for Continuity Planning
Strategies

- Leadership Group Activities
- Continuity Planning Sustainability Activities
  - Phone Call Support
  - Awareness Campaign
  - Continuity Planning Readiness
  - Take advantage of campus real incidents
    - Conduct surveys to find out how BCP worked
- Conduct Tabletop Exercises for the campus

Leadership Group Activities

- Quarterly Reports
  - Generate and distribute reports to each liaison/leader
  - Reports should contain:
    - Continuity Plan Status/Activity
    - Critical Functions
    - Action Items
    - Documents
    - Users
Continuity Planning Sustainability Activities

- Phone Call Support
  - Offer assistance for missing pieces of plan
  - Provide additional training
  - Answer questions or concerns

- Awareness Campaign
  - Monthly emails
    - Tips, Suggestions & Checklists
  - BYOS Webinars
  - Countdown to Continuity Planning Readiness
    - Planning, Testing and Assessment

ITS Business Continuity

- Designated a division coordinator
- Quarterly meeting with each area
- Annual testing
  - Desktop testing
  - 2 to 3 hours
- Developed a new BIA
- Continuous improvement on communications
Challenges

- Changes in management personnel
  - Business Continuity Coordinator
- Divisions/departments re-organization
- Changes in personnel/roles
- Changes in platform – Kuali ready
- Changes in technology
  - Cloud has had a significant impact

Maturity Indicators

- Units BC Plan Readiness
  - Completeness
  - Content quality
  - Availability
- Testing and Revisions
- BC Awareness campaigns
- Training and Assistance
Discussion Questions: Business Continuity

- What is the **obstacle** keeping you from the next maturity level for this dimension?

- Besides time or money, what can help overcome the obstacles? Where you have had **success** in this dimension? What were the keys to that success? What helped you get there?

Tools for Better Decision Making

Campus leaders use EDUCAUSE assessment and benchmarking services to plan for and manage IT service delivery, financials, security and risk, technology-supported learning, and digital initiatives.

- **Learning Space Rating System**
  - Measure how classroom design supports and enables active learning

- **Information Security Program Assessment Tool**
  - Evaluate the maturity of your information security program

- **IT Risk Register**
  - Identify common risks to support your strategic IT risk management program

**ASSESSMENT**

- **Technology Research in the Academic Community**
  - Track student and faculty technology needs and experiences

- **Core Data Service**
  - Compare peer and aspirant data for IT financials, staffing, and services

- **Benchmarking Service**
  - Measure technical and cultural capability for digital initiatives like student success

**BENCHMARKING**

**Session Resources:**

- [https://tinyurl.com/mwmd86o](https://tinyurl.com/mwmd86o)
- [educause.edu/coredata](educause.edu/coredata)
- [educause.edu/benchmarking](educause.edu/benchmarking)