

# Information Security in the CSU

## On the Scoreboard, But Still Playing Catch Up

March 5<sup>th</sup>, 2008

David Ernst  
Assistant Vice Chancellor /  
Systemwide CIO

# Agenda

- CSU Background
- CSU Mission
- Security Perspectives
- CSU Security Program
  - Goals
  - Challenges
  - Accomplishments

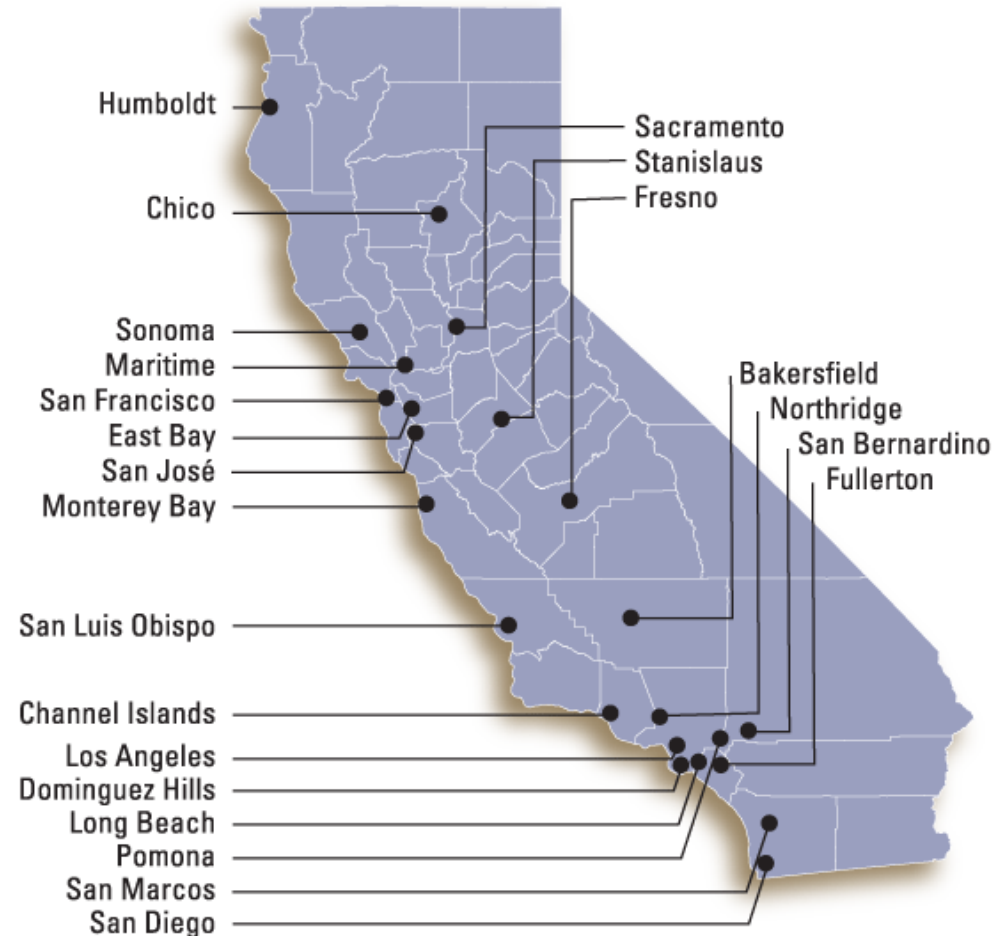


# CSU Background

- Statewide system
  - Largest, most diverse, and one of the most affordable
  - 23 campuses
  - 417,000 students
    - graduate 84,000 annually
  - 46,000 faculty and staff
  - \$4.4 billion annual budget

<http://www.calstate.edu>

## The 23 Outstanding Campuses of the CSU



# CSU Mission

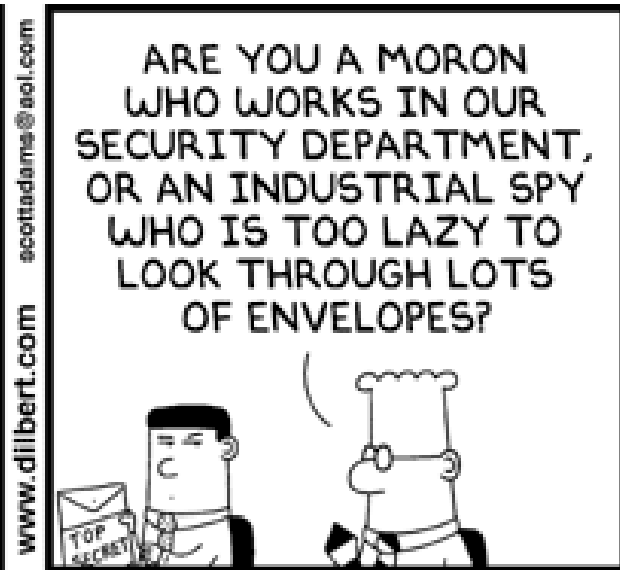
- To provide opportunities for individuals to develop intellectually, personally, and professionally
- To encourage and provide access to an excellent education to all who are prepared for and wish to participate in collegiate study
- To provide public services that enrich the university and its communities

## **CSU Drivers**

- Highest standards of education
- Meet the demand for higher education in California with the available resources
- Commitment to serve the changing educational needs of the state and its people

# CSU Security Program Drivers

- Create a secure environment that provides the opportunity for individuals to develop intellectually, personally and professionally.
- Engage academic and operational units in the development of a security environment that provides access to an excellent education experience



© Scott Adams, Inc./Dist. by UFS, Inc.

# The CSU's Perspective on Security

All members of the CSU community are responsible for protecting assets entrusted to the CSU.

# Definition: Enterprise-Level Security

According to CERT:

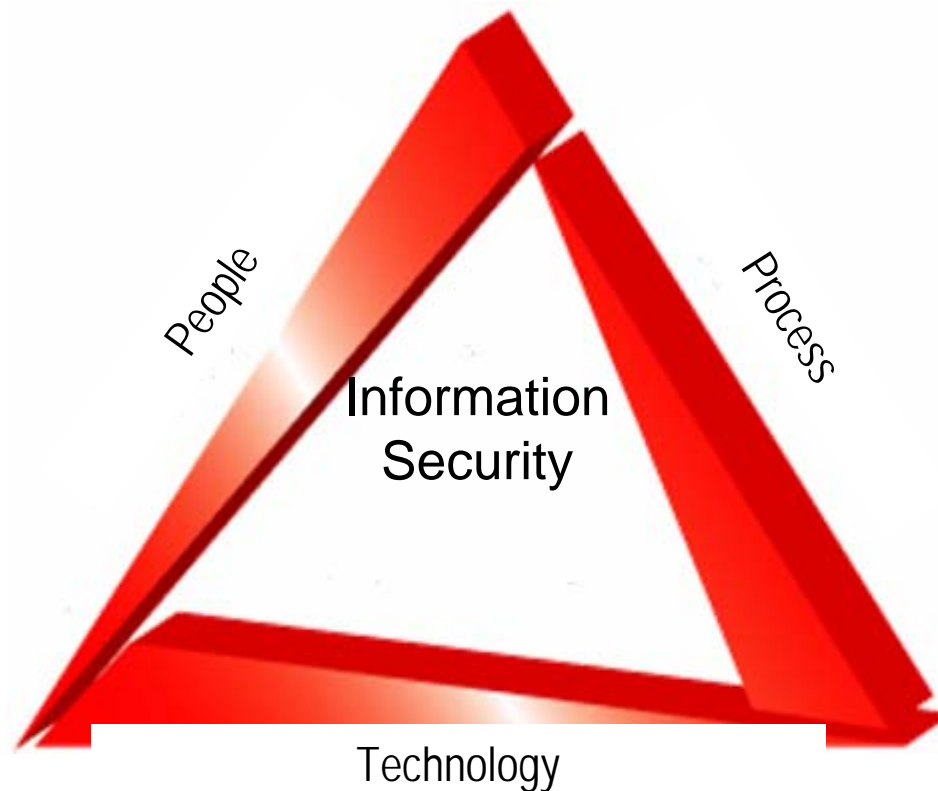
“A desired enterprise security state is the condition where the *protection strategies* for an organization's critical *assets* and business *processes* are commensurate with the organization's *risk appetite* and *risk tolerances*.” –

[www.cert.org/governance/adequate.html](http://www.cert.org/governance/adequate.html)

# CSU Information Security Program Goals

- Support the CSU mission
- Integrate security into the culture of the CSU
- Collaborate with academic and operational units to ensure confidentiality, integrity, and availability of CSU information assets
- Ensuring compliance with applicable federal, state, local and international regulatory/legal requirements related to security and privacy
- Promote Security Awareness
- Develop programs that are flexible and adaptable to change and comply with applicable regulations

# Building an Effective Information Security Program - Security As An Enabler



## **Building an Effective Information Security Program - Articulate the Value of Information Security**

- The expected benefits of investments in security projects must be articulated in non-technical terms and must be linked to drivers that are specific to the university's mission, environment and culture.
- Effective support from the University's senior managers requires that security professionals talk about expected outcomes and risk mitigation.

"Appropriate business security is that which protects the business from undue operational risks in a ***cost-effective*** manner." – Sherwood, 2003

## **Building an Effective Information Security Program— Estimate the Cost - Effectiveness of Security**

Estimation of cost and effectiveness of security requires knowledge and estimation of:

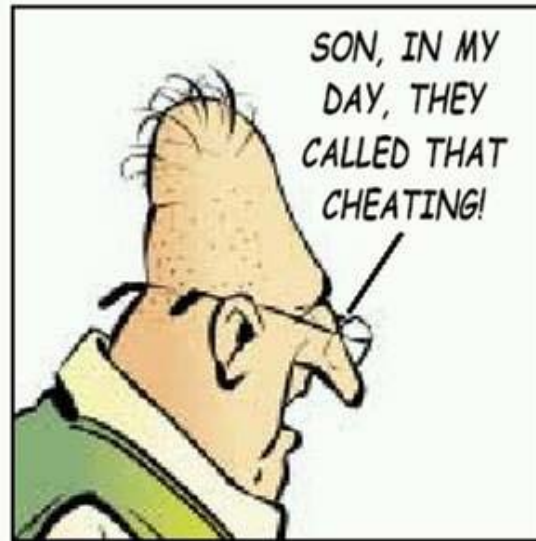
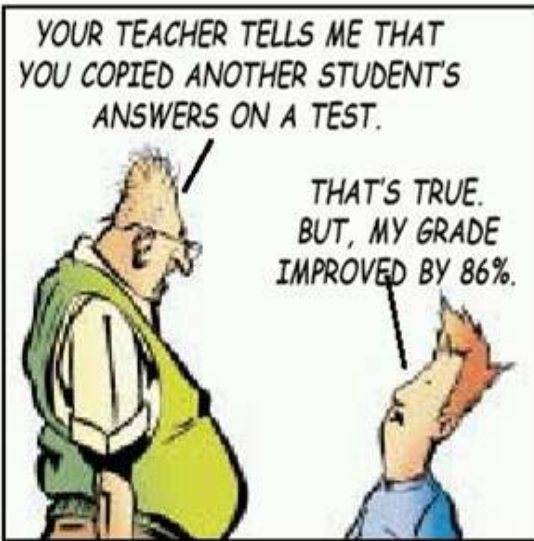
- Assets to protect
- Possible threats or losses
- Cost of mitigating risks
- Cost of contingencies

## **Building an Effective Information Security Program – Leverage Best Practices**

- Security professionals must pay attention to the successes and failures of others.
- In many ways, an effective information security program is built by adopting the best practices of others.

**LEAN THINKING**

by Jim Jacoby



© Ford Production System, December 2000

## **Building an Effective Information Security Program - Obtain Management's Support**

Obtaining and maintaining management support for security initiatives is enhanced by understanding the University's culture and by collaborating with stakeholders on initiatives that support the mission of the University.

To achieve this goal, we align our security initiatives to academic and business drivers.

# Common Problems with Information Security Programs

- Adopting a “one-size” fits all solution
- Developing policies without consulting with all appropriate stakeholders
- Trying to eliminate all security risks
- Assuming the information security team is accountable for information security

# **Building an Effective Information Security Program –**

## **What Other Elements Should You Consider?**

## **CSU Information Security Program Strategies**

- Establish a governance body
- Develop security plan
- Formalize policies and standards
- Promote awareness and training to improve the overall security posture of the CSU
- Develop an information security risk management program

# Security Governance at the CSU

- Establishes responsibility and authority
- Defines strategic direction
- Ensures objectives are achieved
- Manages information security risks
- Ensures resources are being used appropriately

# CSU Governance Structure

- Board of Trustees
- Chancellor
- Campus Presidents
- CIOs/ISOs
- Others

# Developing the CSU Information Security Plan

- Includes:
  - System-wide policies and standards
  - Security awareness and training
  - Data and asset classification and protection
  - Risk assessments
  - Incident management
  - Business Continuity/Resumption Planning
  - Performance measures
  - Implementation strategies

....and more

# CSU Systemwide Policies Project

Our policies and standards ***support*** the strategic objectives of the CSU system-wide security plan

# Promoting Security Awareness

Numerous security incidents at institutions of higher learning across the nation, including the CSU, illustrate that the human factor is both a weak link in the security continuum and an important factors in the success of an information security program.

All CSU employees must understand their respective information security responsibilities, and properly use and protect the information and resources entrusted to them.

# CSU Systemwide Awareness Training Project

The California State University (CSU) recognizes that an information security awareness program is an important component in the overall strategy to protect the CSU's information assets.

The CSU's information security awareness program will inform individuals, who come into contact with CSU assets, of the risks associated with their activities and of their responsibilities to comply with CSU policies and procedures.

## Other Initiatives

- Information Security Risk Management
- Incident Management Program
- Business Continuity and Disaster Recovery Planning
- Infrastructure Terminal Resource Project (ITRP)
- Identity and Access Management (IAM)

# Information Security Risk Management

*The CSU views risk management as an important component of its information security programs.*

*Integrating risk management concepts into the information security program will permit the CSU to achieve its goal of managing internal and external threats and vulnerabilities.*

# CSU Risk Assessment Framework

- Identify and classify assets
- Identify threats and vulnerabilities
- Determine risk and measure impact

*Currently CSU risk assessment tool is largely based on ISO 17799:2005*

# CSU Incident Management Program

Effective incident management practices allow campuses to contain exposures and to quickly recover academic and business operations.

## **Key Elements Of An Effective Incident Management Program**

- Identify and document incidents
- Prioritize incidents based on business impact
- Track incidents
- Communication plan
- Report incidents to appropriate stakeholders

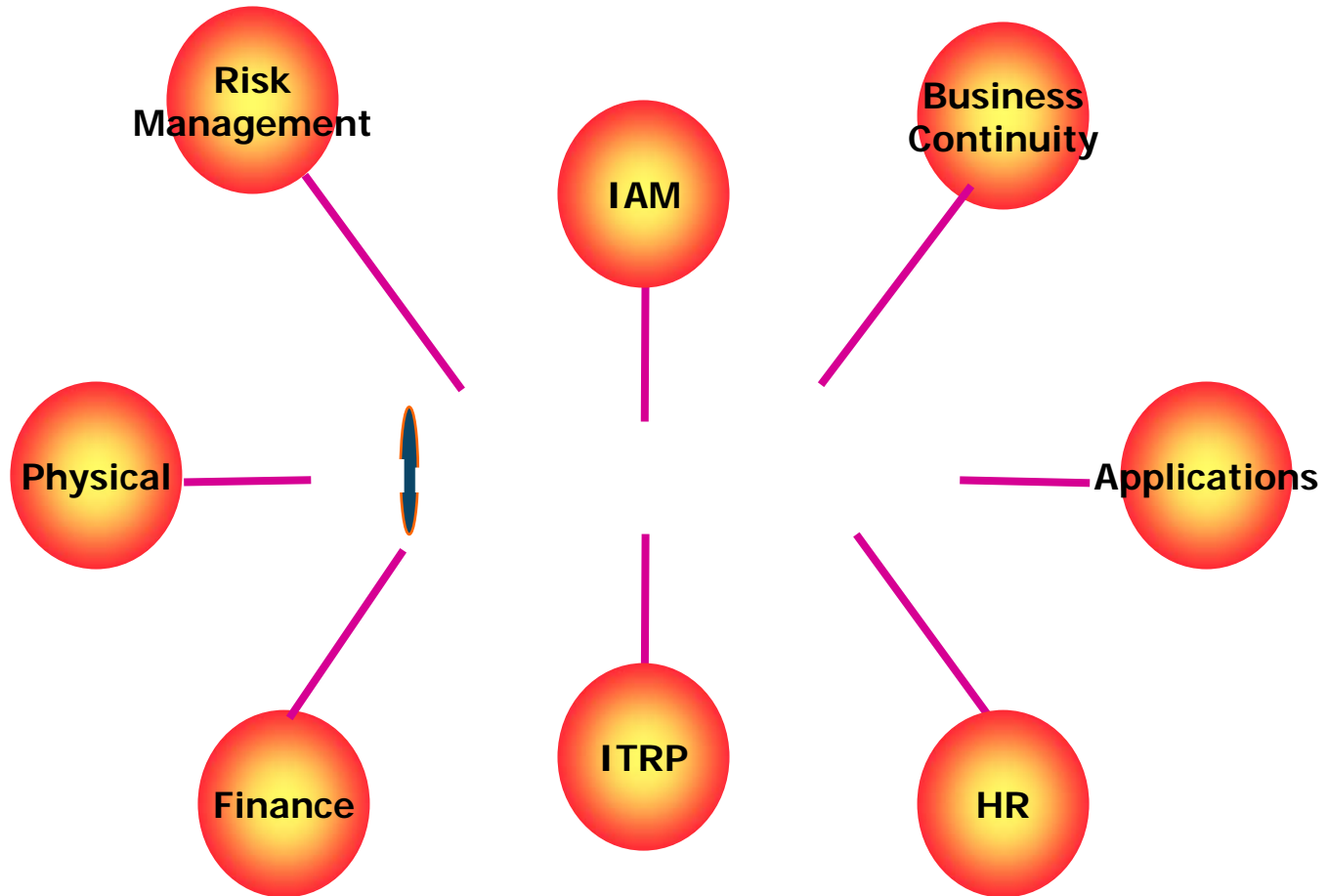
# Business Continuity & Disaster Recovery Planning

- Each campus must develop a business continuity plan that ensures successful maintenance or restoration of essential functions following an unfavorable event.
- Continuity plans will be based on a Business Impact Analysis and Risk Assessment.

# Business Impact Analysis & Risk Assessment

- The Business Impact Analysis:
  - identifies essential functions and workflow;
  - determine the impacts of a vulnerability/threat to essential functions;
  - prioritize/establish recovery time objectives for the essential functions; and
  - if appropriate, establish recovery point objectives for essential functions.
- The Risk Assessment identifies vulnerabilities and threats and define the controls in place to reduce the exposure to the vulnerabilities/threats.

# Bridging the Divide of Information Security



# Security Challenges

- Limited resources
- Culture of Academic Freedom
- Usability vs. Security

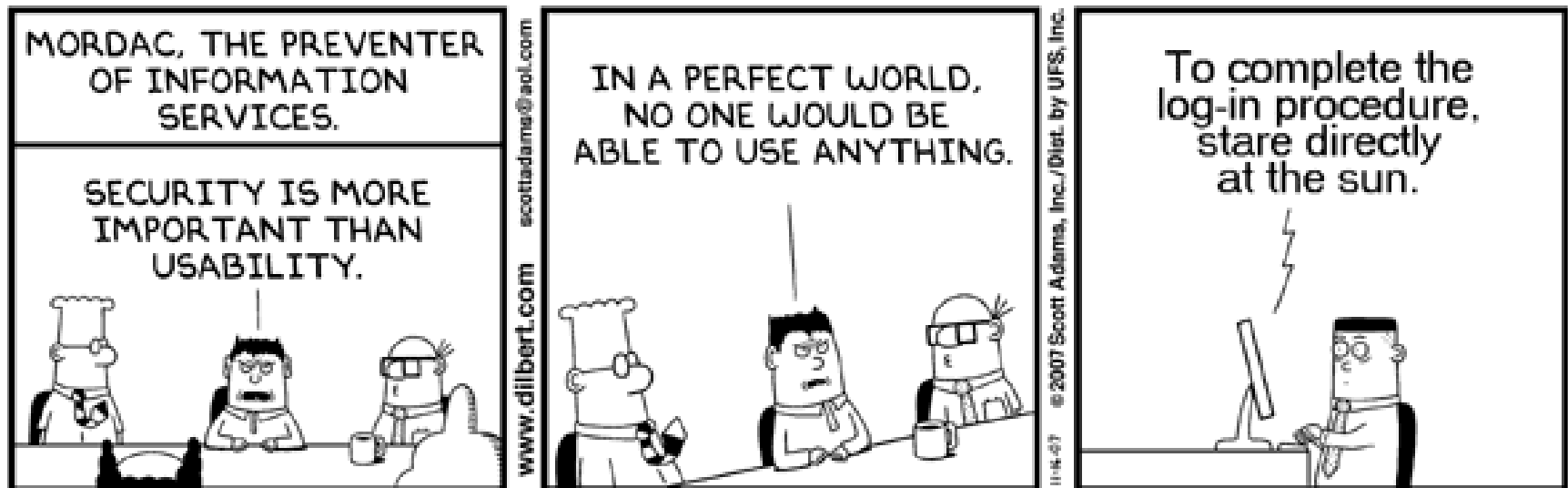
# Challenge: Limited Resources

- Funding
- Personnel

## **Challenge: Culture of Academic Freedom**

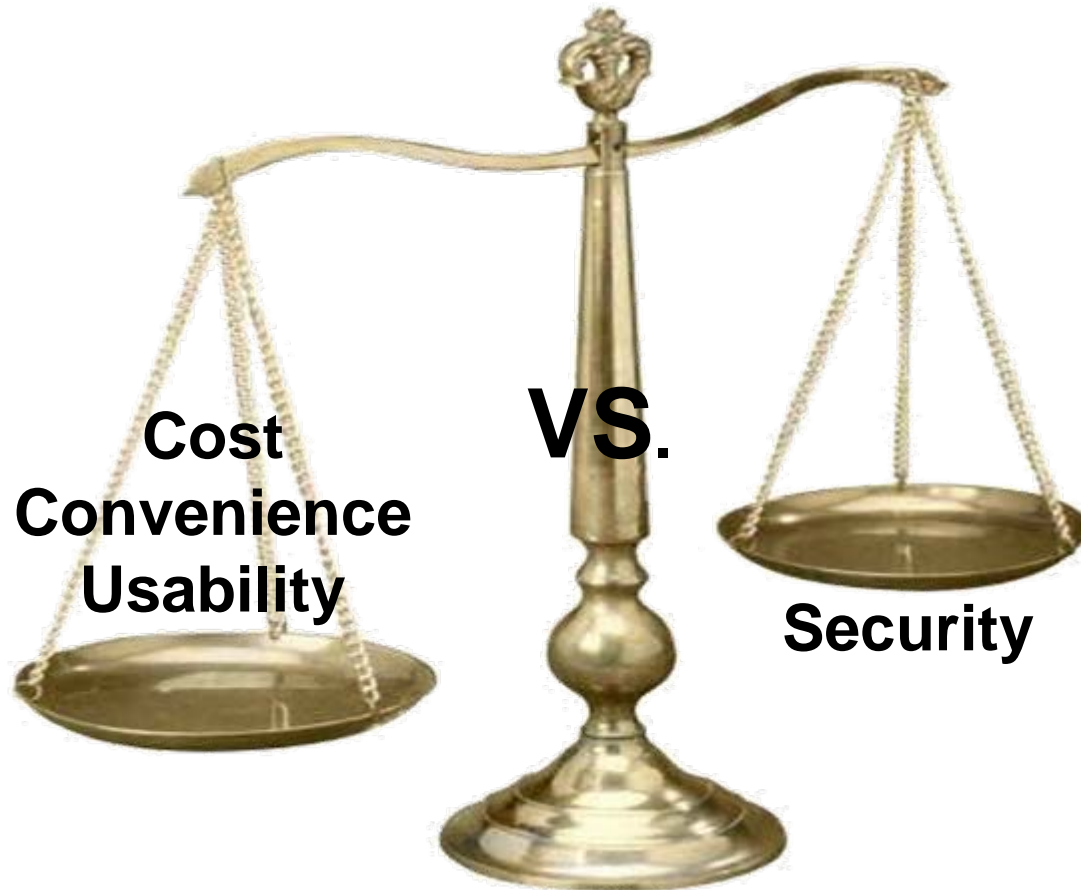
Our openness and computing power makes us an attractive target for individuals who want to launch cyber attacks.

# Security is More Important Than Usability



© Scott Adams, Inc./Dist. by UFS, Inc.

# Challenge: Usability vs. Security Trade-Offs



# Solutions to Security Challenges

- Acknowledge risk as the institutional driver
- Position security as an enabler to resiliency
- Manage security as a process, not an end goal
- Measuring success using critical success factors or key performance indicators (KPIs)

# Future – Where Are We Going?

- Monitoring and compliance
- Measuring success
- Changing the CSU culture

## **Monitoring and Compliance**

The CSU information security program must ensure that programs goals are aligned with applicable regulations

Internal reviews conducted by the campus and internal and external audits monitor campuses for compliance with applicable regulations and CSU policies.

# Measuring Success

- Establish critical success factors
- Track performance
- Analyze results to identify opportunities for improvement

## **Changing the CSU Culture**

**..... *Let's end where we began***

- Information security programs within the CSU must support academic and operational programs.
- Security is everyone's responsibility.
- Effective information security practices must be integrated into the "fabric" of the CSU.

## Closing Thought

*The ultimate measure of a man is not where he stands in moments of comfort and convenience, but where he stands at times of challenge and controversy.*

- Martin Luther King, Jr.

# Questions?

## References

- CERT: Focus on Resiliency: A Process-Oriented Approach to Security by Rich Caralli & James Stevens
- [www.cert.org/archive/pdf/GESppt.pdf](http://www.cert.org/archive/pdf/GESppt.pdf)
- <http://www.csoonline.com/analyst/report816.html>



[www.calstate.edu](http://www.calstate.edu)