Security Review

July 2009 – March 2010

Gabe Lawrence
Director, IT Security

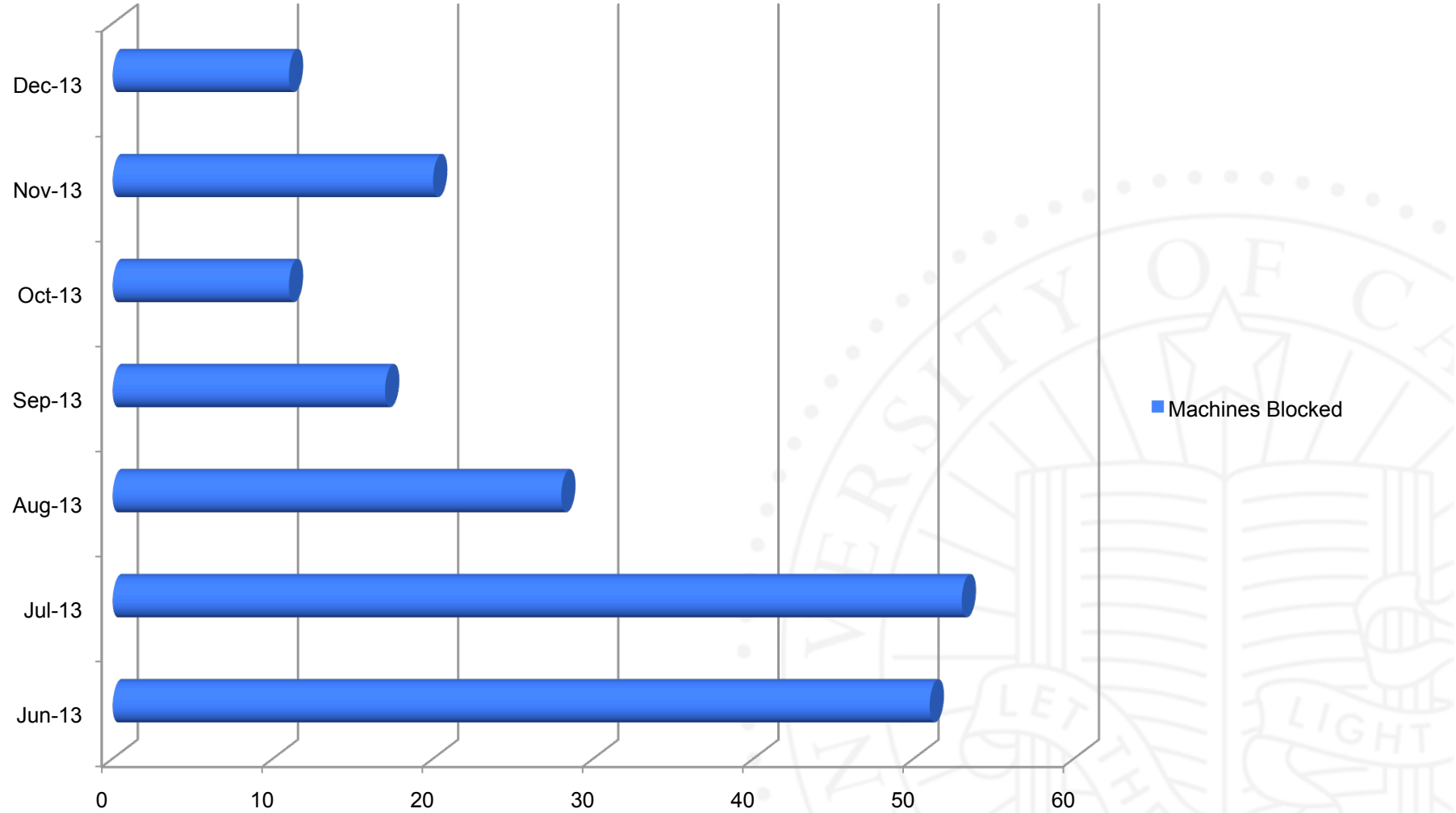
Administrative Computing & Telecommunications

UC San Diego

Information Security and Privacy Council

- Advisory to the UCSD Chief Ethics and Compliance Officer
- Address security weaknesses in high-risk circumstances
  - Policy
  - Best Practices
  - Common Solutions
- Campuswide representation

Blocked Machines/Month



Costs

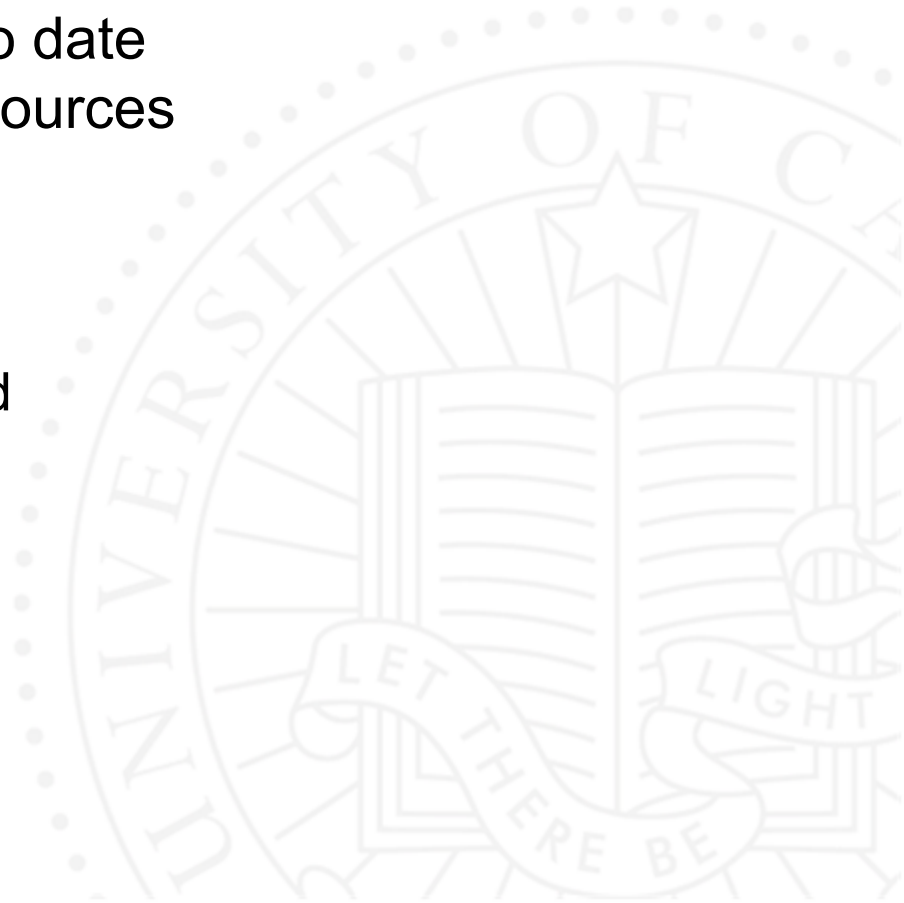
- Notified slightly less than 40,000
- Direct and indirect cost per notification roughly $90-$195

- Direct and Indirect cost to UCSD over last 6 months **~$3.6M to $7.8M**

http://www.tech-404.com/calculator.html
http://www.idtheftcenter.org/workplace_facts.html

Key Risk Areas

- Lack of IT Support Staff
  - Incomplete application of standards
  - Lack of monitoring
  - Failure to keep software up to date
  - Failure to utilize available resources
- Shift of attack vector
  - <2008
    - Network attack vector
    - Vulnerability scanning worked
  - >2008
    - Web applications
    - Web browsers
    - Scanning doesn't work



Security Short/Long Term Goals

- Organizational structure – see ISPS Draft Charter
- Guidance
  - Setting priorities on encryption, network intrusion, data loss prevention, etc..
  - Report back to CARE committee on activities on a semi-annual basis (once in writing and once face-to-face)
- Education and training
  - Web application development security training
  - Attend DSA training and Sysadmin training on a regular basis
  - Use education to help own departments
- Monitoring and auditing
  - Install Host based Intrusion software (campus licensed)
  - Web application attacks
- Optimal use of technical solutions
  - Eliminate reliance on redundant IT infrastructure (Campus Mail and Active Directory)
  - Complete network partitioning and firewalling
  - Install Campus licensed HIPS
  - Enforce Encryption

■ = Short Term

What you should do

- Risk Analysis
  - What data do you have?
  - What protections do you have?
  - Is it enough?
- Address risk with people, process and technology

Resources

- security.ucsd.edu
  - IT Security for UCSD Business Managers

Q & A