How are we keeping Hackers away from our UCD networks and computer systems?

UCDAVIS
University of California, Davis

UCDAVIS
DEPARTMENT OF
ENTOMOLOGY

University of California
UC Davis Plant Pathology

Cybercrime

- Sony's Hacking Scandal Could Cost The Company $100 Million - **http://www.businessinsider.com/sonys-hacking-scandal-could-cost-the-company-100-million-2014-12**
- Annual U.S. Cybercrime Costs Estimated at $100 Billion

  Wall Street Journal: http://www.wsj.com/articles/SB10001424127887324328904578621880966242990
- Ebay 145,000,000 compromised records
- JP Morgan Chase 76,000,000 compromised records
- Anthem 80,000,000 compromised records
- Home Depot 56,000,000 compromised records
- Target 70,000,000 compromised records

Source: DataBreaches.net, IdTheftCentre - http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Cybercrime

- Cybercrime is a growth industry. The returns are great, and the risks are low. We estimate that the likely annual cost to the global economy from cybercrime is more than $400 billion. A conservative estimate would be $375 billion in losses, while the maximum could be as much as $575 billion

McAfee **Center for Strategic and International Studies** June 2014:
http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

Cybercrime

- The cost of cybercrime includes the effect of hundreds of millions of people having their personal information stolen—incidents in the last year include more than 40 million people in the US, 54 million in Turkey, 20 million in Korea, 16 million in Germany, and more than 20 million in China. One estimate puts the total at more than 800 million individual records in 2013. This alone could cost as much as $160 billion
- per year

McAfee **Center for Strategic and International Studies** June 2014:

http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

How can we protect our Networks and Computer Systems?

What is Network Security?

- Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority.

http://en.wikipedia.org/wiki/Network_security

What is Network Security?

- After asking What is network security?, you should ask, What are the threats to my network?
- Many network security threats today are spread over the Internet. The most common include:
- Viruses, worms, and Trojan horses
- Spyware and adware
- Zero-day attacks, also called zero-hour attacks
- Hacker attacks
- Denial of service attacks
- Data interception and theft
- Identity theft

How Does Network Security Work?

- Network security is accomplished through hardware and software. The software must be constantly updated and managed to protect you from emerging threats.
- A network security system usually consists of many components. Ideally, all components work together, which minimizes maintenance and improves security.
- Network security components often include:
- Anti-virus and anti-spyware
- Firewall, to block unauthorized access to your network
- Intrusion prevention systems (IPS), to identify fast-spreading threats, such as zero-day or zero-hour attacks
- Virtual Private Networks (VPNs), to provide secure remote access

What are the benefits of Network Security?

- With network security in place, our departments will experience many benefits
- We will be protected against business disruption, which helps keep employees productive
- Network security helps us to meet mandatory regulatory compliance from campus Cyber-Security policies
- Because network security helps protect our data, it reduces the risk of legal action from data theft
- Ultimately, network security helps protect our department's reputation

What is Computer Security?

- Is security applied to computing devices such as computers, servers and smartphones
- It includes all the processes and mechanisms by which digital equipment, information and services are protected from unintended or unauthorized access, change or destruction
- It includes Physical Security to prevent theft of equipment and Information Security to protect the data on that equipment
- Cybersecurity is the process of applying security measures to ensure confidentiality, integrity, and availability of data. It assures protection of assets, which includes data, desktops, servers, buildings, and most importantly, humans. The goal of cybersecurity is to protect data both in transit and at rest

What is UCD doing to protect our networks and computer system?

- Anti-virus
- Authentic Message Registry (http://security.ucdavis.edu/secure/authentic/index.html)
- Authenticated SMTP
- Central security initiatives (Campus vulnerability scanning, Personal identity information, Security information and event management (SIEM), Web application vulnerabilities and VLAN firewalls
- DNSSEC Implementation project (2013)
- Email Attachment Filtering
- Encryption

What is UCD doing to protect our networks and computer system?

- Campus Firewall Services
- Identity and Access Management
- Personal Identity Information (PII)
- Secure Email Authentication (SSL)
- Sophos Anti-Virus
- Spam Filtering
- Tripwire
- Virus Filtering
- Web Application Security

What is UCD doing to protect our networks and computer system?

- UC Davis Cyber-Safety Program
- UC Davis Policy and Procedure Manual - Chapter 310, Communications and Technology - Section 22, UC Davis Cyber-Safety Program
- http://manuals.ucdavis.edu/PPM/310/310-22.pdf

UCD Cyber-Safety Program

- This policy establishes that devices connected to the UC Davis electronic communications network must meet UC Davis security standards or seek exception authorization. Campus units may develop and implement more rigorous security standards. Computing applications hosting critical and/or sensitive university information are subject to more stringent security standards, as defined in UC Business and Finance Bulletin, IS-3.
- Devices--Includes computers, printers, or other network appliances, as well as hardware connected to the campus network from behind security devices/systems.

UCD Cyber-Safety Program

- Level 1 Practices (Highest Priority)

- Software patch updates
- Anti-virus software
- Insecure Network Services
- Authentication
- Personal Information
- Firewall Services

UCD Cyber-Safety Program

- Level 2 Practices (Secondary Priority)
- Physical Security
- No Open Email Relays
- Proxy Services
- Audit Logs
- Backup, Recovery, and Disaster Planning
- Training for Users, Administrators, and Managers
- Anti-Spyware Software
- Release of Equipment with Electronic Storage
- Incident Response Plan
- Web Application Security

UCD Cyber-Safety Program and Campus Units

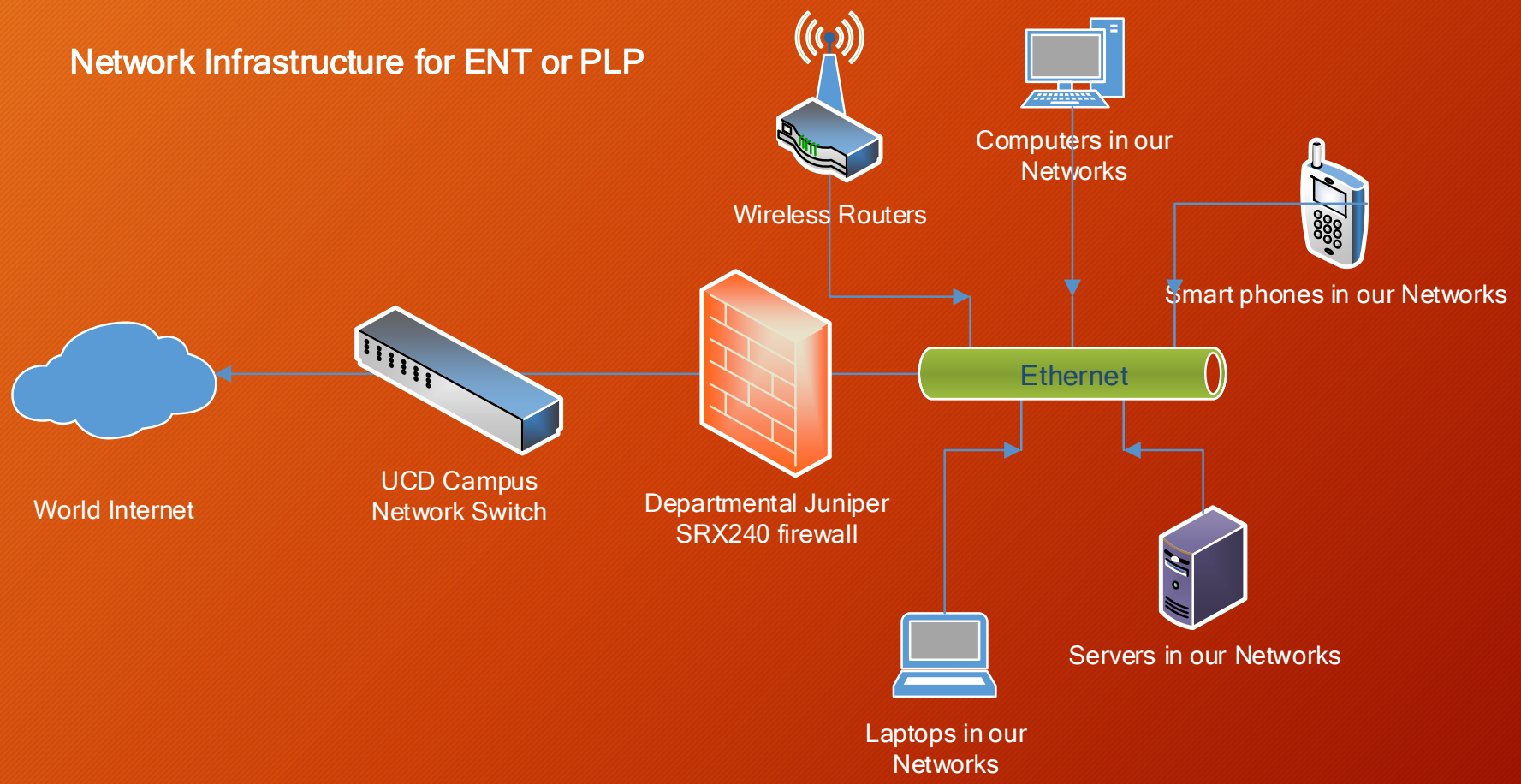
- Campus units must ensure devices connected to the campus network comply with the security standards or develop/implement strategies to mitigate the risks posed by non-compliance.
- Campus units must annually report to their respective Dean, Vice Chancellor or Vice Provost, the extent to which unit operations are consistent with the campus security standards. Where compliance is not complete, the report must document a compliance plan, a statement indicating a specific security standard is not applicable or an acknowledgement and acceptance of the information risks associated with continued non-compliance to the security standard

UCD Cyber-Safety Program and Campus Units

- Campus units are responsible for:
- Developing and implementing measures to ensure campus network connected devices are in compliance with security standards.
- Reviewing unit compliance to security standards and prepare and submit annual unit compliance reports/plans to campus administrative officials.
- Facilitating security training for users, system administrators and managers

How are we protecting our departmental Networks and Computer Systems?

Departmental Network Infrastructure



Network and Computer security in our Departments

- Network Security at the Departmental Level:
  - UCD Cyber-Safety Compliance
  - Departmental Firewalls
  - Network Scans
  - MS Active Directory Group Policies
  - Web Applications and sever security
  - Insecure Network Services
  - Secured Wireless Routers
  - MAC Filtering Implementation

Network and Computer security in our Departments

- Network Security at the Computer System Level:
  - UCD Cyber-Safety Compliance
  - OS Firewall Activation
  - Software Patch Updates
  - Antivirus

Network and Computer security in our Departments

- Computer Security at the Departmental Level (Servers):
  - UCD Cyber-Safety Compliance
  - Strong Authentication
  - Restricted Access to Servers and Computers
  - OS Firewall Activation
  - WSUS – MS Operating System Software Patch Updates
  - BigFix Third-Party Software Updates
  - Antivirus
  - Physical Security

Network and Computer security in our Departments

- Computer Security at the Computer System Level:
  - UCD Cyber-Safety Compliance
  - Strong Authentication
  - MS Active Directory Group Policies
  - Restricted Access to Computers
  - Restricted or Minimized used of the “Administrator” account
  - OS Firewall Activation
  - Software Patch Updates
  - Antivirus
  - Physical Security

How are we keeping Hackers away from our UCD networks and computer systems?

- As you have seen, UCD and ourselves are doing our best to protect you from Hackers, malware, spyware and any other computer threat that may try to get to our networks or to your computers.

How are we keeping Hackers away from our UCD networks and computer systems?

Thank You!

Julio Cardenas

PHOENIX