

Yale University ITS,
Information Security Office

Director - H. Morrow Long

The Internet: Co-Evolution of Technology and Society

CPSC 156a, Fall 2003

Guest Lecture

Title: Information security in the new digital millennium -- How
now Computer and Network Security is everyone's business
(and problem).

November 13 2003

Yale Information Security Committee ▶

YaleCERT ▶
(Computer Emergency Response Team)

ITS INFORMATION SECURITY OFFICE

Establishment ▶

Mission/Charter ▶

FIRST YEAR

Incidents ▶

Initiatives ▶

Plans ▶

Yale University, IT Advisory Cmte, Information Security SubCommittee

Non-ITS Committee Members

Robert McNeil
Director of University Auditing

John Mayes
Director of Procurement

Rotating Position
Associate Provost

Susan Sawyer
Deputy General Counsel
Office of General Counsel

Stacy Ruwe
Executive Director
Financial Operations
School of Medicine

ITS Information Security Office

H. Morrow Long
Director and CISO

Allison MacFarlan
Academic ISO

Jim Hackett
Administrative Systems ISO

ITS Committee Members

Philip E. Long
University Director of Information
Technology

Charles Powell
Director of Academic Computing

Indy Crowley
Director of Administrative Systems

Andrew Newman
Director of Technology & Planning

Joseph P. Paolillo
Associate Director of
Data Network Operations

David Stagg
Director of InfoSec
School of Medicine, ITS

H. Morrow Long, “Yale University”,

Formal Title: Director of Information Security,
DMCA N Agent, CS Fac, He who delivers bad news,
Official Interpreter of IT policy, gentle introducer to DMCA
and Copyright issues to Frosh at Orientation.

Private Institution where Bill met Hillary, dubya was a frat
boy.

In house counsel (20 person office, we get sued a lot!)

Keeping our students from being sued by the RIAA. At
one point I was tasked with finding someone to pay (off).



Yale Information Security



Yale Information Security





From the writer of "CLEAR AND PRESENT DANGER"
and "PATRIOT GAMES"

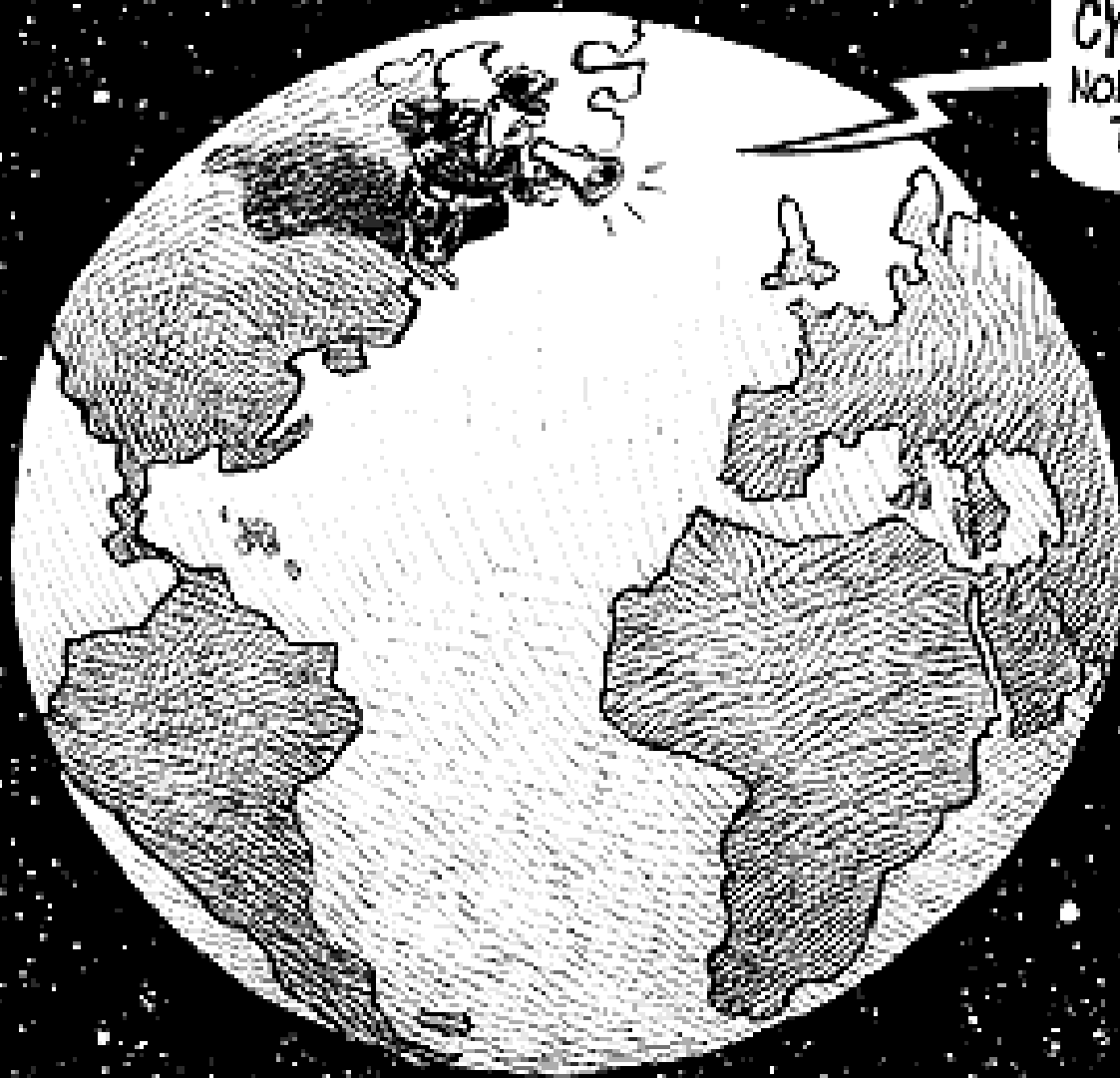
TOM CLANCY'S NETFORCE

THE INTERNET HAS BECOME A WAR ZONE



www.yale.edu/its/security

Security@yale.edu



CYBERPOLICE!
NOBODY LEAVES
THE ROOM!...

CHAPETTE

HACKERS CAN TURN YOUR HOME COMPUTER

By RANDY JEFFRIES / *Weekly World News*

WASHINGTON — Right now, computer hackers have the ability to turn your home computer into a bomb and blow you to Kingdom Come — and they can do it anonymously from thousands of miles away!

Experts say the recent "break-ins" that paralyzed the Amazon.com, Buy.com and eBay websites are tame compared to what will happen in the near future.

Computer expert Arnold Yabenson, president of the Washington-based consumer group National CyberCrime Prevention Foundation (NCPF), says that as far as computer crime is concerned, we've only seen the tip of the iceberg.

"The criminals who knocked out those three major online businesses are the least of our worries," Yabenson told *Weekly World News*.

"There are brilliant but unscrupulous hackers out there who have developed technologies that the average person can't even dream of. Even people who are familiar with

how computers work have trouble getting their minds around the terrible things that can be done.

"It is already possible for an assassin to send someone an e-mail with an innocent-looking attachment connected to it. When the receiver

downloads the attachment, the electrical current and molecular structure of the central pro-

INTO A

... & blow your family to smithereens!



KABOOM! It might not look like it, but an innocent home computer like this one can be turned into a deadly weapon.

"As shocking as this is, it shouldn't surprise anyone. It's just the next step in an ever-escalating progression of horrors conceived and instituted by hackers."

Yabenson points out that these dangerous sociopaths have already:

- Vandalized FBI and U. S. Army websites.
- Broken into Chinese military networks.
- Come within two digits of cracking an 87-digit Russian security code

scariest," Yabenson said.

"Soon it will be sold to terrorists cults and fanatical religious-fringe groups.

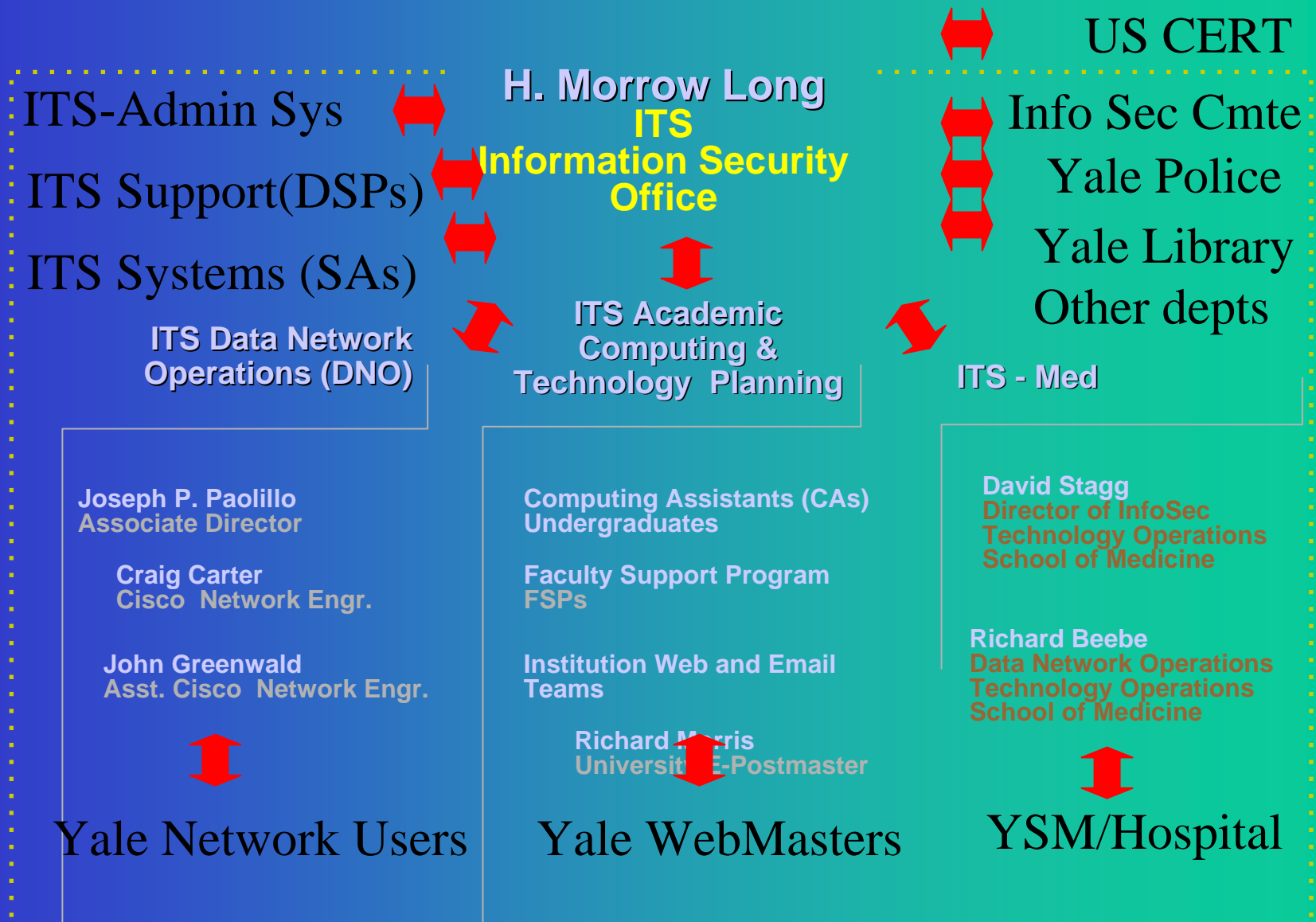
"Instead of blowing up a single plane, these groups will be able to patch into the central computer of a large airline and blow up hundreds of planes at once.

"And worse, this e-mail bomb program will eventually find its way into the hands of anyone who wants it."

Sickos can wreak death and destruction from



YaleCERT (Yale Computer Emergency Response Team)



Establishment/History

Pre-1995	Coopers & Lybrand & Yale Auditing Audit Recommendation	Yale's external auditors (C & L) recommended establishing a Yale Information Security Officer in yearly audits.	Yale's internal auditors recommended establishing a Yale Information Security Officer in yearly audits.
1995	December Position Posted	Yale posts an Information Security Officer position.	Yale interviews Information Security Officer position candidates through the year in 1996.
1997	June ISO Hired.	Yale hires its first Information Security Officer.	Yale Information Security (Policy & Steering) Committee founded in summer of 1997.
1998	Plans, Policies Formalization.	Define formal structure and Mission for Yale Information Security Office.	Official charter for Yale Information Security Committee.

Mission / Charter

MISSION

Statement

To support the goals of the Yale enterprise by assuring the availability, integrity and confidentiality of information.

CHARTER

Points

Policies, Standards and Practices.

- Propose, Advise, Coordinate, Write.

Assurance and Monitoring

- Auditing, Testing, Support, Detection.

Investigation and Enforcement

- Incident Handling and Tracking.

Awareness and Education

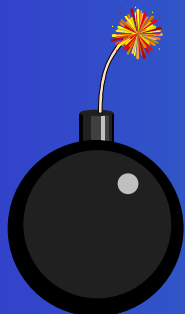
- Communication and Training.

Major Incidents



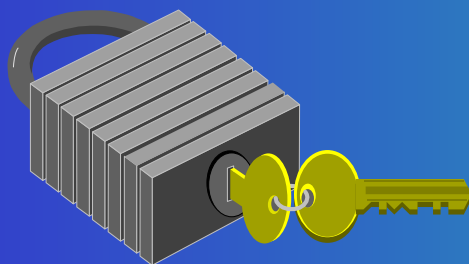
INTRUSIONS

- Departmental Linux PCs - Summer 1997
- Yale Library Web Server Intrusion - Sept. 97
- ITS ACS Pantheon “Minerva” Break-In Oct. 97



DENIAL OF SERVICE ATTACKS

- “SMURF” network broadcast bounce packet flood - Spring 97 through Jan 1998.
- “Pepsi” floods via departmental Linux PCs and Pantheon accounts -- Summer and September 1997.
- “SPAM” relaying via YaleVM, ITS and CS E-Mail servers (Unsolicited Bulk/Commercial E-Mail). 1997-8.



USER ACCOUNTS COMPROMISED

- ITS ACS Pantheon “Minerva” Break-In Oct. 97
- Network Sniffing Reported Nov 97 - Jan 1998.

Yale InfoSec Incidents

- Sniffing
- Spoofing
- Spamming
- Flooding
- E-Mail forgery, harassment, etc.
- Web based identity theft.
- Intrusions (Unix and Linux computers)
- Account compromises (telnet, POP)
- Viruses
- Copyright, Software license infringement



and *Creeping Death Music* VS. **Yale**, et.
al

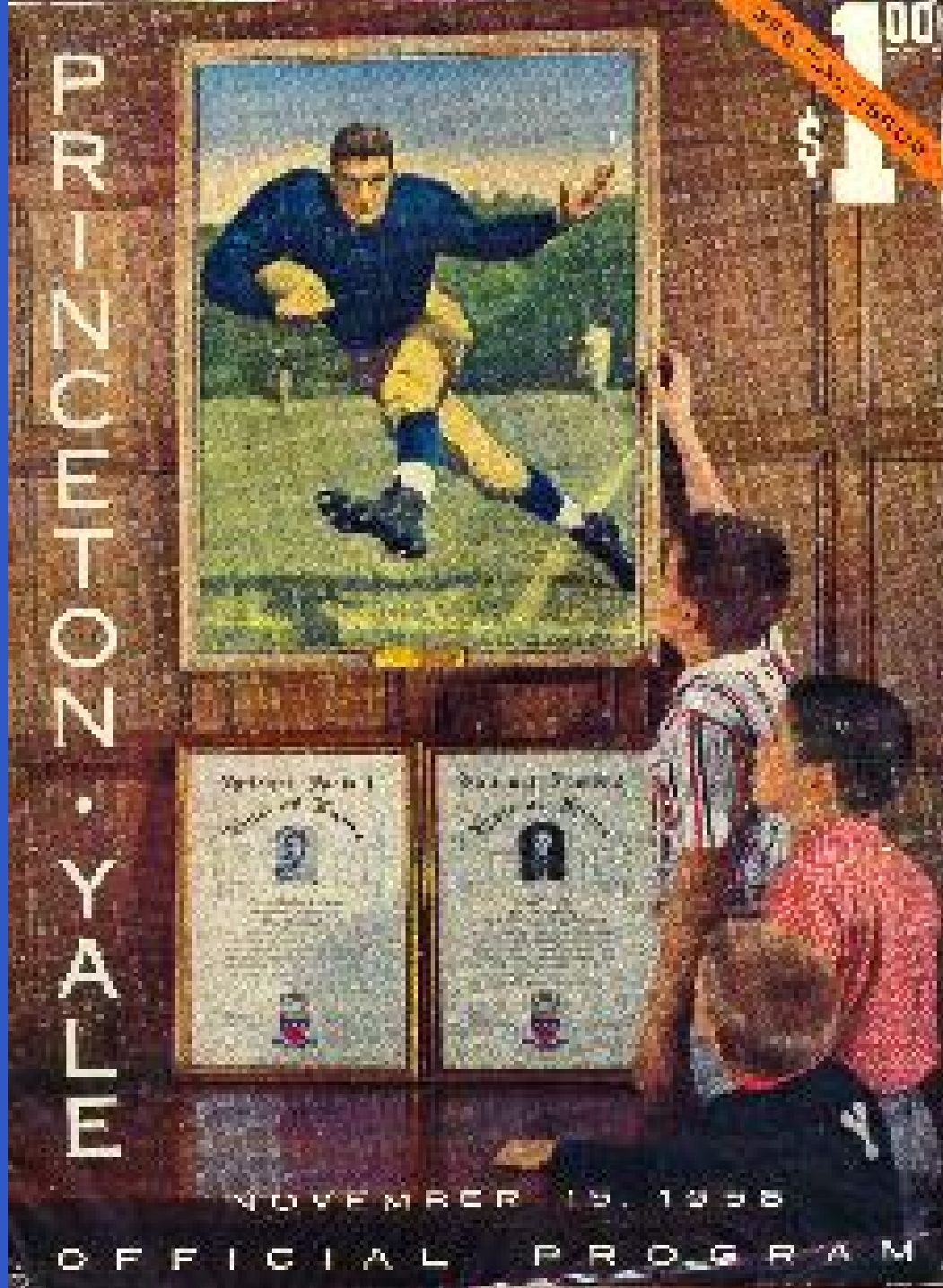
http://www.metallica.com/metdotcom/help/copyright_trademark.html

**EXIT LIGHT..ENTER NIGHT
BE EVIL**



METALLITANIC
000







File-Sharing Application

Name	Size	Copyright
Volcano Red	5MB	© All Rights Reserved
Lady Volcano	6MB	© All Rights Reserved
Volcano Love	5MB	CC Some Rights Reserved
Raging Volcano	4MB	© All Rights Reserved
Volcano Blues	8MB	© All Rights Reserved

Search

Volcano

ITS Academic Computing System (ACS) Pantheon

Anatomy of an incident

"Minerva" October 14 1997 "Break-In"

Incident Handling

ITS ACS Aleks Margan notices break-in.

Aleks pages the Univ. ISO via beeper.

- We investigate.
- We assess damage.
- We determine only one machine affected.
- We plan shutdown and swap with fresh "hot spare" system.
- We contact ITS Dir.

We shut down Minerva and swap in a freshly installed "hot spare" machine as Minerva.

- We meet with ITS TP & ACS directors.
- We decide to shut the Banner student Web.
- We decide to force a password change.
- We prepare a statement.

We shut down the "Banner" student information system Web interface.

- Users logging in on the Pantheon & Yale Web server are prompted to change their password.
- We force students who login to change their passwords in two weeks.
- Other users (E-Mail) are given a grace period.

Aftermath

ISO dissects attack during the night of 10/14-15.

Prepares CERT & YaleCERT reports.

- Minerva infosec audit.
- Evidence of intruder sessions (w/accounts & programs and source of attacks) found in logs.
- Log files secured.
- Press releases to and interviews with Yale Daily News and Yale Herald.

Pantheon Security Review and Prevention Steps

- Solaris OS patch procedure audited & reviewed.
- Tripwire software specified and installed on Pantheon systems.

Follow Through Actions

- Yale Police notified. They contact FBI.
- Other Internet sites & Yale admins notified.
- Offending network's IP address blocked.
- Banner student system re-enabled.
- Pantheon Kerberized login and E-Mail access to be promoted in 1998 (encrypted auth & data).

Initiatives

Ranked by Priority

A

Administrative Systems

Project X Security Design

Firewall Access to Servers from Intra- & Internet

Non-Project X Security Design

- YHP & YSM IDX
- Telecom

Secure Access to Servers by Staff and Vendors

Server Security Standards

- Physical
- Hardware
- Software
 - OS
 - App Encrypt

Business Continuity Planning and Auditing

Std Policies & Procedures

- Password

B

Academic Systems and Data Network

Internet Border & Physical Intranet Security

Increase Security Awareness

- E-Mail
- Network

Secure Access to Systems by Staff and Users

Server Security Standards

- Physical
- Hardware
- Software
 - OS
 - App Encrypt

Business Continuity Planning and Auditing

Std Policies & Procedures

- Password

C

Desktops & Depts Campus-wide

Increase Security Awareness

- E-Mail
- Network

Secure Access to Systems by Staff and Users

Server Security Standards

- Physical
- Hardware
- Software
 - OS
 - App Encrypt

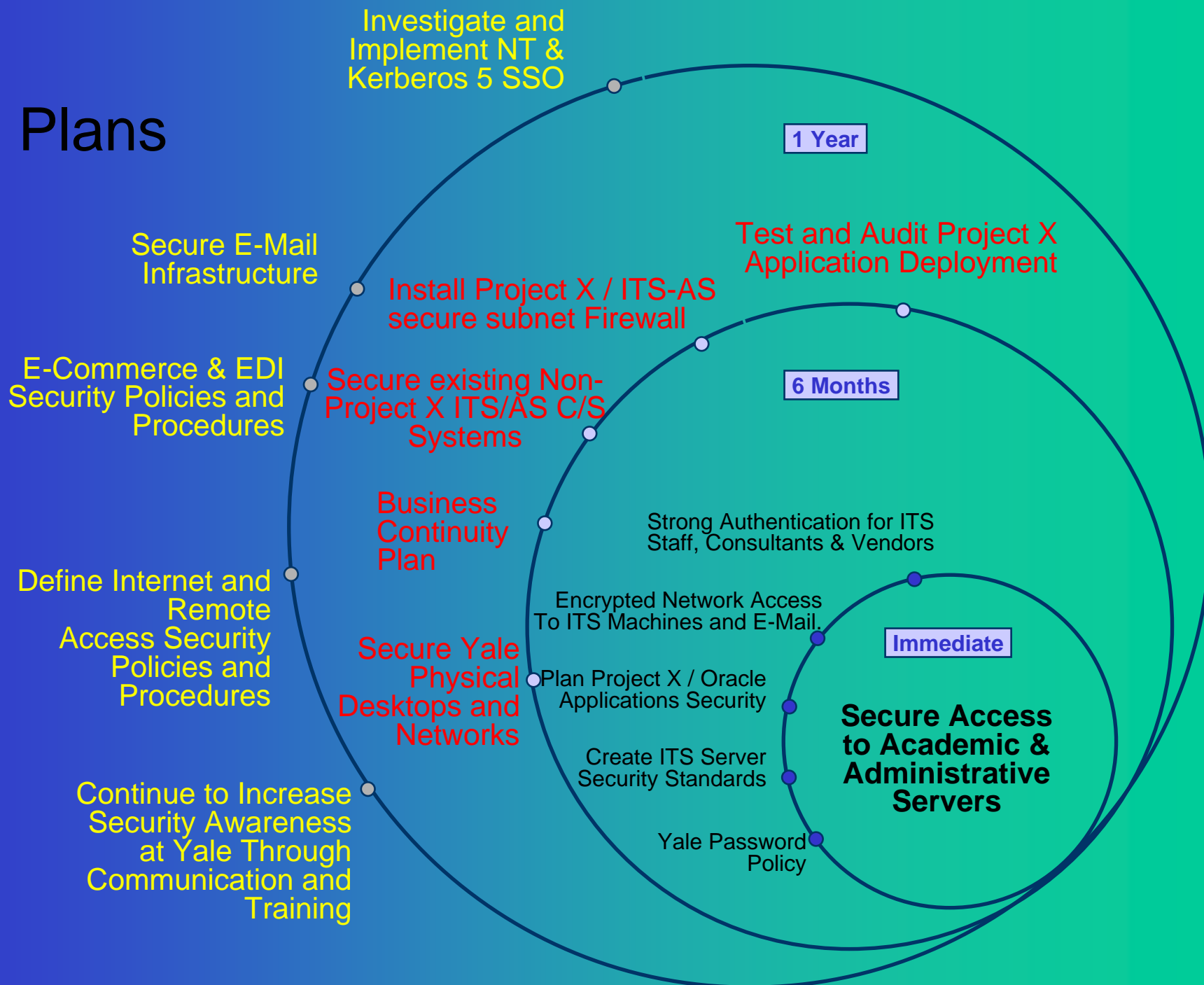
Business Continuity Planning and Auditing

Std Policies & Procedures

- Password

Yale Information Security

Plans



Information Security At Yale

Information Security is responsible for:

- Network monitoring with regard to security (scanning, flow monitoring).
- Investigations: compromise, harassment, denial of service attacks, forensics.
- Providing information about vulnerabilities, patches, viruses and worms.
- PIX firewall configuration and management.
- Content switch management.
- Yale community Information Security education.
- Enterprise security tools management: PGP, Norton Anti-Virus.
- Security Architecture evaluation and enhancement.
- Security policy development.
- Certificates (Verisign, Yale self-signed web and identity certificates).
- DMCA complaint processing and forwarding.
- Departmental/HIPAA/GLBA security audits and risk analysis.

Information Security At Yale

How we know what's up:

- We analyze our snort and firewall logs every day.
- We can see all the DNO monitoring tools and we can look at traffic to specific machines or ports at our “front” connections.
- We scan the enterprise for vulnerabilities.
- We get complaints from other institutions about attacks from Yale student machines.
- Students and staff call us when they notice something weird.
- We get DMCA complaints, warrants and subpoenas.
- The Police/FBI give us a call.

Outline

- Introduction -- Yale Information Security
- Background on Yale University, IT AND Computing Environments
- Key Issues, Axioms and “Lessons Learned”
- Rollout Issues
- Real World (Yale) Security Case Studies
- Conclusion

Background on Yale University

- 20,000 NetIDs (Yale Kerberos/NT Accounts)
- 10,000 students (5,000 undergrad)
- 10,000 employees (faculty and staff)
- \$7.2 billion endowment due to alumni and shrewd investments (\$3.5 billion in 1994).
- 200+ buildings.
- Medical school is 40% and self-sufficient.
- Major employer in City of New Haven.

Yale Univ. Net/Computing Environ

- 16,000+ IP addresses, 300+ Web servers
- 2 Public Class B networks (128.36, 130.132) and several Class C networks.
- 350+ subnets (300 10 mbits, 50 100 mbits)
- 100 mbit switched/routed backbone -> gbit Enet
- 10 megabit/second commercial Internet (TCG/Cerfnet). Soon to be 15 mbits/sec.
- 45 megabit/second Internet2 via vBNS (to be 155 megabits/second via Qwest)
- Used to be heavily Macintosh, now heavily Windows NT on administrative desktops.

Background on Yale University IT Organization (ITS)

- 350+ Employees
- 24x7 Professional Production environment (Administrative, E-Mail, Web, etc.)
- Legacy Mainframe transition to “client/server rightsizing Y2K business-re-engineering” Big Bang : *Project X*
New Oracle Financials and Data Warehouse
 - AP/PO, GA/GL, HR/LD, Data Mart/Mining
- SCT Banner, Telecom, IDX, MPAC

Yale University IT Org (ITS)

ITS Director Phil Long

- Univ. Information Security Officer and Office
- Administrative Systems
- Academic Media and Tech (formerly ACS)
 - includes A/V, Language Labs, etc.
- Data Network Operations
- RIS (merged Repro and Printing)
- Support
 - Desktop, Help Desk, Store, Training, User Accounts
- Technology and Planning
- Telecom (includes CATV)

Yale University IT Org (ITS)

- Almost all ITS subunits are standalone charge-back units (but not Information Security)
- All students are charged a yearly \$200 for:
 - 10 megabit Ethernet jack in dorm room
 - Phone in room.
 - CATV in room.
- Most faculty and staff have a Windows NT PC (Pentium 200, 64MB RAM) on 10BaseT. Approx \$16 to \$25 monthly.

Yale ITS Administrative Client Computing Environment

ADSM

Meeting Maker

Central E-Mail: Pine, Eudora, POP, IMAP

Norton Anti-Virus

Oracle Financials, Oracle Express, OFA, Brio

Kerberos 4, NT 4 (incl. Academic lab PCs)

Static and DHCP (including roaming) IP addr.

Netscape Communicator 4.7

Hummingbird Host Explorer w/Kerberos

Yale ITS Administrative Server Computing Environment

ADSM

Norton Anti-Virus on NT

Oracle 7, 8

AIX 4.3.*, Solaris 2.X, NT 4 w/SP5

SSH, FTP over SSL on AIX, Sun servers

PCAnywhere32 v8 on NT 4 Servers

Netscape Enterprise Web servers on Unix

IIS 3.0 and 4.0 Web servers on NT 4

Oracle (Application) Web servers (Spyglass)

Yale ITS Administrative Server Computing Environment

- Legacy Mainframe - Y2K move to new mainframe
- 25+ IBM RS/6000s (including 2 12 CPU S-70s with several GB RAM and other hi end)
- 25+ IBM PC Servers (several hi end with GB RAM)
- 4 Sun Ultra Enterprise Servers for general timesharing (primarily terminal-based Email)
- 4 Sun Ultra Enterprise POP/IMAP servers
- 10+ Web servers (incl www.yale.edu mirror)
- Redundancy & H/A, DR, Load Balancing Impl.

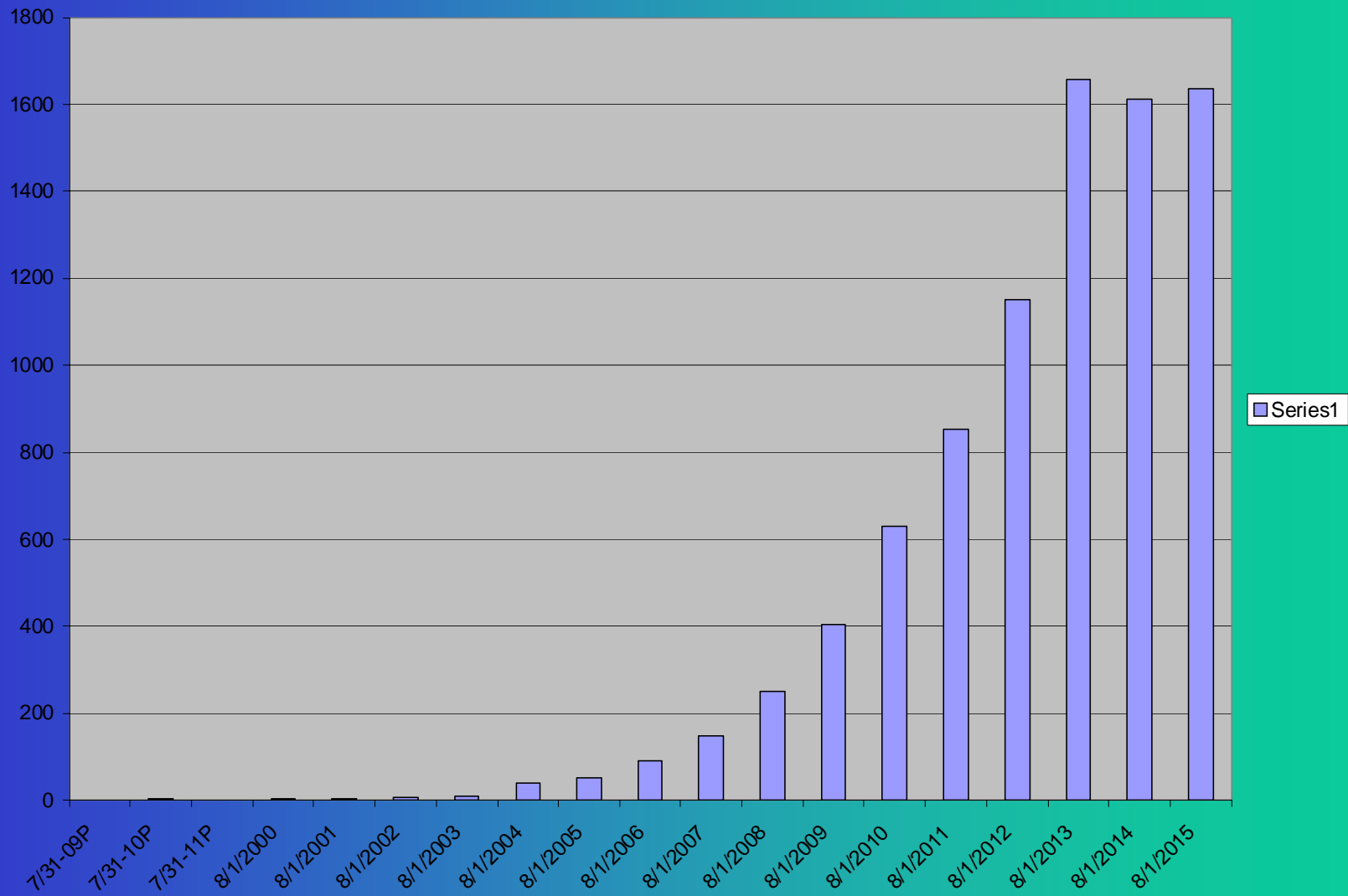
Yale

- Layered approach:
 - Blocked a few ports at campus border in 92, lpr in 2K, NetBIOS in 01, SQLserver in 02.
 - Internal use of firewalls.
 - Add'l use of RFC1918 networks.
 - Some use of VLANs (e.g. for wireless).
- Proactive Scans w/ISS & Nessus.
- Snort IDS at Internet border and internal choke points (custom bidirectional rules).
- Cisco VPN server(s) on campus.
- Packeteer™ inline for bandwidth mgt at Internet border.

Viruses / Worms, NetSec and Reaction

- 1988 RTM Jr. (1988)
- 1998 Melissa/ILOVEYOU
- 2000 Web and Lpr/lpd worms
- 2001 CodeRed 1 & 2, NIMDA (2001)
- 2002 “Slapper” (A/B/C) Apache SSL Worm
- 2003/2 SQL Slammer / Sapphire
- 2003/6 BugBear
- 2003/8 Stealthier / Blaster

CodeRed Worm 1st Activation



Internet Security History & HE IT

- 1986 – Major NSF funding for national backbone & regional supercomputer centers
- 1988 – Robert Morris & the Internet Worm
- 1988 – Creation of CERT at CMU
- 1989 – The Cornell Commission report
- 1989 – Clifford Stoll's *The Cuckoo's Egg*
- 1991 – CIX, commercial use, & Gopher

Internet History, cont'd

- 1993 – Mosaic browser released by UIUC
- 1993-4 ISP Sniffing attacks (PANIX, NearNet)
- 1994-5 Kevin Mitnick demos TCP Hijacking.
- 1995 – National backbone privatized
- 1995 – SATAN released by Farmer & Venema
- 1996 – PANIX, Internet Chess Server, and other web sites shut down by SYN attacks.
- 1996 – Internet 2 consortium formed

2000-2001 Academic InfoSec

- Feb – Distributed Denial of Service (DDoS) attacks bring down key .COM sites; university sites implicated (UC Davis, UCLA, Stanford, etc.)
- June – SANS Top Ten list released.
- June-July – Univ. of Washington Medical Center intrusion. 4000 medical records involved. No firewall protecting server.
- Feb 2001 – Indiana University Bursar server with anon FTP enabled and student records.
- March – 40+ E-Commerce NT/IIS servers hacked from E. Europe. Credit card #s. FBI NIPC alert.

Higher Education Computer Security 2000-2003

- Hacker Steals Personal Data on Foreign Students at U. of Kansas
Chronicle of Higher Education, 1/24/2003
- UMBC students' data put on Web in error *Baltimore Sun*, 12/7/2002
- Why Was Princeton Snooping in Yale's Web Site?
Chronicle of Higher Education, 8/9/2002
- Delaware Student Allegedly Changed Her Grades Online
Chronicle of Higher Education, 8/2/2002

. . . 2000-2003

- Russian Mafia May Have Infiltrated Computers at Arizona State and Other Colleges
Chronicle of Higher Education, 6/20/2002
- Hacker exposes financial information at Georgia Tech
ComputerWorld, 3/18/2002
- College Reveals Students' Social Security Numbers
Chronicle of Higher Education, 2/22/2002
- Hackers Use University's Mail Server to Send Pornographic Messages
Chronicle of Higher Education 8/10/2001

. . . 2000-2003

- Review to ensure University of Montana Web security
Montana Kaimin, 11/14/2001
- ‘Code Red’ Worms Linger
Chronicle of Higher Education, 9/14/2001
- Students Fault Indiana for Delay in Telling Them About Stolen Files
Chronicle of Higher Education, 3/16/2001

. . . 2000-2003

- [UWashington] Hospital records hacked hard
SecurityFocus.com, 7/12/2000
- 3 Universities in California Find Themeselves
Linked to Hacker Attacks
Chronicle of Higher Education 2/25/2000
- Hackers Attack Thousands of Computers on at
Least 25 U.S. Campuses
Chronicle of Higher Education, 3/13/1998
- UT Austin: 55,000 SSNs and Personal Records
'data mined' by intruder
- Princeton University:

2001-2003 Worms

- 2001: CodeRed, CodeRed II, NIMDA Worms
- 2002: “Slapper” (A/B/C) Apache OpenSSL Worm
- 2003: SQL Slammer / Sapphire Worm

The Current Situation

- The Internet is a world-wide, increasingly mission-critical infrastructure
- Internet's underlying structure, protocols, & governance are still primarily open
- Many vendors ship systems w/ insecure configs (NT, Linux, W2K, Unixes, IIS)
- Massive CPU power & bandwidth available to crackers as well as scientists, e-commerce
- Many college & university networks are insecure

Information Security in HE

- Research universities: deployment of workstations & servers by researchers whose talents are usually focused elsewhere
- Smaller institutions: dearth of tech skills
- Dorm networking: little adult supervision
- Too few security experts; weak tools; most institutions have no InfoSec office.
- Few policies regarding systems security

Information Security in US HE

- 3500+ Colleges and Universities
- > 1000 Community colleges
- < 100 major research universities
- 125+ University Medical Schools
- 400 Teaching Hospitals
- 150+ Institutional members of Internet2

Targets of Opportunity on US HE Computer Networks

- Sensitive Data
 - Credit Card #s, ACH (NACHA) bank #s
 - patient records (SSN)
 - student records (SSN)
 - institution financial records
 - Investment records
 - donor records
 - research data

Why US HE Computer Networks are attractive targets

- Platforms for launching attacks
 - Wired dorms (insecure Linux PCs, PC Trojans)
 - High bandwidth Internet (Fract T3, T3, T3+)
 - High computing capacity (scientific computing clusters, even web servers, etc.).
 - “Open” network security environment (no firewalls or only “light” filtering routers on many high bandwidth WANs and LANs)
 - Trust relationships between departments at various Universities for research (e.g. Physics)
 - Univ research lab computers are often insecure and unmanaged.

Unique Challenges to implementing Information Security in Higher Ed

- Academic “Culture” and tradition of open and free networking
- Lack of control over users
- Decentralization (no mainframe anymore)
- Lack of financial resources
- Creative Network Anarchy – anyone can attach anything to the network
- IT has not always been central to institutional mission -- changing attitudes and getting “buy in” requires politics and leadership.

What should US HE IT be doing W.R.T. Information Security

- Investigating network security methods.
- Investigating strong authentication methods (e.g. smart cards, tokens).
- Evaluating “best practices” in:
 - Higher Education
 - Corporations
 - Government
 - Military
- Developing common recommended policies.

Trends in Academic InfoSec

- E-Commerce site threaten litigation against future DDoS sites. Liability for negligence?
- Insurance companies begin to rewrite liability policies, separate 'cyber' policies to require info security vulnerability assessments & changes.
- Funding agencies to require firewalls, security?
- HIPAA is a "forcing function" in academic Medical Centers.
- FERPA, COPPA, DMCA, Privacy legislation.
- If HE InfoSec doesn't improve, will more federal legislation be far behind?

InfoSec Trends Elsewhere

- Some of the K-12 school system networks are the only sites (in the US) which have worse network and system security than .EDU sites.
- Information security at State gov. agencies and municipal governments is a mixed bag.
- Outside US some academic institutions are more tightly controlled (e.g. Internet access is severely restricted), some not.

InfoSec Trends Elsewhere

- .MIL sites take steps to secure data and servers (Mac web servers, data isolation/classification). Broke initial ground in IDS (Intrusion Detection Systems).
- .GOV – NIST has released draft guidelines/recommendations for info security to be implemented at Federal Government agencies.

InfoSec Trends Elsewhere

- .COM sites – Some web sites have poor security (even those outsourced), some (e.g. financial) strive to be state of the art.

- Insurance/auditors requiring security assessments for policies.

- BS 7799 / ISO/IEC 17799-1 InfoSec Mgt stds

- CISSP / CISA / SANS GIAC / Vendor (Microsoft/Cisco/Checkpoint) certifications of Information Security personnel

Corporate InfoSec Trends,

(relatively rare in US HE)

- Firewalls, proxies, user access control
- Network monitoring, bandwidth management
- Extensive logging, logfile analysis
- IDS – Intrusion Detection Systems
- VPNs (Virtual Private Networks)
 - PPTP, L2TP, IPSEC
- Strong Authentication – PKI, Smartcards
- Vulnerability scanning (internal, external)
- Change Control / Management
- Managed Security Services (e.g. outsourced)

Why should higher ed care?

- Improperly secured computers and networks present considerable institutional risk and can impact ability to achieve mission
- Improperly secured college and university IT environments can cause harm to third parties, including gov't and industry, and create liability

Higher Ed and Cybersecurity

- Education and Training
 - Centers of Excellence
 - Professional Training and Certification
- Research and Development
 - Cyberinfrastructure
 - Basic and Applied Research (DARPA, NSF, etc.)
- Securing Our Corner of Cyberspace!