Security/ Privacy: Building Public Confidence in Electronic Transactions

A Presentation by Idaho’s Two National Centers of Excellence
Why are your Universities here?

*America’s New Deficit* drew attention to the significant decline (more than 40 percent between 1986 and 1994) in bachelor’s degrees awarded in computer science. Recent data indicates that the decline has come to a halt, and there has been modest but steady growth in the number of computer and information sciences bachelor’s degrees awarded between 1993 and 1996, rising from a ten-year low of 26,338 in 1993 to 26,837 in 1996 (see Figure 15). In addition, there is evidence to support the prospect for rapid growth in the number of bachelor’s degrees awarded in computer science and computer engineering.

Contrary to the precipitous decline in bachelor’s degrees in the late 1980s, the number of associate (Figure 10, see page 33) and master’s degrees (see Figure 16, next page) awarded in information technology grew moderately between 1987 and 1996, while the number of doctoral degrees more than doubled (431 in 1987 to 950 in 1996, though the 1996 figure represents a drop from 1,024 in 1995) (see Figure 17, next page).

ONLY 10 PhDs in Direct Information Assurance Areas
There is nothing to worry about

- This is one approach to the problem
JUST HACKED:
- www.china.com
- www.zapnow.com
- www.linux.org.mx
- www.affiliatedrecords.com
- www.mxcert.org.mx
- www.alaramx.com.mx
- www.cruzoja.org.mx
- www.oceanica.com.mx
- www.carnaval.com.mx
- www.mazcity.com.mx
- www.exxor.com.mx
- www.bandaelrecodo.com.mx
- www.ibalpe.com.mx
- www.haciendadelmar.com.mx
- www.lasflores.com.mx
- www.grupotecnia.com.mx
- www.mazatlangolfking.com.mx
  www.yellowpages.ca, www.sprint.net,
  www.cs.purdue.edu, www.playboy.com,
  www.hornyrob.com

April Fools!
Not every hacked web site is really a hacked web site, as many of us recently learned.

NOT HACKED:
- movies.go.com
- www.simcity.com
- www.artbell.com
- security.pine.nl
- Hacker News
  - White House
  - Kipling
  - MTV

Microsoft HACKED?
We should not do anything on the Internet!

♦ Progress Stops
Where are Computer Systems Vulnerable?

Here.

1. Hardware
2. Software
3. Data
4. Communications
5. PEOPLE
Good News

Sound Management
Risk Management
Awareness
Training
Education
Good Practices

All Address The Problem
They Are Effective Countermeasures
Bad News

Security system failures have been with us since there were systems of any kind to secure.

*It is important to realize that there will be failures and plan for contingencies.*

Washington Post
March 30, 1996
FACT 1

TOPICS

♦ COMPUTERS ARE CRITICAL TO FULFILL YOUR AGENCY MISSION!

Oil & gas delivery & storage
Telecommunications
Electric power
Transportation
Banking & finance
Water
Emergency services
Government services
FACT 2

♦ THERE ARE DEFINED THREATS TO YOUR COMPUTER SYSTEM!

“A highly computerized society like the United States is extremely vulnerable to electronic attacks from all sides. This is because the U.S. economy, from banks to telephone systems...relies entirely on computer networks.” —Foreign Government Newspaper

<table>
<thead>
<tr>
<th>National Security Threats</th>
<th>Insiders</th>
<th>Outsiders</th>
</tr>
</thead>
<tbody>
<tr>
<td>Info Warrior</td>
<td>Reduce U.S. Decision Space, Strategic Advantage, Chaos, Target Damage</td>
<td></td>
</tr>
<tr>
<td>National Intelligence</td>
<td>Information for Political, Military, Economic Advantage</td>
<td></td>
</tr>
<tr>
<td>Shared Threats</td>
<td>INSIDERS</td>
<td>OUTSIDERS</td>
</tr>
<tr>
<td>Terrorist</td>
<td>Visibility, Publicity, Chaos, Political Change</td>
<td></td>
</tr>
<tr>
<td>Industrial Espionage</td>
<td>Competitive Advantage</td>
<td></td>
</tr>
<tr>
<td>Organized Crime</td>
<td>Intimidation</td>
<td></td>
</tr>
<tr>
<td>Local Threats</td>
<td>Revenge, Retribution, Financial Gain, Institutional Change</td>
<td></td>
</tr>
<tr>
<td>Institutional Hacker</td>
<td>Monetary Gain</td>
<td></td>
</tr>
<tr>
<td>Recreational Hacker</td>
<td>Thrill, Challenge, Prestige</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Thrill, Challenge</td>
<td></td>
</tr>
</tbody>
</table>
FACT 3

♦ COMPUTER SYSTEMS ARE VULNERABLE!

♦ THREATS BY PEOPLE
  – Unintentional Actions => 50-60%
  – Intentional Actions => 15-20%
  – Outside Actions => 1-3%

♦ PHYSICAL and ENVIRONMENTAL THREATS
  – Fire Damage => 10-15%
  – Water Damage => 1-5%
  – Natural Disaster => 1%
FACT 4

COMPUTER SECURITY IS ESSENTIAL TO PROTECT YOUR SENSITIVE INFORMATION!
FACT 5

♦ RISK MANAGEMENT IS AN EXECUTIVE RESPONSIBILITY!
FACT 6

♦ COMPUTER SECURITY AWARENESS AND TRAINING PROGRAMS REDUCE RISK!
FACT 7

♦ A COMPUTER SECURITY PLAN IS AN EFFECTIVE EXECUTIVE TOOL

<table>
<thead>
<tr>
<th>Executive Summary</th>
<th>V. System Audit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table of Contents</td>
<td>A. Manual</td>
</tr>
<tr>
<td>I. Introduction</td>
<td>B. Automated</td>
</tr>
<tr>
<td>A. General</td>
<td>VI. Media and Hdw Control</td>
</tr>
<tr>
<td>B. Security Management</td>
<td>A. Control and Accountability</td>
</tr>
<tr>
<td>C. System Overview</td>
<td>B. Sanitization</td>
</tr>
<tr>
<td></td>
<td>C. Maintenance</td>
</tr>
<tr>
<td>II. Computing Facility</td>
<td>VII. A. Concept of Ops.</td>
</tr>
<tr>
<td>Description/Configuration</td>
<td>B. Duties</td>
</tr>
<tr>
<td>III. System Description</td>
<td>C. Virus Protection</td>
</tr>
<tr>
<td>A. System Configuration</td>
<td>VIII. Policy</td>
</tr>
<tr>
<td>B. Hardware Description</td>
<td>A. Introduction</td>
</tr>
<tr>
<td>C. Software Description</td>
<td>B. Applicable Documents</td>
</tr>
<tr>
<td>IV. System Accesses and Ops.</td>
<td>C. Compliance</td>
</tr>
<tr>
<td>A. System Access</td>
<td>IX. Documentation &amp; Training</td>
</tr>
<tr>
<td>B. System Preparation</td>
<td>A. Documentation</td>
</tr>
<tr>
<td>C. Data Process</td>
<td>B. Security Training</td>
</tr>
<tr>
<td>D. Mode Termination</td>
<td></td>
</tr>
</tbody>
</table>
Risk Management

Risk = Threat X Vulnerability — Security
What is “Security”? 

♦ To decide whether a computer system is “secure”, you must first decide what “secure” means to you, then identify the threats you care about.

- Cyberterrorism
- Espionage
- Equipment Theft
- Denial of Service
- Modified Databases
- Virus
- Identity Theft
Current Incidents

Contacted 3 American youth to help infiltrate computers in U.S.

Used internet to break into
  – Pentagon
    • (During Op Prep)
  – U.S. Universities
  – Own Country

Arrested/Trial Pending
  – In Israel
Current Issues

Confidentiality

Integrity

Availability

Biographical Data

Payroll Data

Health Data

Packet Switch

File Server

Gateway

Other Networks
Current Issues
Confidentiality, Integrity, Availability

Confidentiality

Integrity

Availability
Current Issues
Data Aggregation and Sensitivity

- Biographical Data
- Payroll Data
- Health Data
Current Issues  Common Misconceptions

- Computer Security Deters Only Criminals
- Implementation and Costs are Prohibitive
- No One Cares
- Firewall, I don’t need no stinking firewall
- Virus Protection is the Key
- Once Secure — Always Secure
- Encryption Is The Solution
Who can attack a computer system?

It comes down to access. If there is any kind of access, the system might be vulnerable to misuse of that access.

Of course, if there is no access, the computer isn’t much use!
F.B.I. STATISTICS

♦ Computer Crime:
  – 1% is detected.
  – 7% of the detected crimes are reported.
  – 3% result in jail sentence.
  – Jail sentences are short term
  – 75% increase per year in computer intrusions.
  – 36% increase in Computer crime
  – Very little physical harm risk
HOW IT COMPARES?

- Avg. Bank Robbery $2,500
- Avg. Bank Fraud $25,000
- Avg. Computer Crime $500,000

♦ Computer Crime Loss:
  • $5 - $10 BILLION annually.
The Financial Stakes Are High

Applicable Federal Statutes

♦ Public Law 97-255
  – Federal Managers Financial Integrity Act of 1987
♦ Public Law 98-473
  – Comprehensive Crime Control Act of 1984
♦ Public Law 99-474
  – Computer Fraud and Abuse Act
♦ Public Law 99-508
  – Interception or Disclosure of Wire, Oral or electronic Communications
♦ Public Law 100-235
  – Computer Security Act of 1987
♦ Public Law 100-503
  – Computer Matching and Privacy Protection Act
What do you do if you find a problem?
Information Assurance Countermeasures Triad

Fundamentally, only THREE countermeasures available to protect infrastructure.
There are a number of technologies which can be used to help implement your security policy.

Of course, none of them are perfect.
Passwords

♦ We have met the enemy and he is us
  – Post-it Note Syndrome
  – “Too Many Passwords”
  – Rotating names
  – Bad password choices
BioMetrics Solutions

- Face recognition
- Fingerprints
- Voice recognition
- Retinal scans

State of Connecticut is using this to help in Fraud detection

Pics from PC magazine
Principles of Perimeter Defense:

♦ Watch Your Boundaries (all of them!)
Styles of Firewalls and VPNs
Watch Out For Intruders

♦ Why do Intrusion Detection at all?
– **Second line of defense.** Even the best intrusion detection system can fail. Many intruders are insiders.
– **Ejection.** Catch intruders before they can do much damage.
– **Deterrent.** Intruders may stay out if they think they'll be caught.
– **Educational.** Learn how intruders do what they do and use this to improve both prevention and detection techniques.
Data only a specialist could love

...
FedEx | Registration has the following structure:


**Form 1:**
- Action URL: [https://www.fedex.com/cgi-bin/us-acct-reg.cgi](https://www.fedex.com/cgi-bin/us-acct-reg.cgi)
- Encoding: application/x-www-form-urlencoded (default)
- Method: Post

**NetSite:** [https://www.fedex.com/us/registration/account.html](https://www.fedex.com/us/registration/account.html)

**File MIME Type:** text/html

**Source:** Currently in memory cache

**Local cache file:** none

**Last Modified:** Wed, Feb 4, 1998 8:57:59 AM Local time

**Last Modified:** Wed, Feb 4, 1998 4:57:59 PM GMT

**Content Length:** 14482

**Expires:** No date given

**Charset:** Unknown

**Security:** This is a secure document that uses a medium-grade encryption key suited for U.S. export (RC4-40, 128 bit with 40 secret).

**Certificate:**

<table>
<thead>
<tr>
<th>This Certificate belongs to:</th>
<th>This Certificate was issued by:</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.fedex.com">www.fedex.com</a></td>
<td>Secure Server Certification Authority</td>
</tr>
<tr>
<td>SAC</td>
<td>RSA Data Security, Inc.</td>
</tr>
<tr>
<td>Federal Express</td>
<td>US</td>
</tr>
<tr>
<td>Memphis, Tennessee, US</td>
<td></td>
</tr>
</tbody>
</table>


**This Certificate is valid from Tue Jul 29, 1997 to Wed Jul 29, 1998**

**Certificate Fingerprint:**

Certificates and Keys

This Certificate belongs to:
Deborah A. Frincke
frincke@cs.uidaho.edu
Digital ID Class 1 - Netscape
www.verisign.com/repository/CPS Incorp. by Ref., LIAB, LTD(c)(c)96
VeriSign Class 1 CA - Individual Subscriber
VeriSign, Inc.
Internet

This Certificate was issued by:
VeriSign Class 1 CA - Individual Subscriber
VeriSign, Inc.
Internet

This Certificate is valid from Mon Feb 09, 1998 to Fri Apr 10, 1998
Certificate Fingerprint:
Comment:
This certificate incorporates the VeriSign Certification Practice Statement (CPS) by reference. Use of this certificate is governed by the CPS.

The CPS is available in the Verisign repository at:

OK
Secure Development
MALICIOUS CODE

- Trapdoors
- Trojan Horses
- Bacterium
- Logic Bombs
- Worms
- Virus
“The greatest threat you face is not the viruses or the hackers or the whatever, but rather complacency.”

Michael Tucker, Editor, SC Magazine, Sep 99
VIRUS GROWTH

♦ 1988 - Less than 10 known viruses
♦ 1990 - New virus found every 2 days
♦ 1993 - 10 to 30 new viruses per week
♦ 1999 - 45,000 + viruses and variants*

* Source: Mc Afee
“Packaging” of Virus Detection

♦ Online services which will “detect” and “clean” your site are becoming more common. One example is the McAfee online “clinic” for detection of viruses.
  – Downloads software and signatures for scan
  – Subscription-based
Virus SWAT Teams??

♦ There are a number of organizations which include individuals and/or teams who specialize in virus management, particularly identification and removal. The response time and size (and cost) of these teams differs. A recent CNN article referred to these as “Virus SWAT Teams” *(Security elite form SWAT teams to attack viruses* by Matthew Nelson, CNN’s web site, 1/19/99)

♦ Examples:
  – Anti-Virus Emergency Response Team, Network Associates
  – Symantec’s Anti-Virus Research Center, Symantec
From Single DOS to DDOS

See source: www.hackernews.com/bufferoverflow/00/dosattack/dosattack.html
The Back Alleys of E-Commerce

♦ “All this talk of fifteen-year-old kids vandalising the Web is a smoke screen behind which dangerous, professional crackers are pleased to take cover”

♦ “The lure of big, fast-money scores in virtual commerce is making it common for skilled hackers to attack competitors in search of free intellectual property”

Mike Rasch, VP Global Security, testimony before the Senate Appropriations Subcommittee, February 2000 reported in The Register and online testimony transcript.
Threats to Personal Privacy

♦ Buying and selling confidential information from Social Security files.
♦ Browsing IRS files.
♦ Buying and selling bank account name lists.
♦ A Princeton University student stole ~1800 credit card numbers, customer names, and user passwords from an e-commerce site.

10., Washington Post, S. Barr, 2 Aug. 1993
(4) Freeh, Testimony 2000
CyberTerrorism

- The Internet Black Tigers conducted a successful "denial of service" attack on servers of Sri Lankan government embassies.
- Italian sympathizers of the Mexican Zapatista rebels attacked web pages of Mexican financial institutions.
- Rise of “Hack-tivism”

Freeh, Testimony before Senate, 2000.
PREVENTING VIRUS INFECTION

♦ Boot floppy based systems using a specific, clearly labeled boot diskette.
♦ Never boot a hard disk system from an unprotected diskette.
♦ Never use untested software (test off line or on a single purpose dedicated system).
♦ Backup files and programs, securely store and routinely check for infection.
♦ Minimize software sharing within the organization.
♦ Prohibit use of unapproved software from any source.
♦ Educate users to watch for changes in patterns of system activity.
♦ Install virus detection software.
Security Plan

♦ The Plan Must
  – Identify All Actions Needed To Implement Security Safeguards
  – Cite All Applicable Laws, Policies and Regulations
  – Describe Degree of Compliance With Regulations
  – Provide For A Review and Revision Process
# Security Plan

## Executive Summary

## Table of Contents

I. Introduction
   A. General
   B. Security Management
   C. System Overview

II. Computing Facility Description/Configuration

III. System Description
   A. System Configuration
   B. Hardware Description
   C. Software Description

IV. System Accesses and Ops.
   A. System Access
   B. System Preparation
   C. Data Process
   D. Mode Termination

V. System Audit
   A. Manual
   B. Automated

VI. Media and Hdw Control
   A. Control and Accountability
   B. Sanitization
   C. Maintenance

VII. A. Concept of Ops.
    B. Duties
    C. Virus Protection

VIII. Policy
    A. Introduction
    B. Applicable Documents
    C. Compliance

IX. Documentation & Training
    A. Documentation
    B. Security Training
Executive Action Items – Step 1

- Validate Number and Function of Systems
- Appoint Security ‘Officer’ To Each System/Network
- Assign Responsibility and Deadline for Documentation Package of Each System
Executive Action Items – Step 2

♦ Appoint Program Manager
♦ Determine Boundary For Each System/Network
♦ Assign Responsibility For Evaluation
♦ Develop Security Policy For Each System/Network
♦ Assign Organizational Responsibility To:
  – Security Tasking
  – Configuration Management Tasking
  – Mission and Function Tasking
Executive Action Items – Step 3

♦ Prepare Program Management Plan (Include Security Plan)
♦ Implement Security Policy
♦ Develop And Implement Risk Analysis
♦ Evaluate and Monitor Resource Expenditures
Why Are You Here –
Y’all add to the problem

Between 1983 and 1998, data from the Current Population Survey (CPS)—a joint project of the U.S. Departments of Commerce and Labor—shows the number of “computer systems analysts and scientists”—which includes computer engineers—and “computer programmers” soared from 719,000 to 2,084,000, an increase of 190 percent, more than six times faster than the overall U.S. job growth rate of 30.4 percent. Computer systems analysts and scientists have shown the most rapid growth, 433 percent, during this period. In contrast, computer programmers grew by 38.4 percent, much closer to the overall U.S. job growth rate (see Figure 2).

FIGURE 2. Employment in Core IT Occupations

University of State University
Two National Centers of Excellence

Corey Schou
Schou@mentor.net

Deborah Frincke
frincke@uidaho.edu

State University
Might Be A CRIMINAL’S BEST FRIEND

♦ The Internet offers:

– Little regulation.
– World exposure to potential victims.
– Easy to “pack up and change identity”
– Users for the most part trust each other.
– General attitude of Net users is minimum of control.
– New, “unsuspecting” users to prey on.
**Argentine Hacks Harvard - DoD**

**Landmark:** 1st Time Feds use court order to monitor private electronic communications.

1. Ardita uses PC & modem to crack Telecom Argentina, other Argentine Internet sites

2. Ardita hacks Harvard, thru Harvard to Internet systems around the world.

**Cracks -**
US, Brazil, Chile, Korea, Mexico, Taiwan

**Washington Post, March 30, 1996**
By Maryann Jones Thompson

- Time it took to register the first million domain names: four years.
- Time to move from 4 million to 5 million domain names: three months.
- Number of pages on the Web: 800 million.
- Web pages covered by the best search engine: 16 percent.
- 70 percent of global Web traffic goes to fewer than 4,500 sites.
- Ratings firms miss as much as 32 percent of Net traffic to large sites.
- Women online: 48 percent of surfers, up from 42 percent in 1996.
- Net homes watch 10 percent less TV than non-Net homes.
- Number of Web surfers in Japan: 8 million. In Latin America: 3 million.
- Americans are 44 percent of the Web population.

- 1.2 million surfers bought via a Web auction in 1998.
- $51 billion in 1998 offline spending was influenced by Net shopping.
- 14 percent of music will be sold online by 2003.
- Online prescription sales will hit $970 million in 2003.
- 25 million Web gamblers worldwide will produce $1.2 billion in revenues for online gaming sites.
- Online brokerages accounted for 14 percent of equity trades in Q4 1998.
- B-to-b sales of products and services online will grow from $131 billion this year to $1.5 trillion in 2003.
- The average e-commerce site costs $1 million and takes five months to develop.
- 32 percent of business travel ($38 billion) will be booked online by 2003. Insurance firms not selling online: 88 percent. Banks not offering online banking: 94 percent.
Electronic Communication

Intermediaries forward messages along the way, using the messages’ address to figure where it should go along the way.
You can combine Smart Cards With Nearly Anything.

Integrated Smart Cards

- A growing trend is to integrate smart cards with other technologies... so that the smart card is providing access to a particular transaction (such as secure payments), and may include other customer information as well. VISA/MOTOROLA have used this approach to better manage some credit cards (here's a snippet from their press release):

- ... Smartcards are plastic cards housing a 'smart' silicon chip with the power to store and process information. The Visa Stored Value smartcard is powered by Motorola's MSC0406 microcontroller, which offers 1K bytes EEPROM, 9K bytes ROM and 240 bytes RAM. The MSC0406 sells for $1.49 per 100,000 units... 12/97 Exopa Terra
The Changing Picture of Insiders

♦ The increasingly distributed nature of corporate resources, creates and expanded view of insiders

- Developers
- Testers
- Everyone who works in the development lab
- Staff working in the company
- Sales force
- Consultants
- Delivery/Transport
- Customer
- Customer’s insiders

♦ “There is no longer a clear distinction between insiders and outsiders, between a corporate ally and a corporate enemy. And preventing access is the exact opposite of what companies are trying to do.”

Beyond Computing, S. Dickey
Tracking the Internet Economy: 100 Numbers You Need to Know, Sept 13, 1999
[excerpts, see www.thestandard.com]

By Maryann Jones Thompson

Time it took to register the first million domain names: **four years.** Time to move from 4 million to 5 million domain names: **three months.**

Number of pages on the Web: **800 million.** Web pages covered by the best search engine: **16 percent.**

70 percent of global Web traffic goes to fewer than 4,500 sites.

Global Web population in 1998: **142 million.** In 1999: **196 million.** In 2003: **502 million.**

Women online: **48 percent** of surfers, up from **42 percent in 1996.**

Net homes watch **10 percent less** TV than non-Net homes.

Number of Web surfers in Japan: **8 million.** In Latin America: **3 million.**

Americans are **44 percent of the Web population.**

Global e-commerce spending 1998: **$50 billion.** 1999: **$111 billion.** 2003: **$1.3 trillion.**


14 percent of music will be sold online by 2003.

Tax-free online shopping's cost to state and local governments: **$170 million, or only 0.1 percent** of the tax base.
INTERNET “1999 User Estimates”

“Information Super Highway”

♦ 100 Million Users in United States Nielsen ratings 1999
  – 24% of internet users are in the education professions
♦ 286 Million Internet users Worldwide NETREE Internet Survey 1/98
♦ 56 Million hosts worldwide http://navigators.com