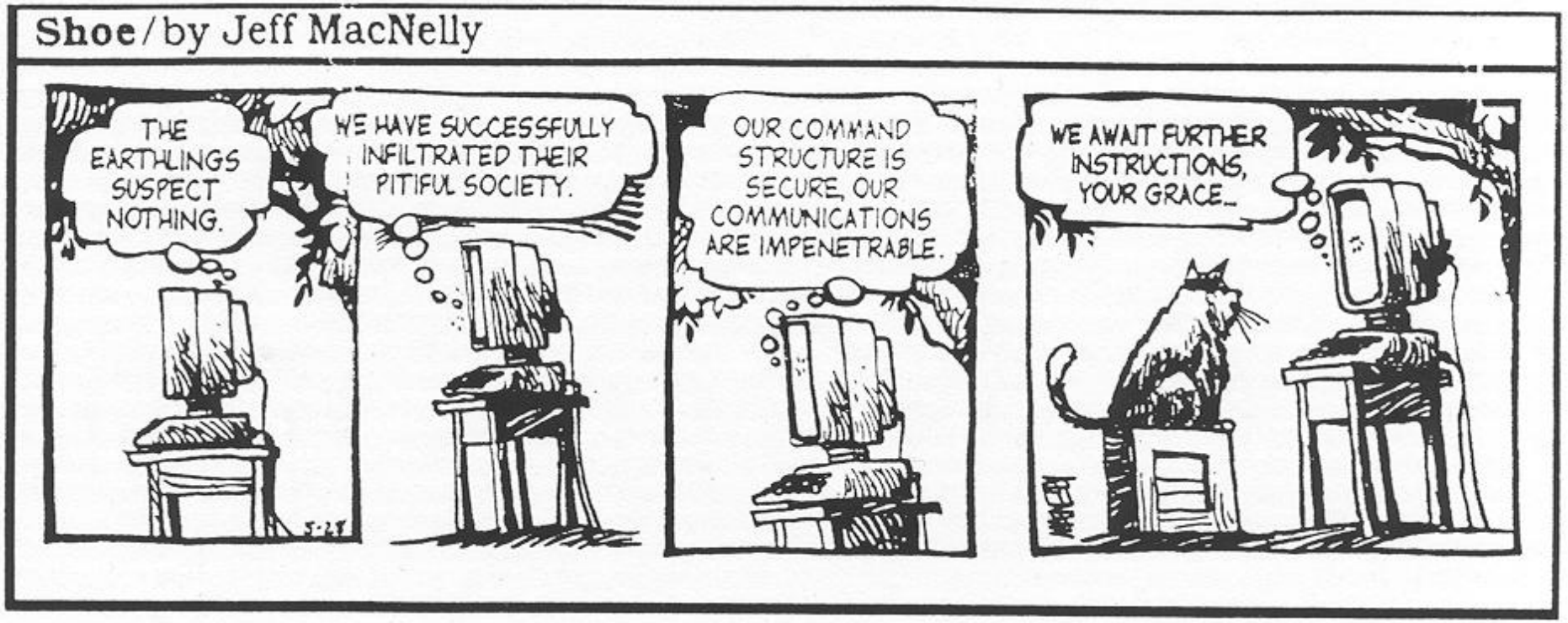
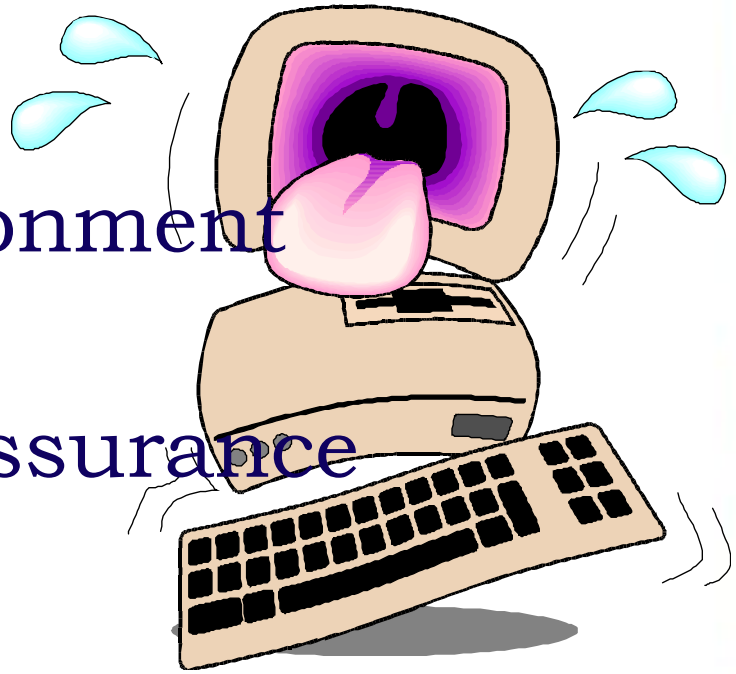
Information Assurance and Transportation

Presented to the
Midwest Transportation Consortium
18 January 2002

Kip Peters
Chief Information Security Officer
State of Iowa
515-725-0362
Kip.Peters@itd.state.ia.us
http://www.itd.state.ia.us/security/


Shoe / by Jeff MacNelly
THE EARTHLINGS SUSPECT NOTHING.
WE HAVE SUCCESSFULLY INFILTRATED THEIR PITIFUL SOCIETY.
OUR COMMAND STRUCTURE IS SECURE, OUR COMMUNICATIONS ARE IMPENETRABLE.
WE AWAIT FURTHER INSTRUCTIONS, YOUR GRACE...

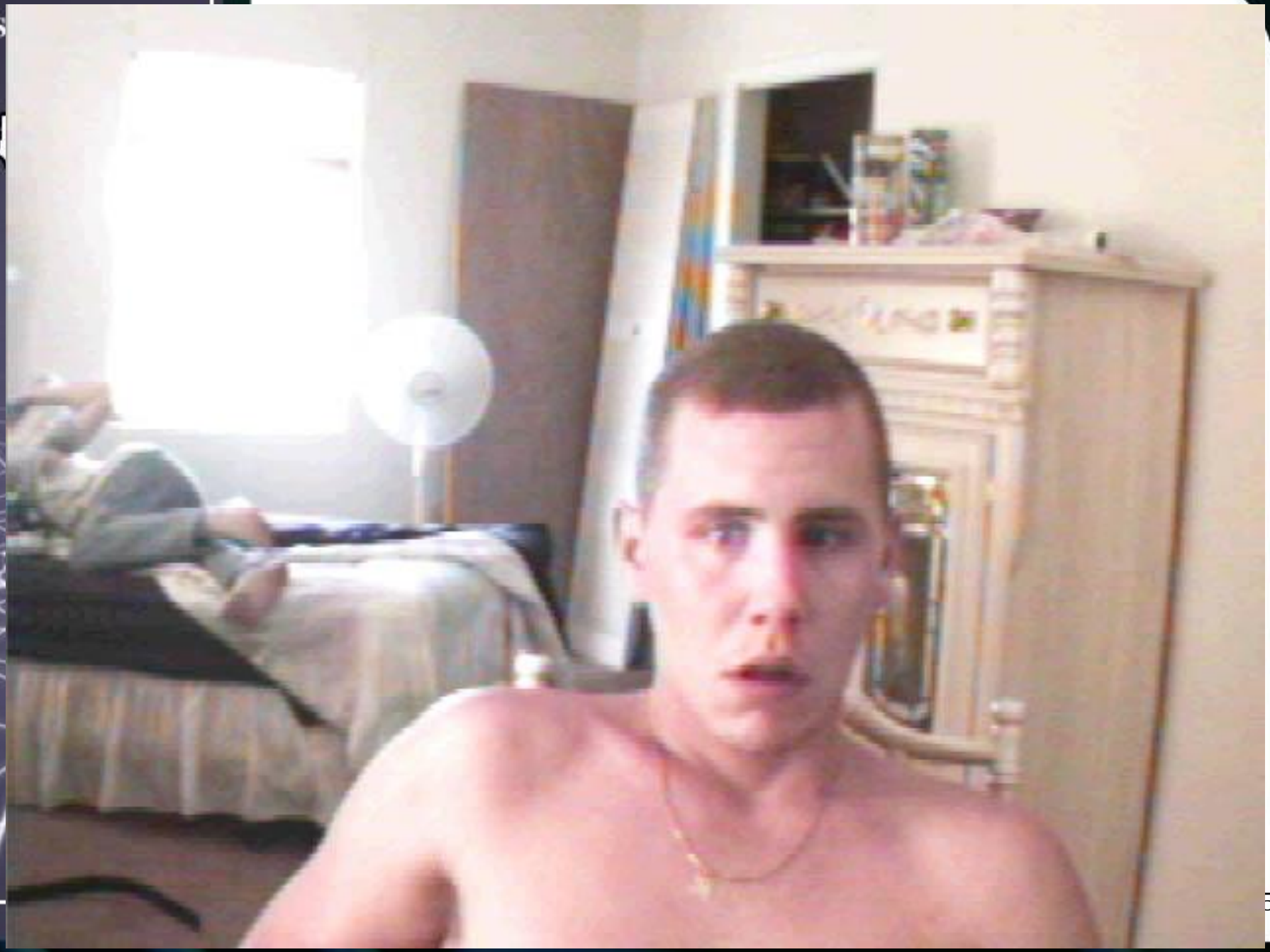
What I'm Gonna Tell 'Ya

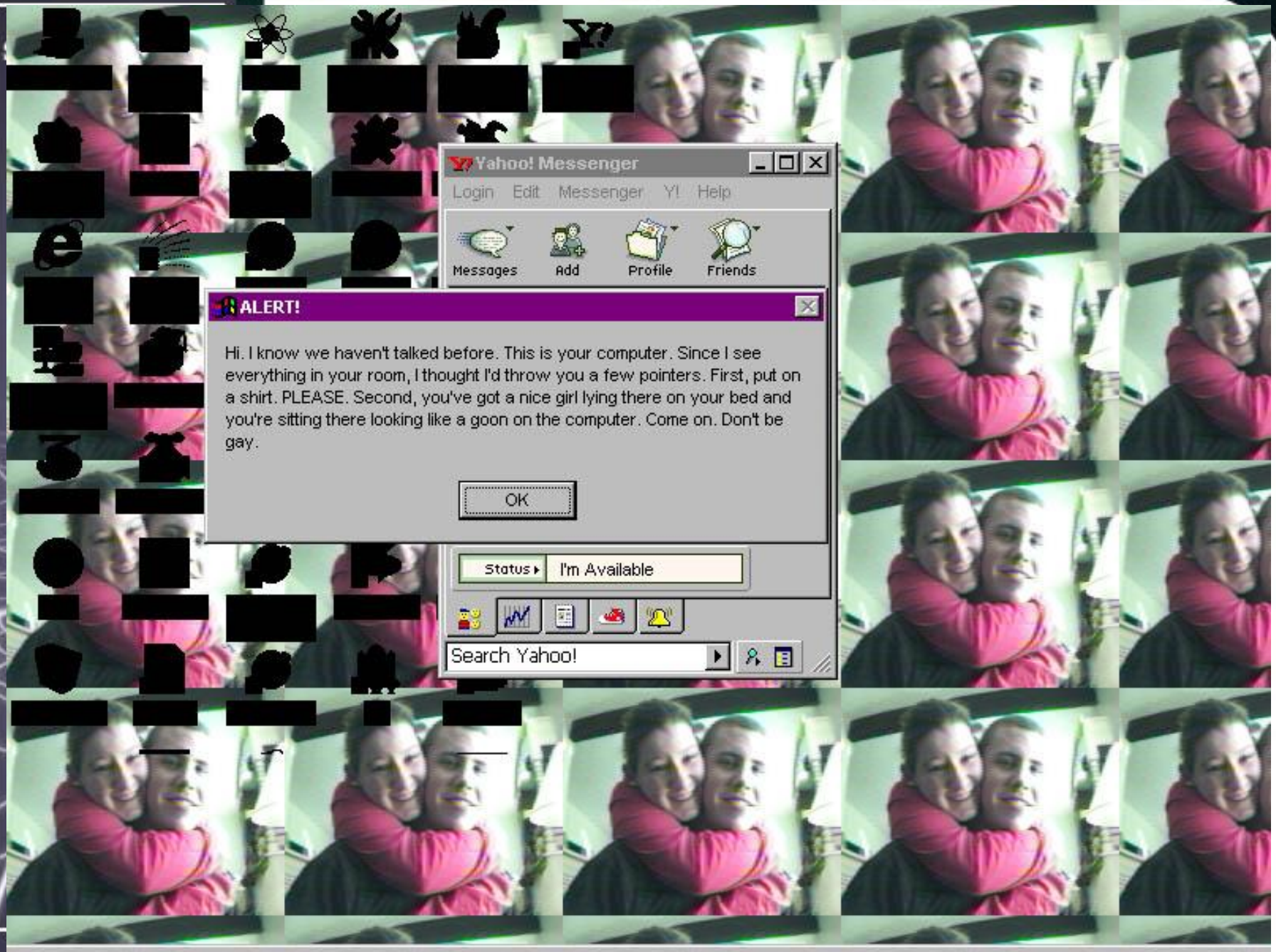


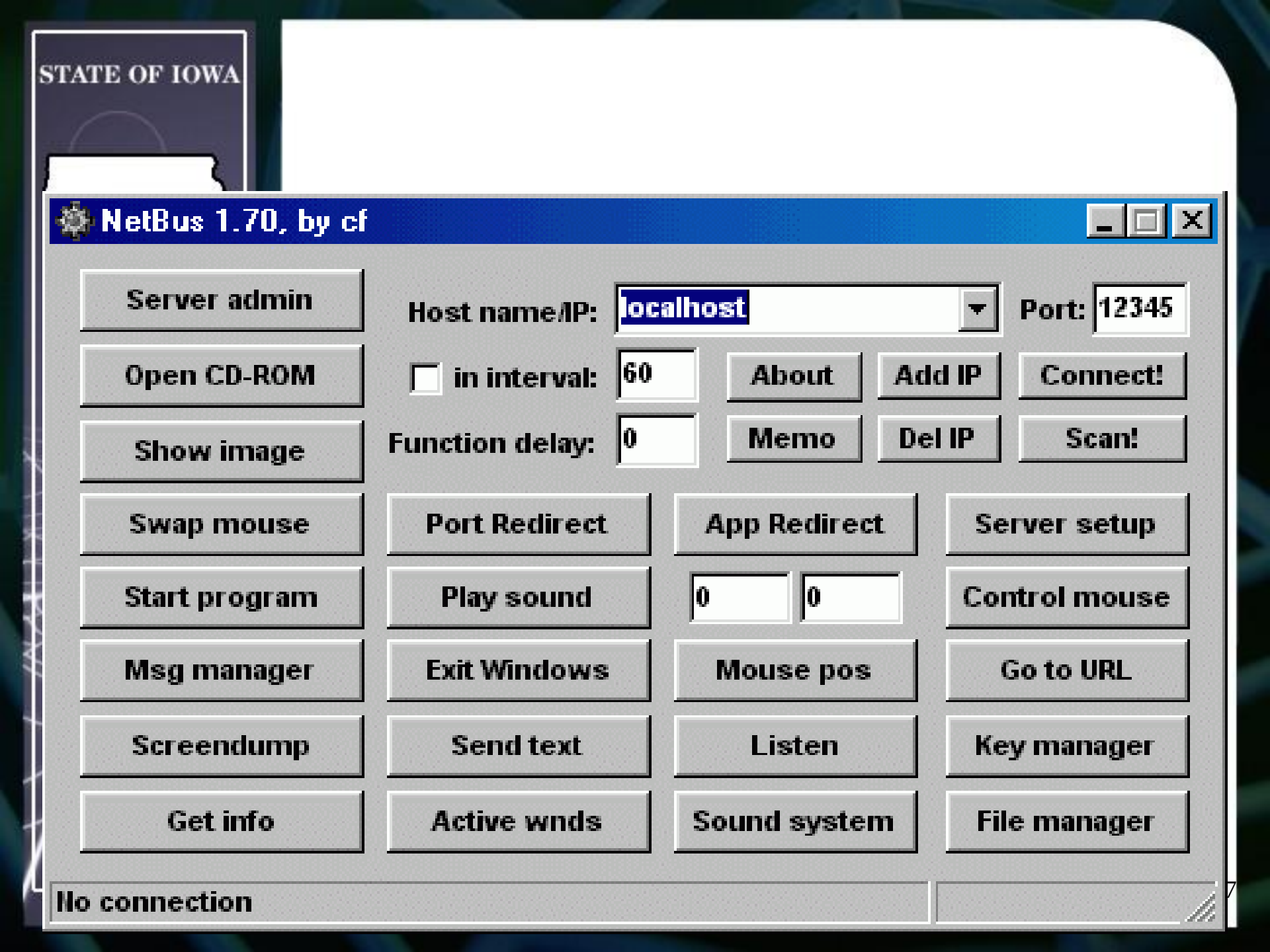
- Introduction
- Today's Environment
- Threats
- Information Assurance
- Challenges
- Elements
- Critical Infrastructures
- Transportation and Security
- Initiatives

Introduction

- Networks increasingly important
- Increasingly under attack
- New security emphasis
- It's a new world out there




Yahoo! Messenger
Login Edit Messenger Y! Help
Messages
Add
Profile
Friends
ALERT!
Hi. I know we haven't talked before. This is your computer. Since I see everything in your room, I thought I'd throw you a few pointers. First, put on a shirt. PLEASE. Second, you've got a nice girl lying there on your bed and you're sitting there looking like a goon on the computer. Come on. Don't be gay.
OK
Status
I'm Available
Search Yahoo!


STATE OF IOWA
NetBus 1.70, by cf
Server admin
Host name/IP:
localhost
Port:
12345
Open CD-ROM
in interval:
60
About
Add IP
Connect!
Show image
Function delay:
0
Memo
Del IP
Scan!
Swap mouse
Port Redirect
App Redirect
Server setup
Start program
Play sound
0
0
Control mouse
Msg manager
Exit Windows
Mouse pos
Go to URL
Screendump
Send text
Listen
Key manager
Get info
Active wnds
Sound system
File manager
No connection

Today's Computing Environment

Advanced societies are dependent upon vulnerable computer systems

- Power grid, dam controls, train switching
- Paychecks, social security and welfare checks, stocks, money transfers
- Criminal records, medical information
- Transportation systems
- $600B/day in Federal Reserve transfers
- $2T/day in international wire transfers
- $15B/day lost

Today's Computing Environment

- New, Internet-based approaches
  - Enhance communication
  - Increase customer satisfaction
  - Reduce cost
- Leverage existing public infrastructures
- Increasingly mobile workforce

Today's Computing Environment

What does this mean?

- Information, resources, and capabilities available at unprecedented levels
- Shop on-line
- Renew licenses, banking, stocks
- Track inventories
- Communicate throughout the world
- Convenience is astonishing
- Opportunities

Today's Computing Environment

But other opportunities exist as well…

The Security Threat

- Technological advances that contribute to these conveniences also make systems vulnerable to attack
- Hacker networks share information and work together fairly well

The Security Threat

"The electron is the ultimate guided weapons system."

--Dr. John Deutch, Director, CIA

Testimony to U.S. Senate Permanent Subcommittee on Investigations Hearings, 25 June 96

The Security Threat

- Hackers
- Crackers
- Phreakers
- Subversives
- Political Dissidents
- Insiders
- Terrorists

STATE OF IOWA

ITD

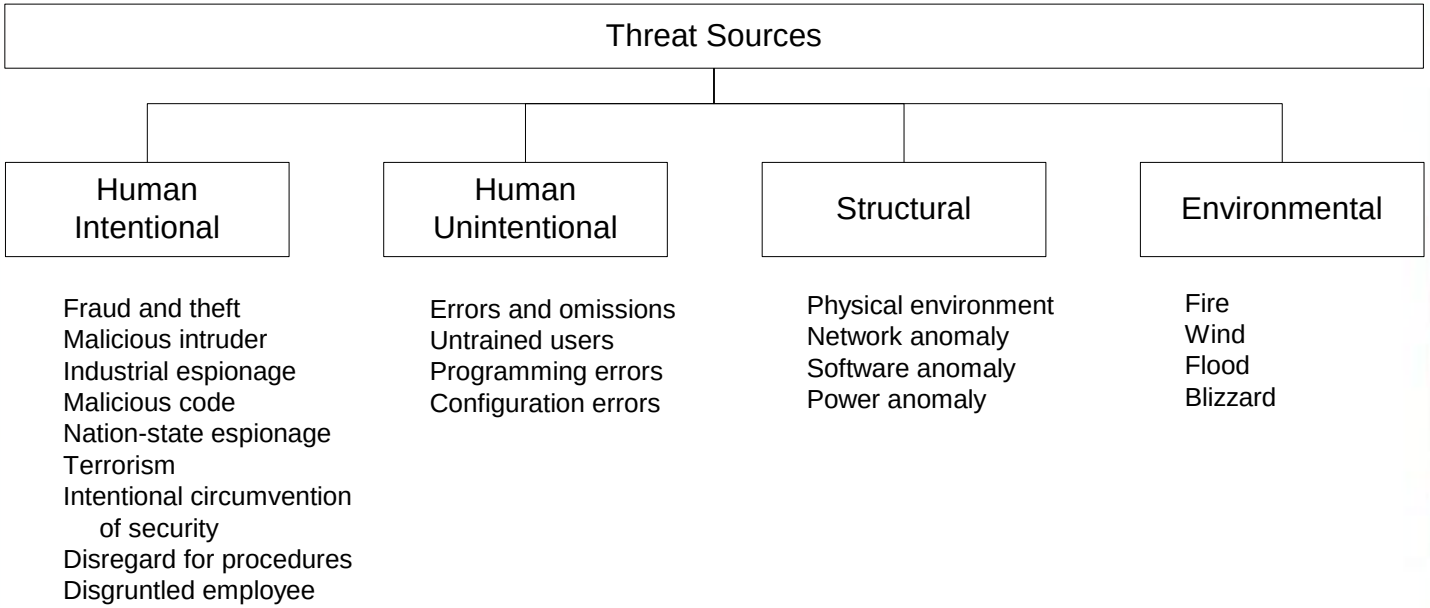
STATE OF IOWA

ITD

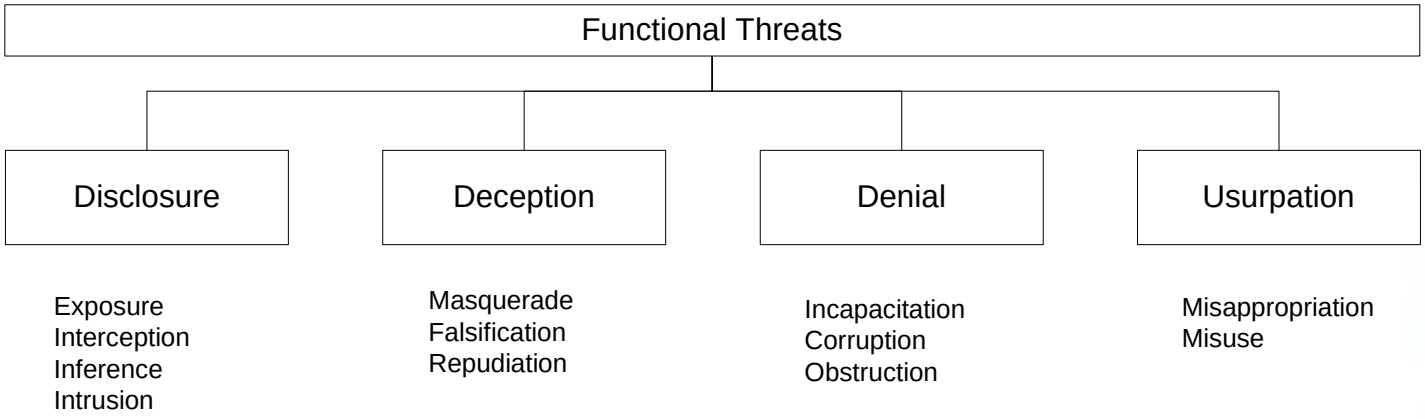
STATE OF IOWA

ITD

Threats



Threats


Functional Threats
Disclosure
Deception
Denial
Usurpation
Exposure
Interception
Inference
Intrusion
Masquerade
Falsification
Repudiation
Incapacitation
Corruption
Obstruction
Misappropriation
Misuse

Threats

- Difficult to ascertain
- Wide and varied
- Intelligence
- Difficult to apply to the risk equation

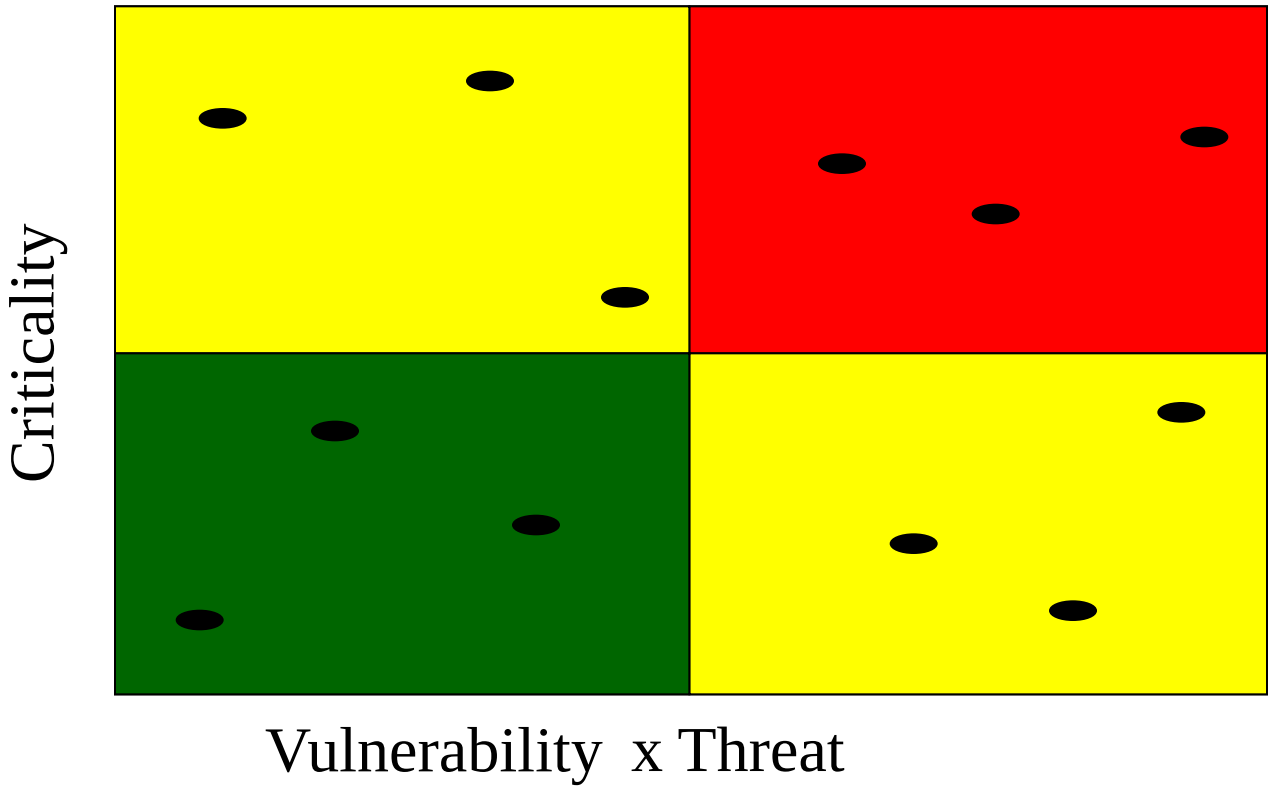
Risk

- Classical risk concept: risk = threat x vulnerability
- New risk concept: risk = criticality x vulnerability

STATE OF IOWA

ITD

Concept of Risk



Risk Management

- What can hurt me?
- How can it hurt me?
- How critical is the asset?
- What can I do to protect myself?

Security is not…

- Easy
- A product
- Static
- A condition
- Risk elimination

Security is…

- Complex
- A process
- Highly dynamic
- Elusive
- Risk management
- Not complete

Information Assurance

- **Protect** information and information systems from intentional, unintentional, structural, and natural threats
- **Detect** threats to information and information systems
- **Restore** capabilities in an efficient and prioritized manner
- **Respond** appropriately with an integrated, coordinated, and focused effort to cope with, reduce, or eliminate the effects of attacks or intrusions

Protect

- Confidentiality
- Integrity
- Availability

STATE OF IOWA

ITD

Protect

Risk Management, and thus, Information Assurance, is a *process*, not a product.

Detect

- Host and network-based intrusion detection
- Auditing and log review
- User reporting
- Daily status update

Restore

- Backups in a secure location
- Test
- Exercise
- Identify critical assets

Respond

- Configuration changes
- Law enforcement
- Hardware, software
- Policy changes

Challenges

- Protect confidentiality, integrity, and availability
- Protect while allowing user to function
- Promote security as an enabler, not an obstacle

AGONY

Not All Pain Is Gain.

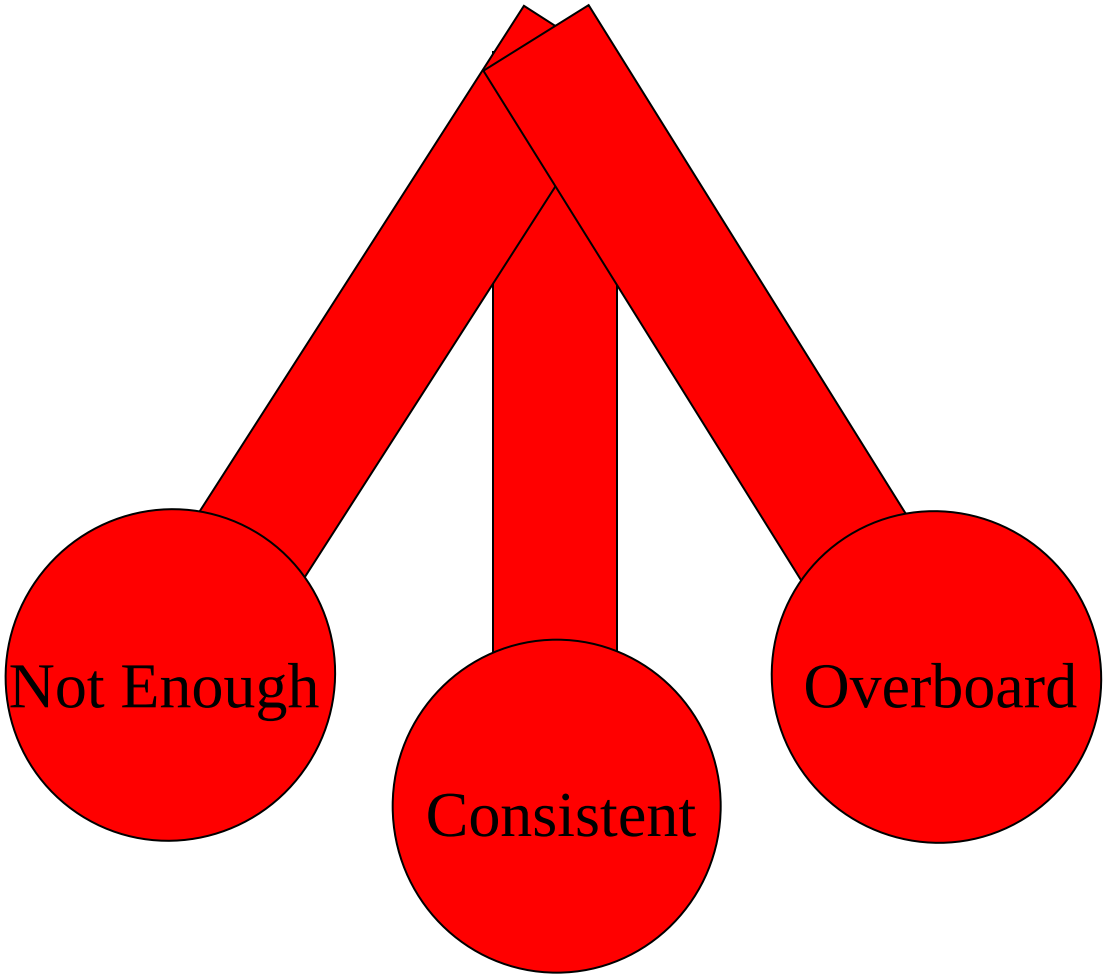
Challenges

- Management
- Operations
- Law
- Users
- Administrators
- Resources

APATHY

If We Don't Take Care of the Customer,
Maybe They'll Stop Bugging Us.

The Pendulum

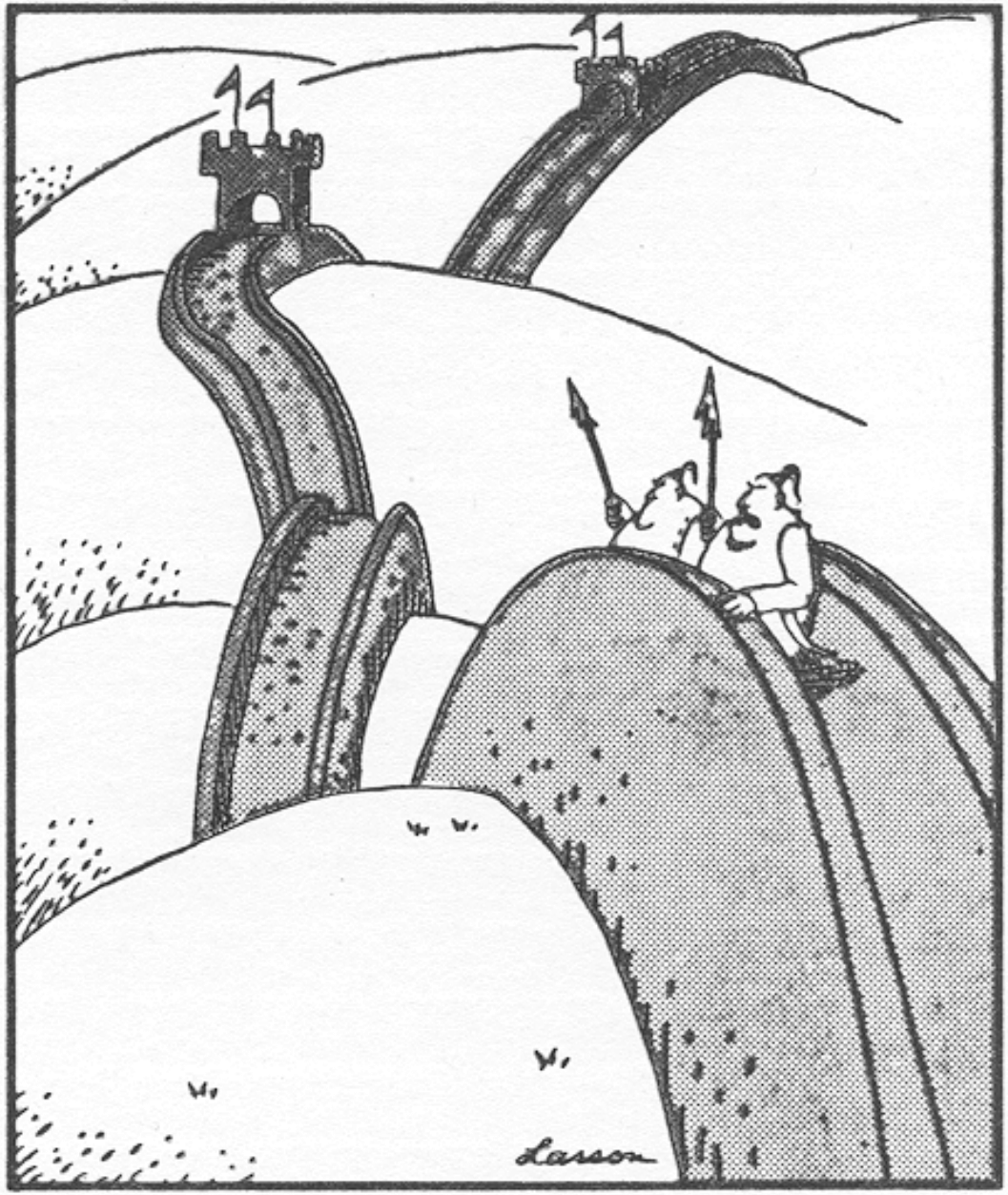


Challenges

- Security standards
- Vendors
- Products
- No such thing as a state of perfect knowledge
- Reactive vs. proactive
- Just enough

STATE OF IOWA

ITD



"Now we'll see if that dog can get in here!"

Guiding Principles

- The state is entrusted with the information and owns the accountability for its protection.
- Security exists only to mitigate risk.
- Security must be an enabler.
- Security input must be value added.
- Security input must be practical and fast.

Elements

- Policy
  - Standard
    - Procedure
- Guidelines
- Acceptable use
- Physical security

Elements

- Asset identification
- Vulnerability assessments
- Risk assessments
- Event reporting
- Incident response
- Defense in depth
- Enterprise approach

Elements

- Security awareness
- Malicious logic protection
- Backup and recovery
- Portable devices
- Telecommuting
- Roles & responsibilities

Elements

- Intrusion detection
- Contractors & vendors
- Privacy
- Business continuity
- Identification & authentication
- Access control

Elements

- Logging
- Audit
- Configurations
- Change management
- Testing
- Compliance
- Environmental controls

Critical Infrastructures

"…the nation's critical infrastructures—telecommunications, water supply, electric power, banking and others—have substantial vulnerabilities that can be exploited by terrorists and foreign powers."

--*General Robert T. Marsh*
Chairman, President's Commission on Critical Infrastructure Protection

Critical Infrastructures

"Certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States."

--President William J. Clinton, Executive Order 13010


Government Operations
Gas & Oil Storage and Delivery
Emergency Services
Water Supply Systems
Critical Infrastructures
Telecommunications
Banking & Finance
Electrical Energy
Transportation

Targetability

- The US is extremely targetable
- US contains 42% of the world's computing power – 1997 figures
- Advanced societies increasingly dependent on vulnerable systems
- A **national** digital nervous system

Critical Infrastructures

- Essential to economic and national security of US
- Vital to health, welfare, and safety
- Increasingly interdependent and interconnected systems

Critical Infrastructures

- Owners & operators primary responsibility for protecting
- Generally not designed to cope with significant military or terrorist threats
- Government and industry must work together to deal with protecting our homeland

Critical Infrastructures

- Requires an unprecedented partnership
- Goal - assured service delivery

No Problem?

"To suppose that national utilities and infrastructure could be taken out by cyber terrorists, is, quite frankly, bollocks."

--Neil Barrett
Information Risk Management

Omega Engineering

- Tim Lloyd planted a software time bomb
- Destroyed software controlling manufacturing machines
- $10 million + in losses
- $2 million + for reprogramming
- 80 layoffs

Transportation

- Trucking
  - Dispatching, load planning, routing, mobile communications, fuel purchasing, vehicle tracking, driver settlements, human resources, wireless
  - Integration of information from all sources into one system
  - Allow customers to make better decisions and become more profitable

Transportation

- UPS
  - Ring scanner
  - Wearable computer
  - Track packages
- Lower costs, boost profits
- Improve connectivity, communications, and collaboration

Transportation

- US Dept of Transportation involved in PCIS
- Intelligent Transportation Society of America

ITS America

- Data Security and Privacy Task Force
- Promoting awareness of security and privacy issues
- Transportation information available to more people than ever before
- Have not been adequately addressed

Transportation Security

- Dec 2000 figures
- $2.7 trillion industry
- 17% of U.S. economy
- $30 - $50 billion in cargo stolen worldwide each year
- http://www.nas.edu/trb/publications/security/ebadolato.pdf

Transportation Security

- Vast amount of info on shipments, customers' inventories in motion, and equipment
- Just in time delivery
- Privacy

Transportation Security

- E-commerce
- Asset identification
- Customer profits
- More information contained in a common system

Transportation Security

- Traffic light systems
- Wireless networks
- Rail systems
- Any transportation asset that uses computer-based systems

Transportation Security

- Threats
  - Fraud
  - Money laundering
  - Penetrate systems to identify cargo content and location
  - Reroute cargo
  - Reroute trains, plains, etc.

Transportation Security

- Stephen Flynn, "Transportation Security: Agenda for the 21st Century"
- http://www.nas.edu/trb/publications/security/sflynn.pdf
- Talks about lack of defenses and openness
- Discusses the need to remove all weak links

Flynn

- Five initiatives
  - Awareness
  - Global cooperation
  - Increased transparency
  - Private-public partnerships
  - Marshalling resources and expertise

NIPC

- FBI's National Infrastructure Protection Center
- Created in response to PDD 63
- National critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation & response entity
- The local level's link to federal efforts

NIPC

- Share, analyze, and disseminate information
- Training for federal, state, and local cyber investigators
- Coordinate FBI computer intrusion investigations

InfraGard

- Part of the NIPC
- Outreach and information sharing with public and private sector
- Owners & operators of critical infrastructures
- Local chapters
- An Iowa chapter now in operation

InfraGard

- Formal and informal information exchange
- Promotes protection of critical infrastructures
- Representatives from private industry, government agencies, academic institutions, state & local law enforcement

InfraGard

- Intrusion alert network
- Secure Web site
- Seminars and training
- Meetings with colleagues
- Develop contacts with each other and local FBI personnel

FBI Benefits

- More reported intrusions
- Satisfies PDD 63
- New channels for threat warning dissemination
- New contacts in business community

Private Sector Benefits

- Threat warnings
- Better understanding of law enforcement and available resources
- Education and training
- Interaction with a wide variety of personnel

PCIS

- Partnership for Critical Infrastructure Security
- Supposed to coordinate cross-sector initiatives
- Industry driven
- Setting up information sharing and analysis centers

New Mexico

- New Mexico Critical Infrastructure Assurance Council
- http://www.nas.edu/trb/publications/security/doneil.pdf
- Cooperative, private-public sector, all volunteer

NMCIAC

- Addressing
  - Information and communications
  - Transportation
  - Utilities
  - Banking and finance
  - Emergency management and government services

Iowa

- InfraGard chapter
- Critical Infrastructure Assurance Coordinator
- Working with Emergency Management
- Terrorism conferences
- Will be branching out this year

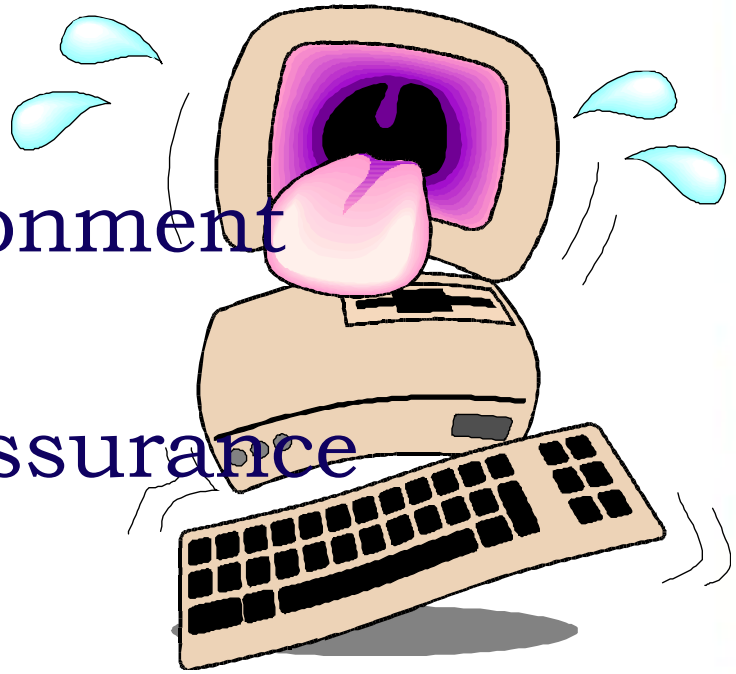
Links

- Iowa Security: http://www.itd.state.ia.us
- NIPC: http://www.nipc.gov/
- InfraGard: http://www.infragard.net/
- PCIS: http://www.pcis-forum.org/index.cfm
- CIAO: http://www.ciao.gov
- ITS America: http://www.itsa.org/
- ITSB Transportation Security: http://www4.trb.org/trb/homepage.nsf/web/security

STATE OF IOWA

ITD

What I Told 'Ya



- Introduction
- Today's Environment
- Threats
- Information Assurance
- Challenges
- Elements
- Critical Infrastructures
- Transportation and Security
- Initiatives

Information Assurance and Transportation

Presented to the
Midwest Transportation Consortium
18 January 2002

Kip Peters
Chief Information Security Officer
State of Iowa
515-725-0362
Kip.Peters@itd.state.ia.us
http://www.itd.state.ia.us/security/