INFORMATION SECURITY:

The Human Side

Keith A. Rhodes, PE, CCP

Chief Technologist

A *Final* Thought

- **"The only system which is truly secure is one which is switched off and unplugged, locked in a titanium lined safe, buried in a concrete bunker, and is surrounded by nerve gas and very highly paid armed guards. Even then, I wouldn't stake my life on it."**

  - Dr. Gene Spafford, Purdue university

The General Accounting Office: "What Do THEY Do?"

- Reviews included:
  - Ability to Protect
  - Ability to Detect
  - Ability to React
- Reviews covered both internal and external threat
- Reviews included both physical and logical penetration testing

The General Accounting Office: "What Do THEY Do?"

- Reviews Test:
  - Entity-wide Security
  - Access Controls
  - Change Control
  - Segregation of Duties
  - System Software
  - Service Continuity

OPSEC Risk Context

- $T \times V \times I = R$

- T = Threat
- V = Vulnerability
- I = Impact
- R = Risk

- $T = A + I + C$

- T = Threat
- A = Adversary
- I = Intent
- C = Capability

Vulnerability / Capability

Public Sources:
Web pages, news papers
periodicals, phone book, . . .

Standard OS Commands:
whois, nslookup, ping,
finger, traceroute, dig, . . .

Social Engineering:
Help desk, employees,
contractors, temps, . . .

Information Gathering

Port Scanners:
nmap, Xscan, nlog, ss,
snmpsweep, . . .

Password Crackers:
l0phtCrack, IMP / Pandora,
Crack, John the Ripper,
CiscoCrack, . . .

Select Targets

Data Extraction & Analysis:
DumpEvt, DumpACL, Null,
Logcolorise, CA-Examine,
Chknull, Hunt, . . .

Modem Locators:
THC, PhoneSweep,
Toneloc, . . .

Sniffers/Capture Utilities:
NetXRay, tcpdump, Xscan,
snoop, sniffit, keycopy,
dsniff, pdump, snort, . . .

Test for Vulnerabilities

Standard OS Commands:
cat, more, find, grep, telnet, ftp,
tftp, net use, nlist, . . .
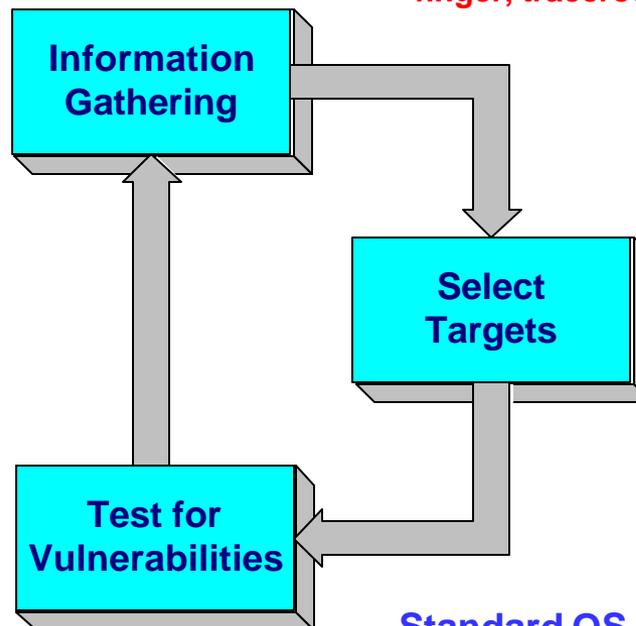
Vulnerability Scanners:
ISS, Database Scanner,
CyberCop Scanner, NetRecon,
SAINT, SARA, Whisker . . .

6

Impact / Intent
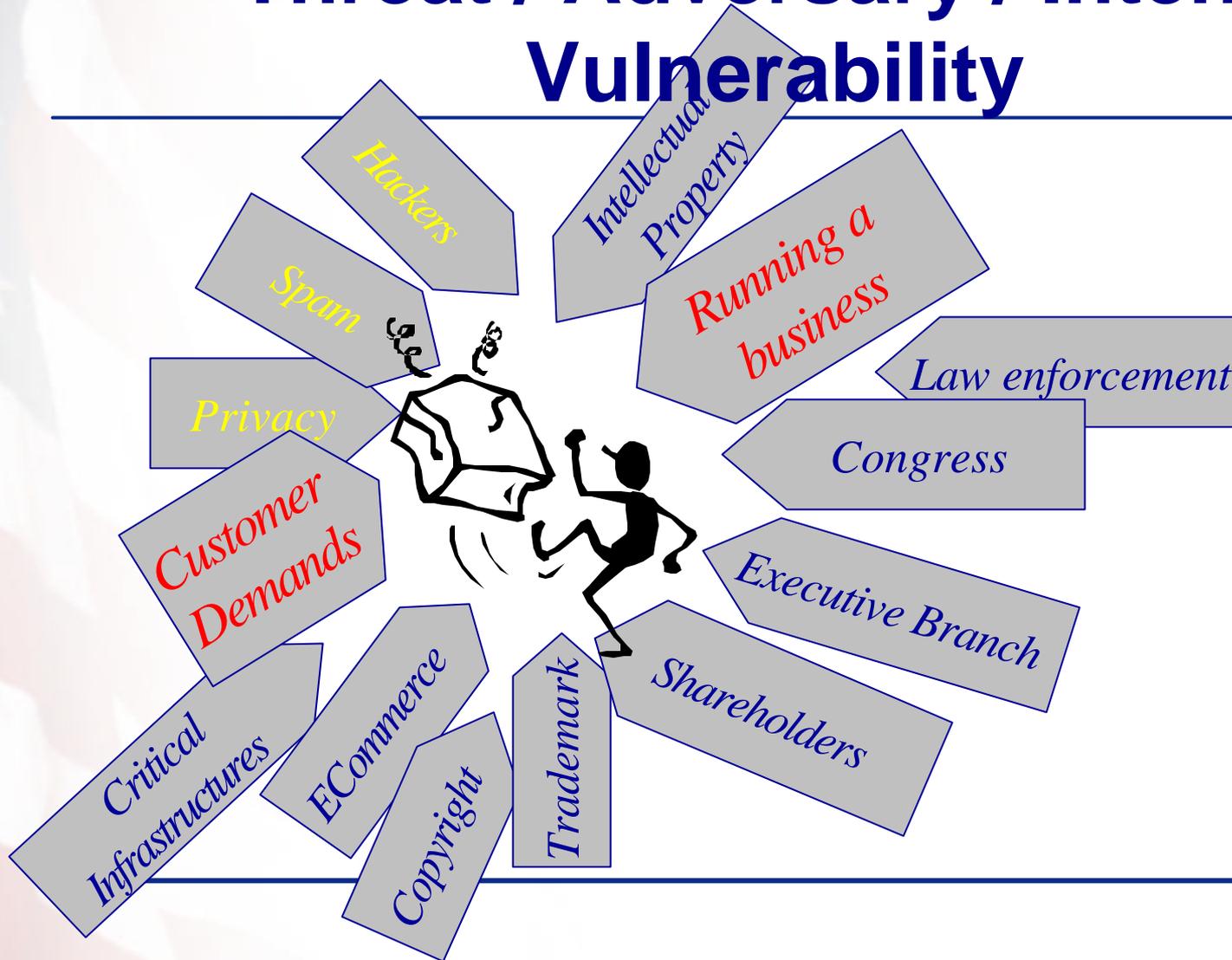
- Global web population: 605.6 M
- US electronic clearing: $702 T
- Domains as of Jul, 2002: 162,128,493

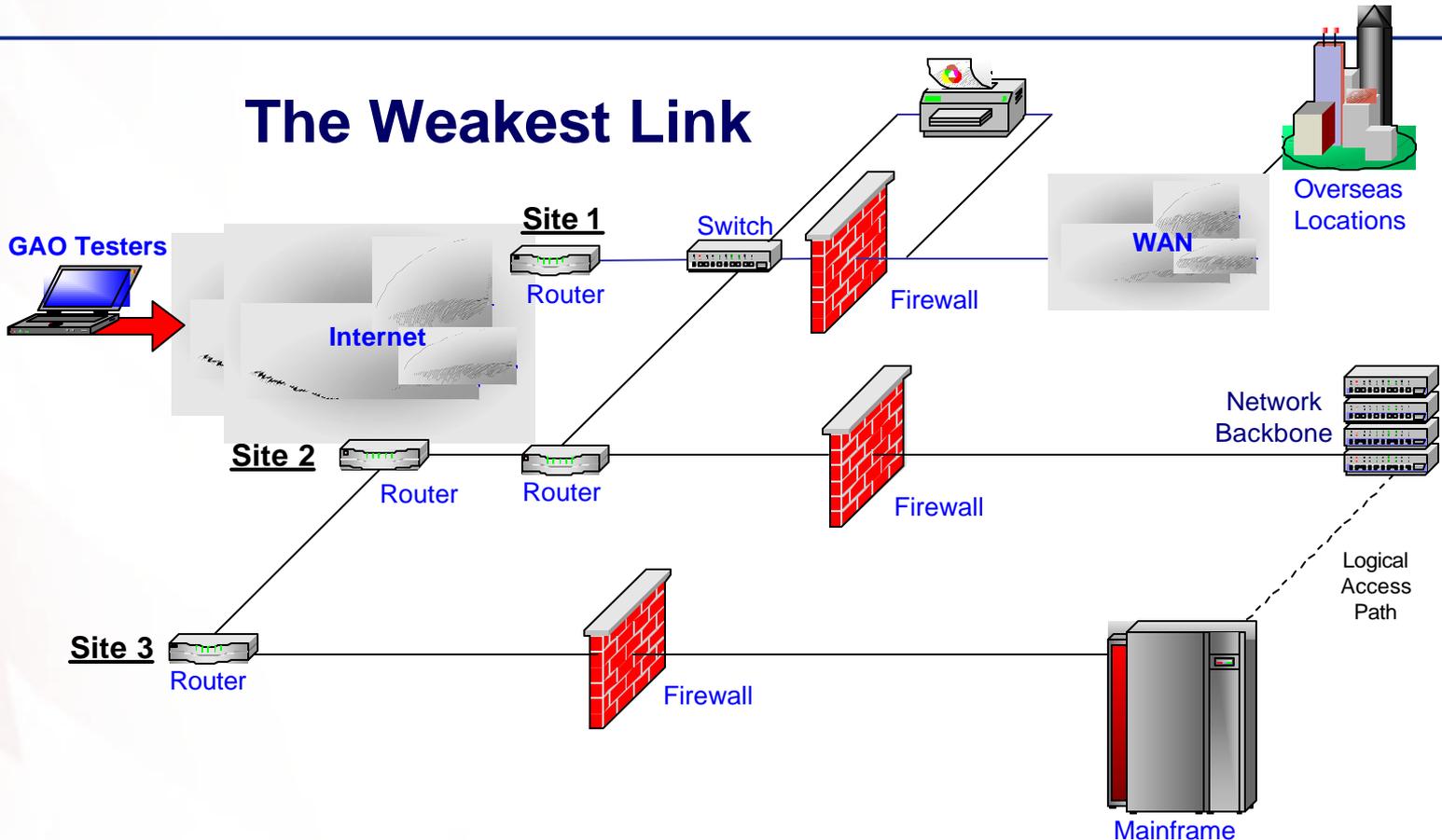# Threat / Adversary / Intent / Vulnerability

Adversary / Intent / Capability

- 41% of all MOs - Requests for Information
- 4% - INTERNET

- 36% - Commercially Sponsored
- 19% - Government Affiliated

- #1 - Information Systems (30%)
- #15 - Information Warfare (0.5%)
- source: DSS 2001 Technology Collection Trends in the US Defense Industry --http://www.dss.mil/cithreats/2001_trend.pdf
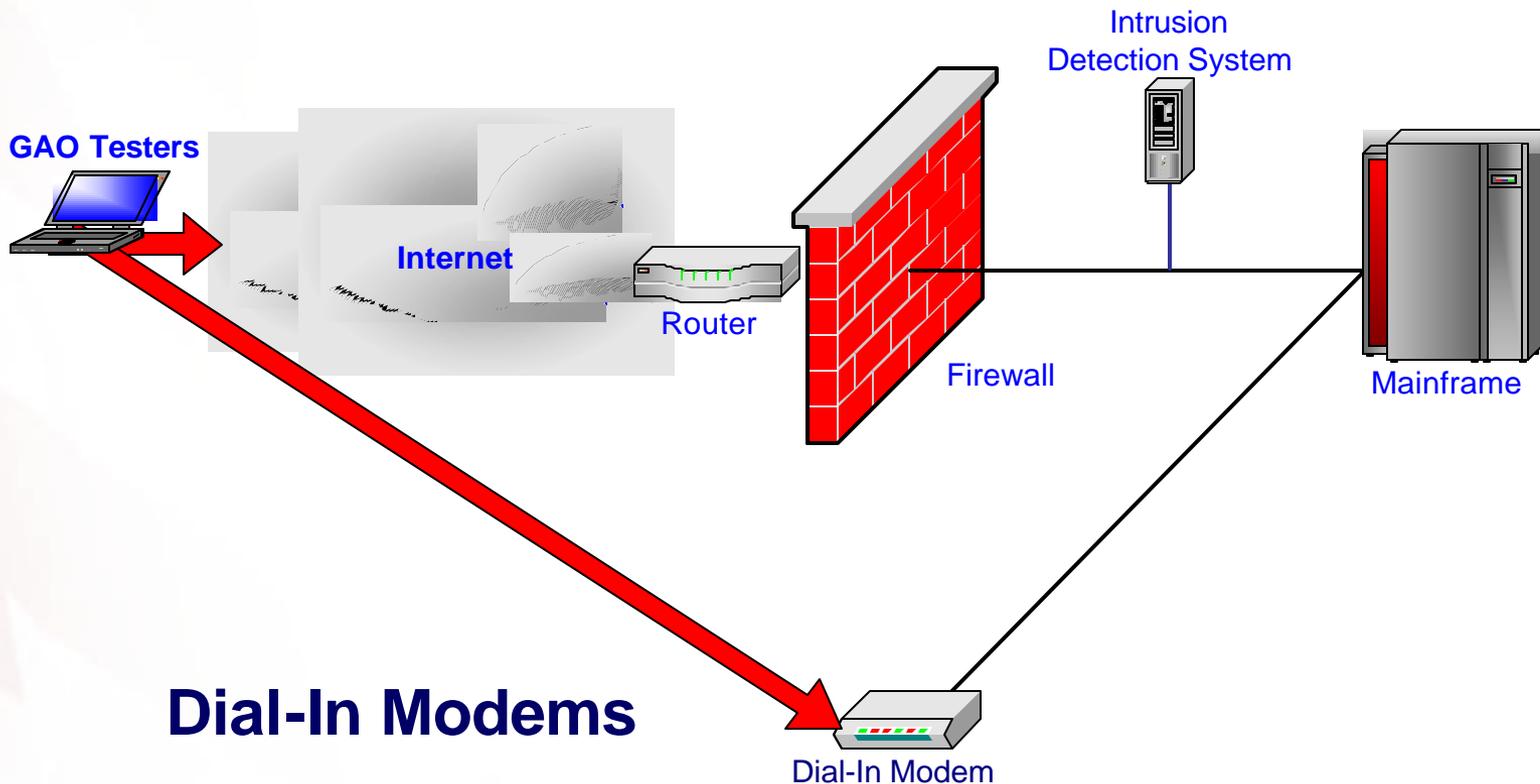
Vulnerability / Opportunity / Capability

"These are a few of my favorite things …"
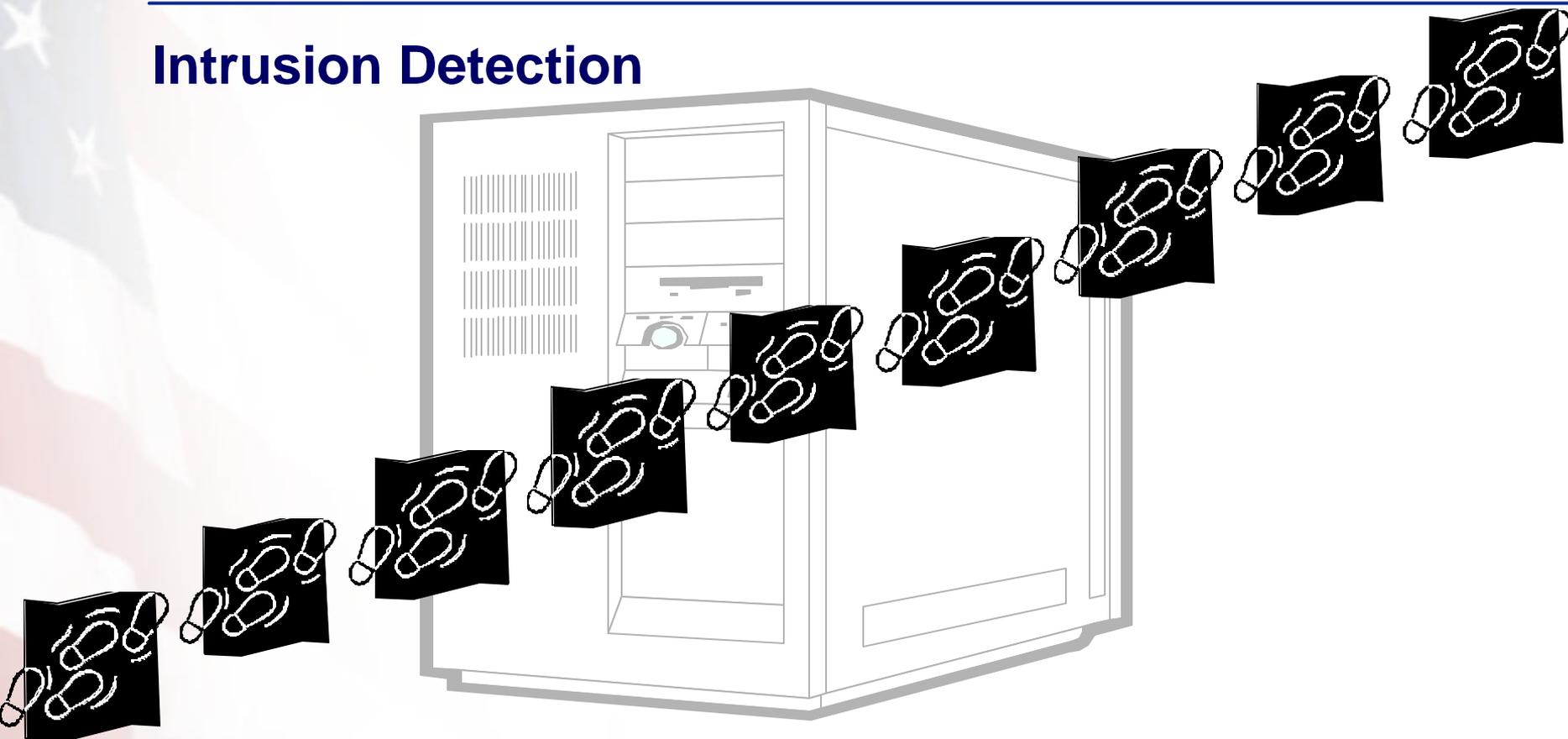
"We Were Hacked by a Toaster?"

The Weakest Link

GAO Testers

Internet

Site 1
Router

Switch

Firewall

WAN

Overseas Locations

Site 2
Router   Router

Firewall

Network Backbone

Site 3
Router

Firewall

Logical Access Path

Mainframe

"The Front Door Was Locked …"

GAO Testers

Internet

Router

Firewall

Intrusion Detection System

Mainframe

Dial-In Modems

Dial-In Modem

"Someone's Been Here ..."

Intrusion Detection

"We Have a Very Helpful Helpdesk …"
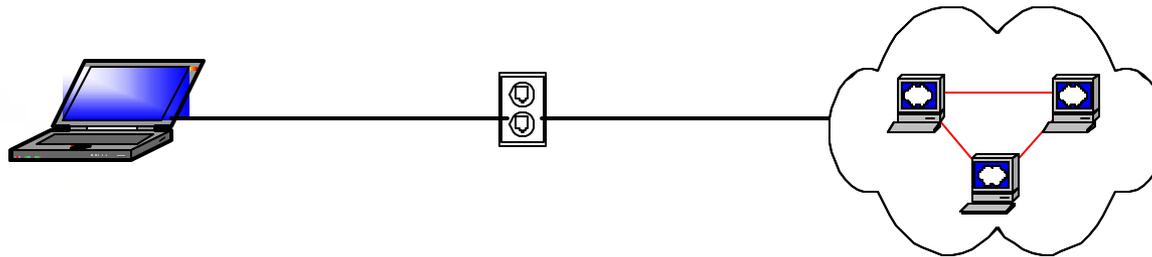
Social Engineering

"We Have Trusted Employees ..."

Insider Threats

"We're Being Attacked by Our Conference Room …"

"Live" But Unattended Network Drops

- Conference Rooms
- Training Rooms
- Team Rooms
- Vacant Offices

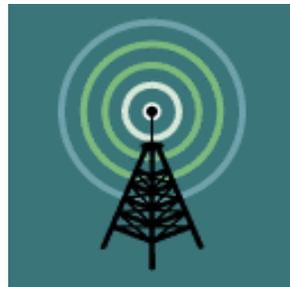# "… But He's Only 14 Years Old."

Script Kiddies

- No Experience Required

- Easy to Use Tools

- Freely Available

- Freeware, Shareware & Evaluation Software
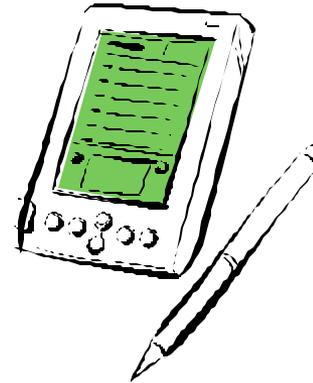
"He Was a Victim of a 'Drive-by" Hack."

Wireless Networking

- *Range of about 450 yards*
- *Affordable with prices dropping*
- *Encryption not enabled by default*
- *Configuration issues*

"It's Only an Organizer."

Personal Digital Assistants

Store Sensitive Information From Desktop
Transport Sensitive Information From Desktop
Wireless Connectivity
  - Wireless Modem
  - Wireless Network
  - Infrared
Password Cracking
War Dialing
Digital Camera

"It Was a 10-second Hack …"

Keystroke Capturing Devices

Before

After

- *Installs in a few seconds*
- *Doesn't need batteries*
- *Impossible to detect or disable with software*
- *Stores up to 2,000,000 keystrokes can be stored with 128 bit encryption*
- *Works on all operating systems*
- *From only $139*

Conclusions

- **NO** single security standard
  NO single vendor
  NO single product can meet an organization's security needs

- One size **DOES NOT** fit all

- This morning's vendor solution **WILL NOT** protect against this afternoon's technique

- Attack morphology is faster, but attacks are even faster … and software is buggier

Recommendations

- Assess the value of your assets
  - "What do we do for a living?"
  - "Who is the competition?"
  - "What are the critical data (i.e., What data are most valuable to my competitor)?"
  - "How long can I go without an update?"
  - "How many steps must I execute to build (re-build) these data?"

Final **Final Thoughts**

- A lack of institutional will is more destructive than any technology
- **NOTHING BEATS WELL-TRAINED PERSONNEL**
- If we can't write or buy good code, we can't protect ourselves
- Any system that ignores human nature **WILL FAIL**

Weak Risk Management: Chernobyl April 25-26, 1986
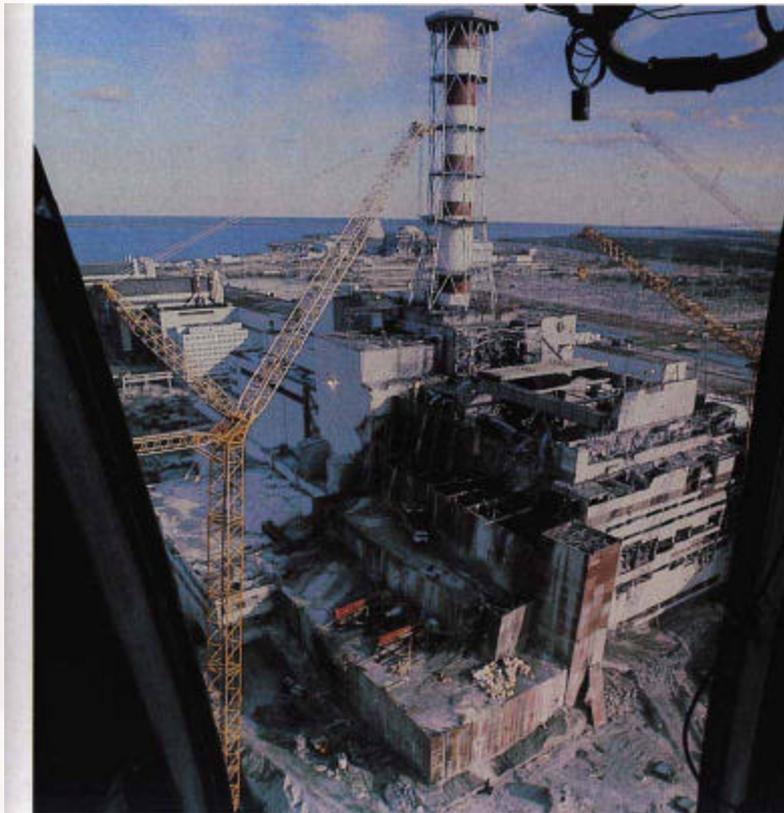
- April 25 @1400 hrs. Operators disconnect Emergency Core Cooling System

- No manager approval for continued operation

- April 26 @ 0100 hrs. Emergency protection signals blocked by operators

- April 26 @ 0119 hrs. Excessive radioactivity ignored by operators

- April 26 @ 0123:48 Explosion occurs followed by second explosion

Questions

Contact

Keith A. Rhodes, PE, CCP

Chief Technologist

Director, Center for Technology & Engineering

U. S. General Accounting Office

441 G street, N. W., Washington, D. C. 20548-0001

V: (202) 512-6412

F: (202) 512-6451

E: rhodesk@gao.gov