Proprietary Information

SYSTEM SECURITY AND INFORMATION WARFARE:

NETWORKS AT RISK

TED PHILLIPS
BOOZ·ALLEN & HAMILTON INC

April 1997

Today's Agenda

- System Security Issues -- Understanding The Risks
  - Telecommunications Industry Trends
  - Network Vulnerabilities
- Threats And Case Histories
- Strategies To Reduce Your Risk Exposure

This Briefing Is Based On Entirely On Unclassified And Open Source Information.

SYSTEM SECURITY ISSUES: UNDERSTANDING THE RISKS

Understanding the Risks

Electronic Intruders Are Targeting Core Communications Technologies

Networks Are Highly Interconnected And International. . .

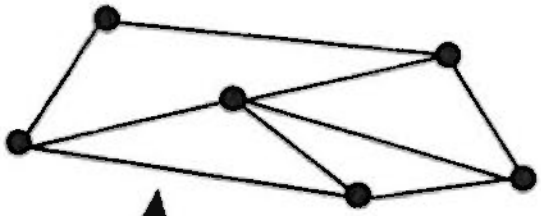
They Are Very Attractive Targets For Electronic Intruders. . .

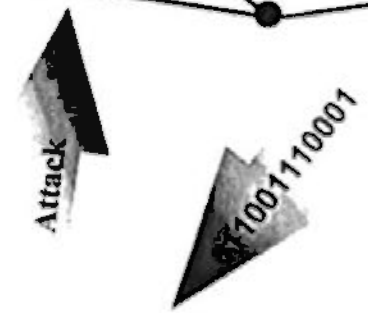
Understanding the Risks

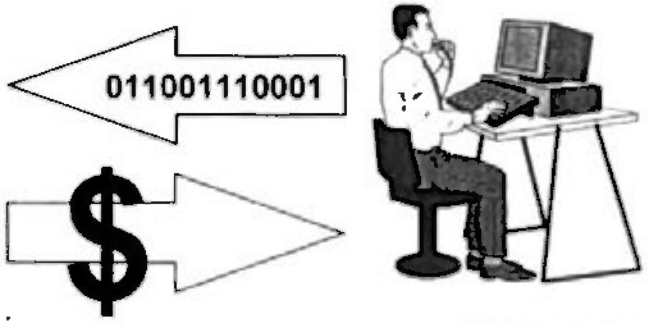
Financial Gain Is A Strong Motivator

Foreign Intelligence Services
Organized Crime
Terrorist Organizations
Industrial Espionage Agents
Private Investigators
Information Brokers

Many groups have a high level of interest in electronic intrusion skills







Understanding the Risks

During The Past 3 Years. . .

Network Attacks Have *Increased Significantly*

Intruders Have Attacked
All Major Categories Of Network Elements

Intruders Have Attacked
A Wide Variety Of End User Systems

Intruders Have Attacked
All Major U.S. Telecommunications Carriers

Intruders Have Attacked
Many Major International PTT Networks

Intruders Have Attacked
All Major Internet Service Providers

Telecommunications Industry Trends

Industry Trends Will Increase Risk

Industry Competitive Issues

Privacy And Confidentiality Trends

Architectural Trends

Technology Trends

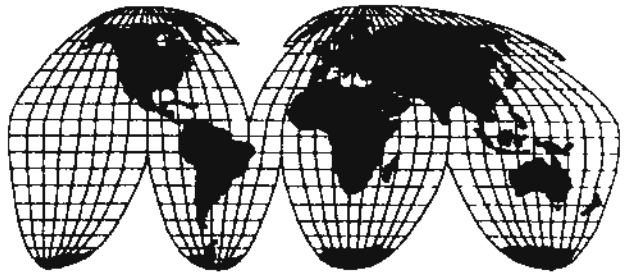
Industry Competitive Issues

- Financial Pressures Reduce Security's Priority
- Metrics To Conduct Security Cost/Benefit Analyses Not Fully Developed
- Downsizing Reduces Worker Loyalty And Creates Disgruntled Ex-Employees

Privacy And Confidentiality Trends

- Sensitive Customer and Network Information Is Created And Stored On Network Elements
- Sensitive Information Is Openly Exchanged Among Network Elements
- End User Systems Are Directly Connected To Public Networks

Architectural Trends



- Network Administration Is Increasingly Shared Between Carriers, Service Providers, And Users
- Customer Premise Equipment (CPE) Is More Interconnected With Public Network Elements
- Public Network Elements Are Richly Interconnected, Creating Extremely Complex Network Structures
- The Communications Industry Is Moving Toward A Cell-Switched Architecture

Technology Trends

- Public Network Elements Are Virtually All Computerized And Software-Controlled
- Network elements are increasingly complex and difficult to securely administer
- Wireless Technology Will Be Important For End-User Network Access

New Technologies Will Increase Risk

- Synchronous Optical Networks (SONET)
- Asynchronous Transfer Mode (ATM) Networks
- Internet Protocol, version 6 (IPv6)
- Digital Subscriber Line Technologies (xDSL)
- Advanced Intelligent Networks (AIN)
- Integrated Services Digital Network (ISDN)
- Wireless Local Loop Technologies
- Wireless Data Networks (CDPD, PCS)

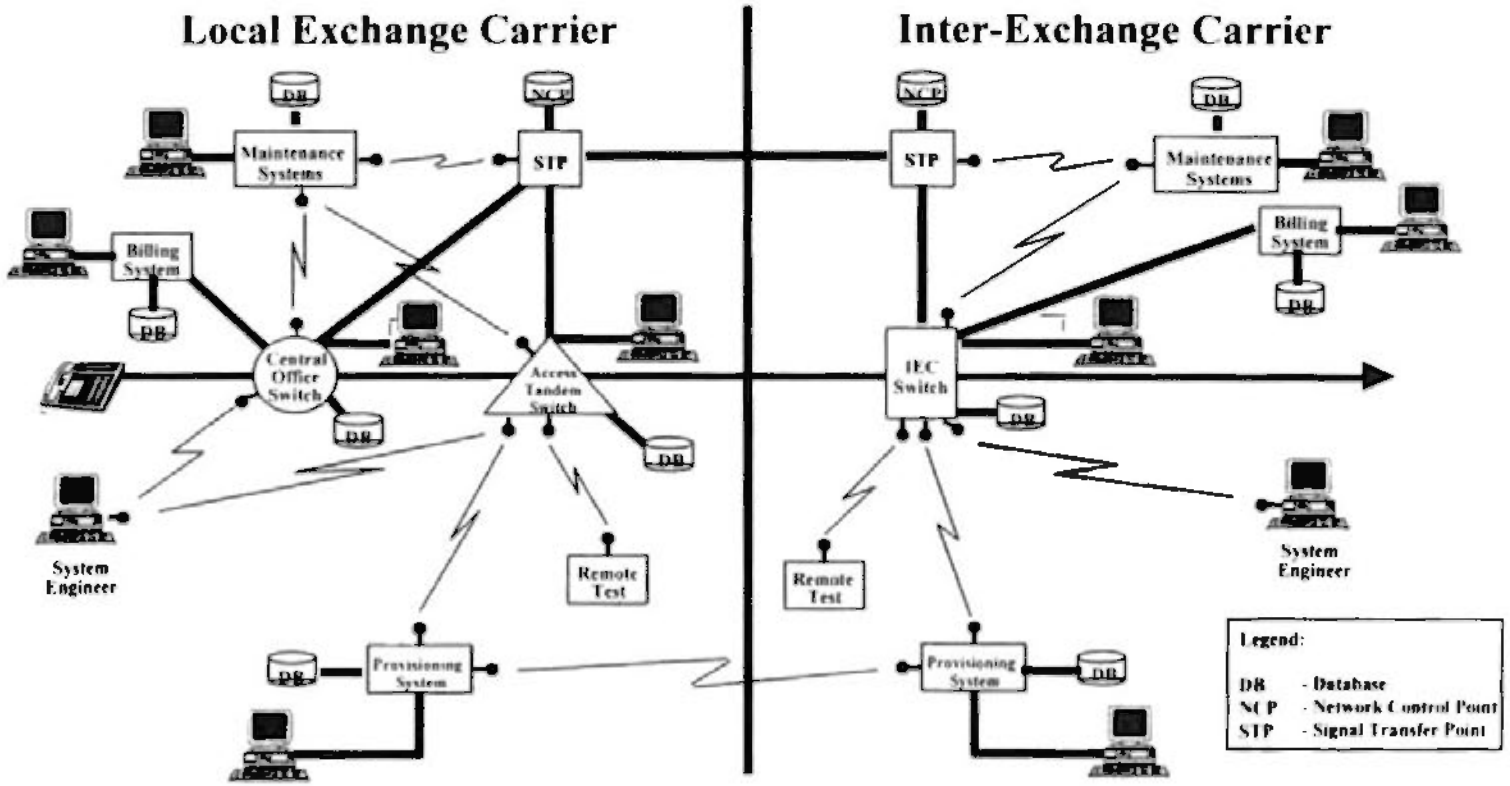
⇨ ***Electronic Intruders Are Developing Techniques To Attack Each Of These Technologies***

Network Vulnerabilities

Understanding the Risks

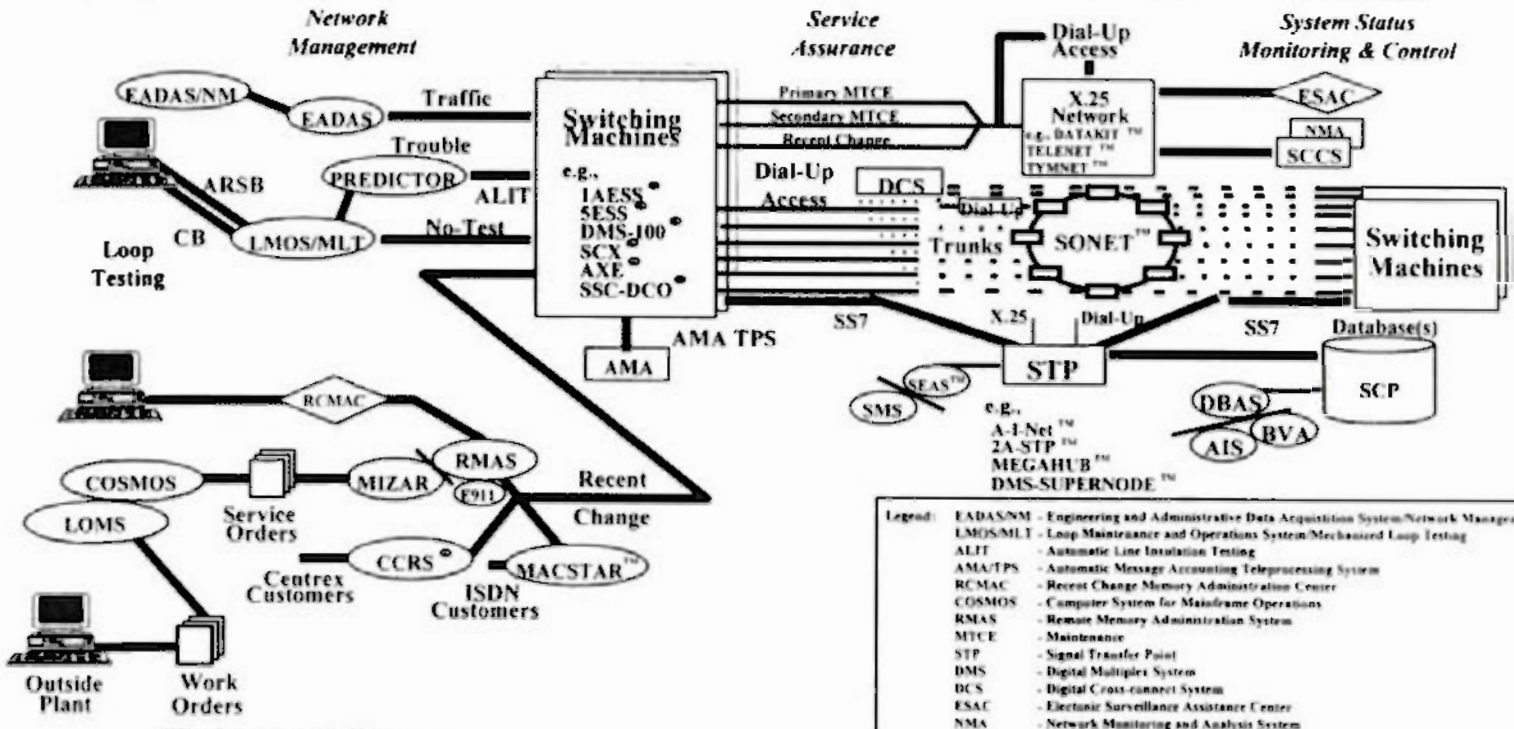
Network Vulnerabilities

All Systems On This Diagram Have Been Penetrated At Least Once In The Past 3 Years



Understanding the Risks

Network Vulnerabilities (cont.)

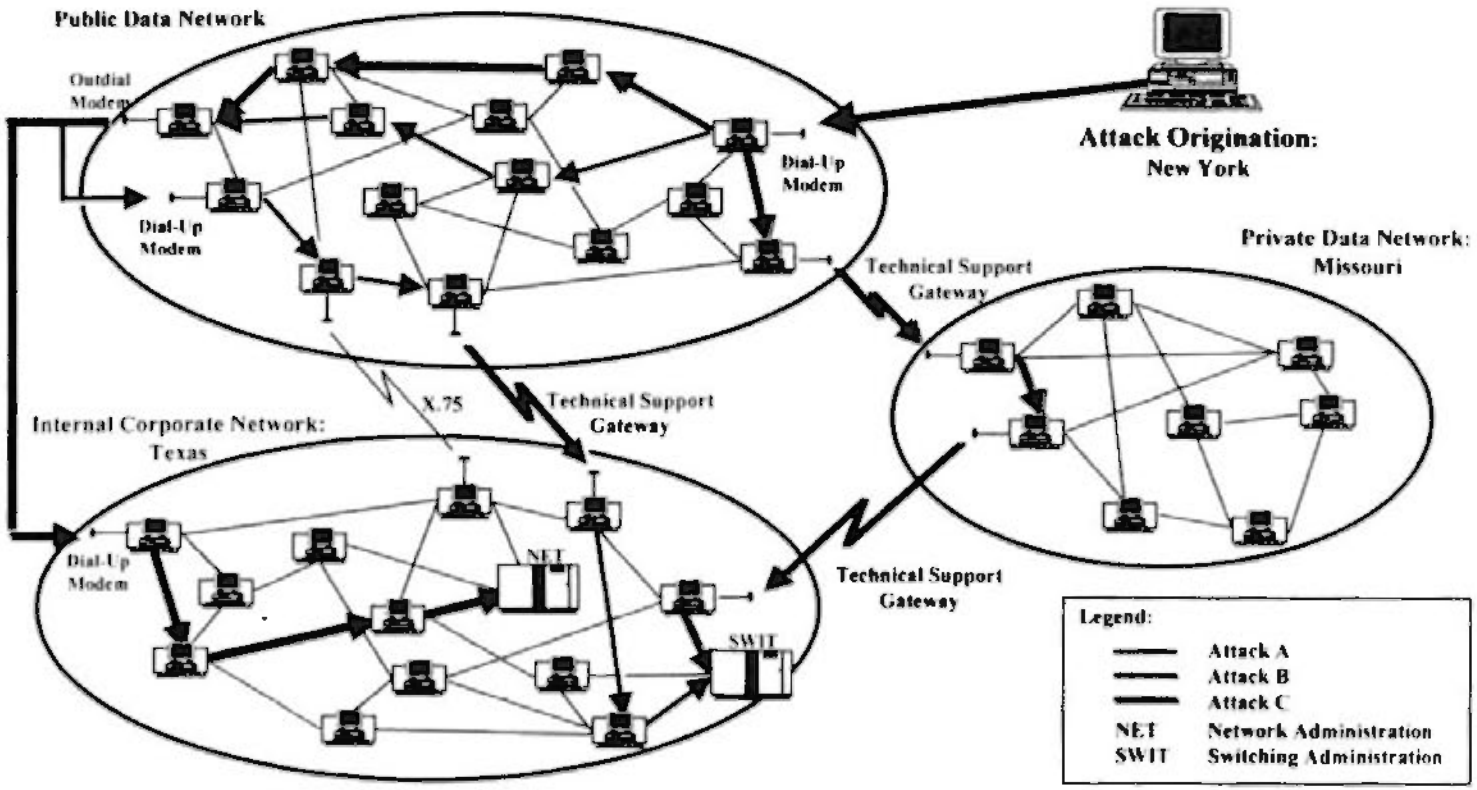


CCRS is a Registered Service Mark of Bellcore
SONET and SEAS are Registered Trademarks of Bellcore
1AESS, 5ESS, A-1 Net, 2A-STP, DATAKIT, and MACSTAR are Registered Trademarks of AT&T
DMS is a Registered Trademark of Northern Telecom
SCX is a Registered Trademark of Rockwell
TELENET is a Registered Trademark of Sprint
TYMNET is a Registered Trademark of British Telecom
MEGAHUB is a Registered Trademark of DSC Communications
AXE is a Registered Trademark of Ericsson
SSC-DCO is a Registered Trademark of Siemens Stromberg Carlson

Legend:	EADAS/NM - Engineering and Administrative Data Acquisition System/Network Management
	LMOS/MLT - Loop Maintenance and Operations System/Mechanized Loop Testing
	ALIT - Automatic Line Insulation Testing
	AMA/TPS - Automatic Message Accounting Teleprocessing System
	RCMAC - Recent Change Memory Administration Center
	COSMOS - Computer System for Mainframe Operations
	RMAS - Remote Memory Administration System
	MTCE - Maintenance
	STP - Signal Transfer Point
	DMS - Digital Multiplex System
	DCS - Digital Cross-connect System
	ESAC - Electronic Surveillance Assistance Center
	NMA - Network Monitoring and Analysis System
	SCCS - Switching Control Center System
	SCP - Signal Control Point
	SEAS - Signaling Engineering and Administration System
	SMS - Service Management System
	AIS - Automatic Intercept System
	BVA - Billing Validation Application
	DBAS - Database Administration System

Understanding the Risks

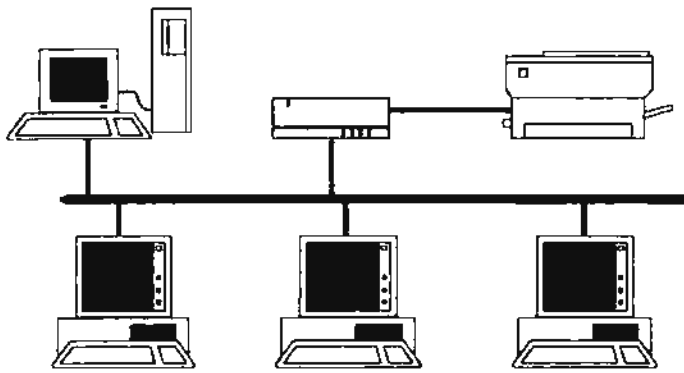
Data Network Vulnerabilities:
Attack Scenario



Understanding the Risks

Computer Networks Have A Long History Of Intrusions

⇨ *The Computer Emergency Response Team (CERT) And Other Similar Bodies Have Averaged 3 Advisories A Month For The Past 8 Years. . .*



CA-94:15 NFS Vulnerabilities
VB-94:02 ULTRIX OSF/1 Vulnerabilities
CA-94:12 Sendmail Vulnerabilities
F-06 Novell UnixWare Vulnerabilities
VB-94:01 SCO System Software Vulnerabilities
F-07 New & Revised HP Bulletins
D-04 SunOS Security Patches
93-29 Sendmail Exploitation
CA-92-14 Altered System Binaries
92-07 Attempts to Steal Passwords
92-09 Automated TFTP Probes
92-53 UNIX System V Security Problem
92-70 Cisco Access List Vulnerability
CA-92:19 Keystroke Logging Banner
CA-92:16 VMS Monitor Vulnerability
DDN05 ULTRIX 3.0 BREAK-IN
CA-91:14 SGI "IRIX" Vulnerability
C-21 AIX REXD Daemon Vulnerability
A-1 UNIX TFTP Attacks
A-22 Hacker/Cracker Attacks

Understanding the Risks

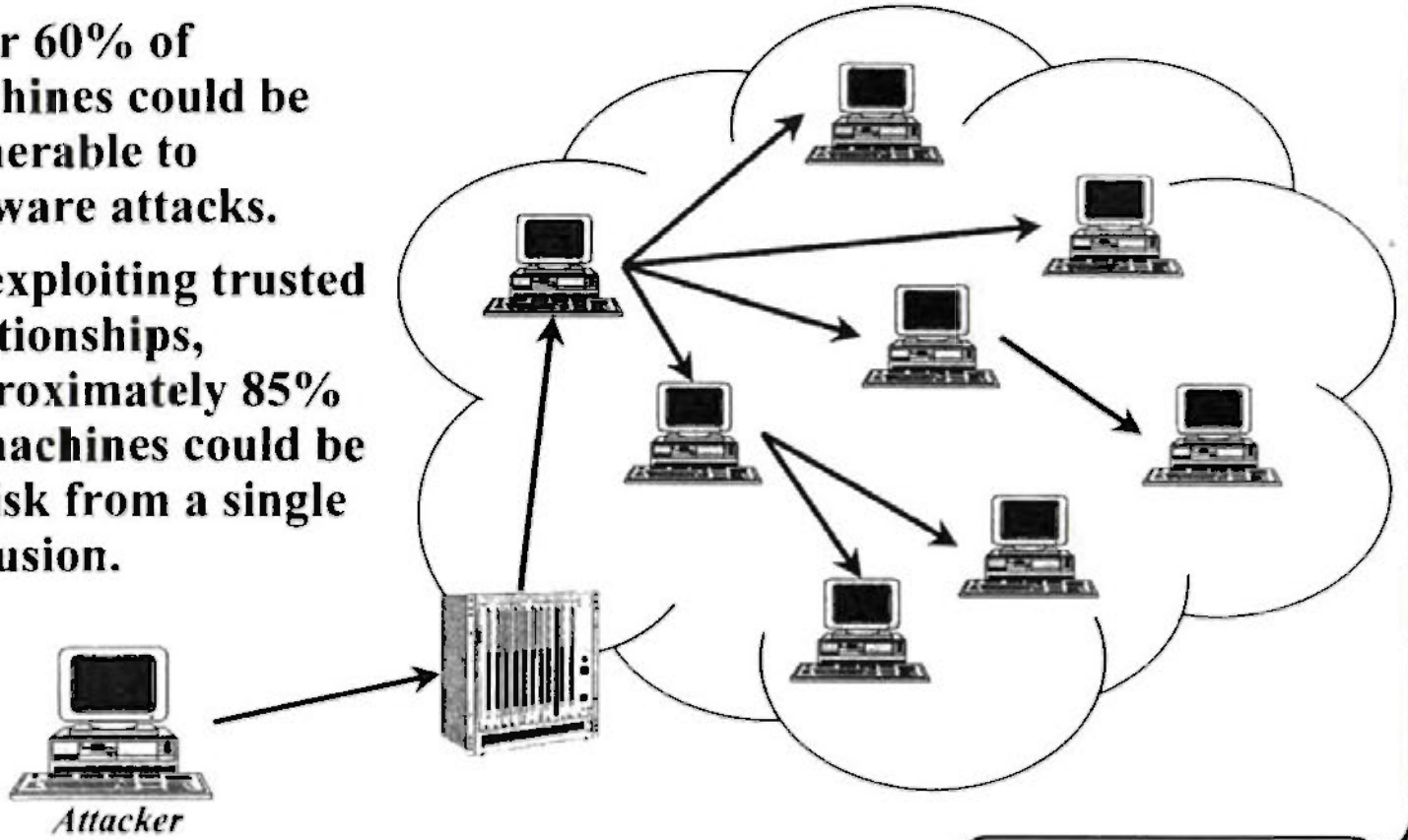
The Internet Security "Dirty Dozen"

• Trusted Host Relationships	"+" in .hostequiv file
• Network File System	World readable/writable
• Xwindows Vulnerabilities	Keystroke capture
• Rexec/Rexecd	Remote execution without authentication
• TFTP	Access without authentication
• FTP Servers	Default login/password on PCs, Macs, Novell
• Anonymous FTP	Check for writable areas, encrypted password file
• Ybind/Ypserv	Domain name server weaknesses
• Default Logins	bin, lp, guest, sysadm, demo, ftp, root, field
• Weak/Null Passwords	Easily guessable, null passwords
• CGI Script Vulnerabilities	Web server vulnerabilities
• Sendmail	A new vulnerability every week!

Understanding the Risks

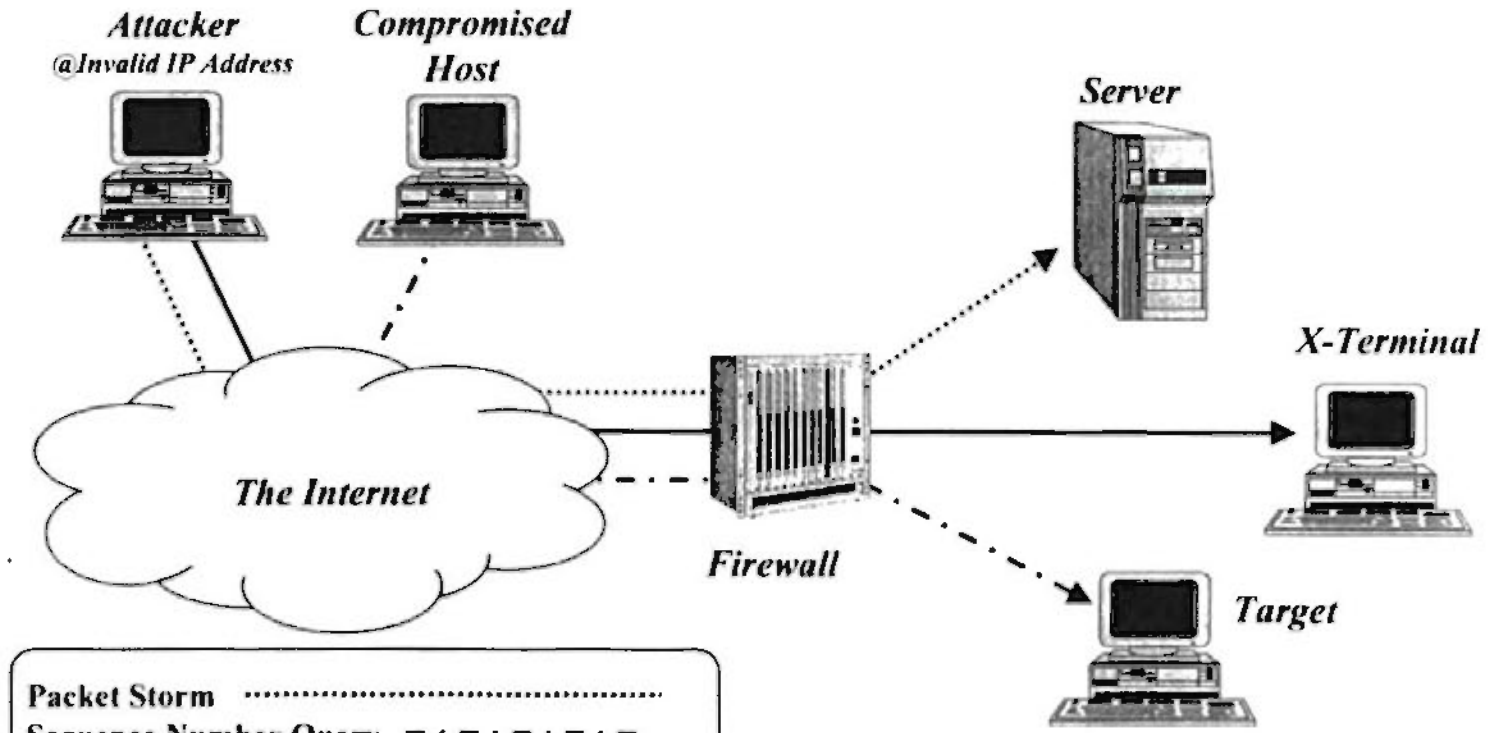
Exploitation Of Trusted Relationships

- Over 60% of machines could be vulnerable to software attacks.
- By exploiting trusted relationships, approximately 85% of machines could be at risk from a single intrusion.



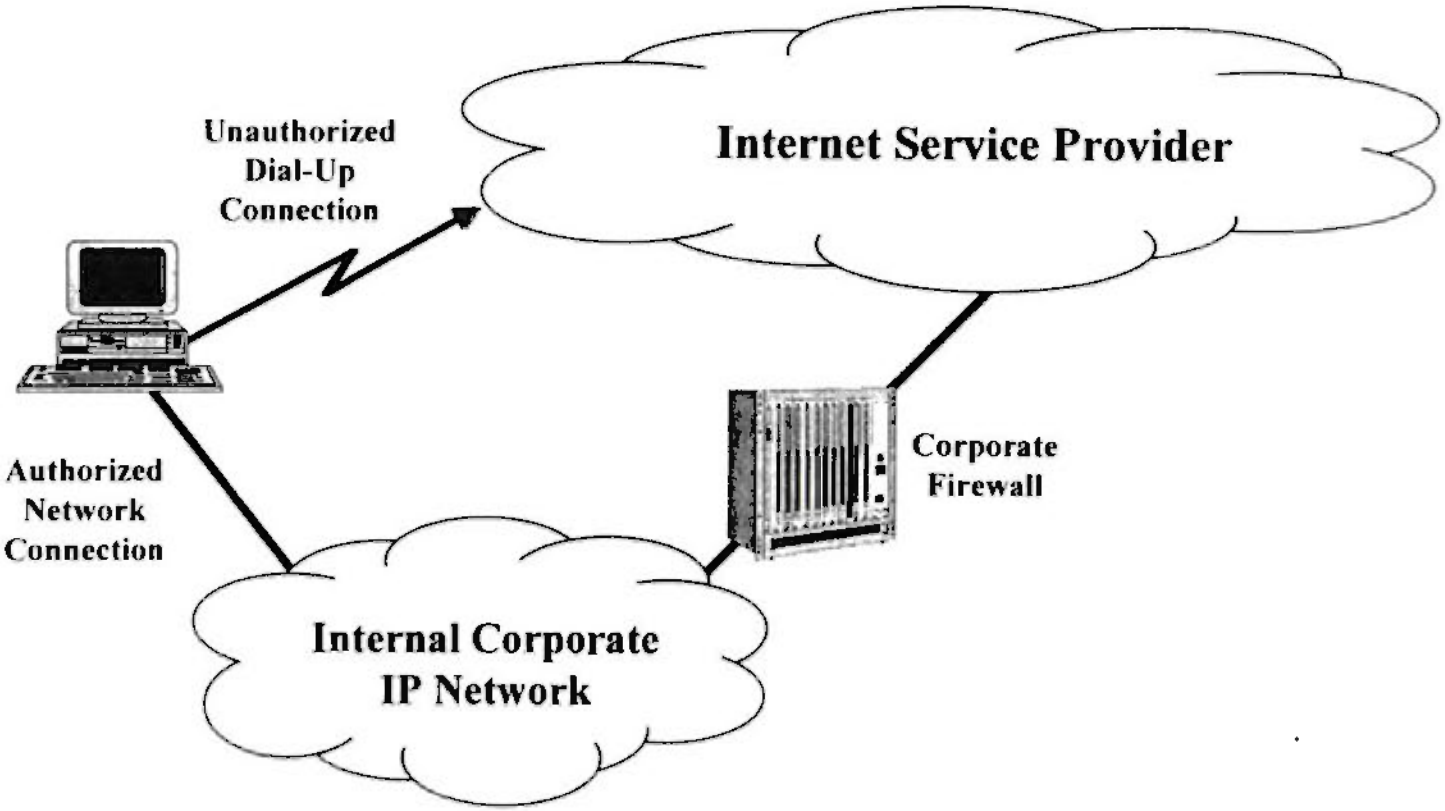
Understanding the Risks

The IP Spoofing Attack



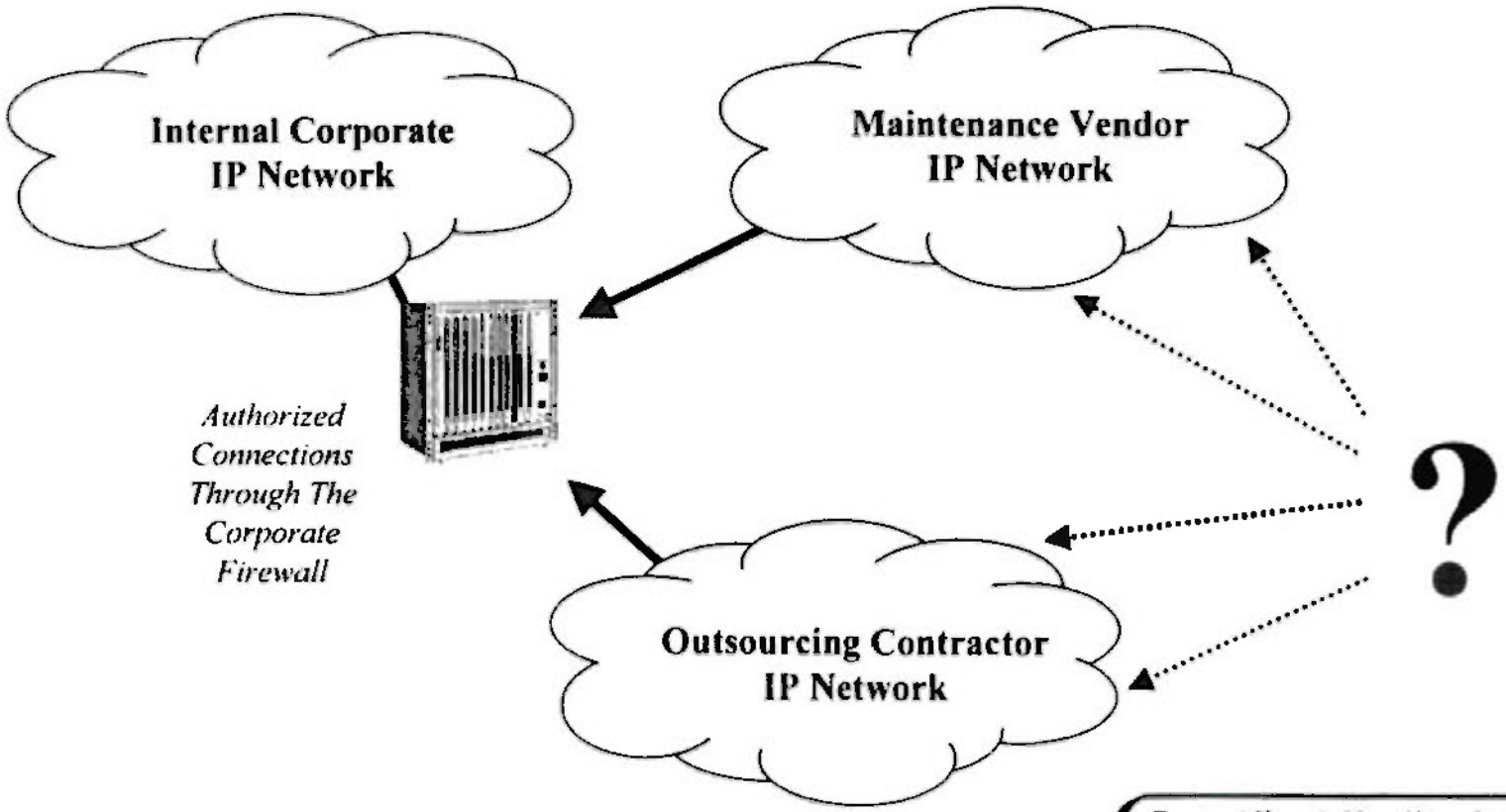
Understanding the Risks

Network Configuration Issues

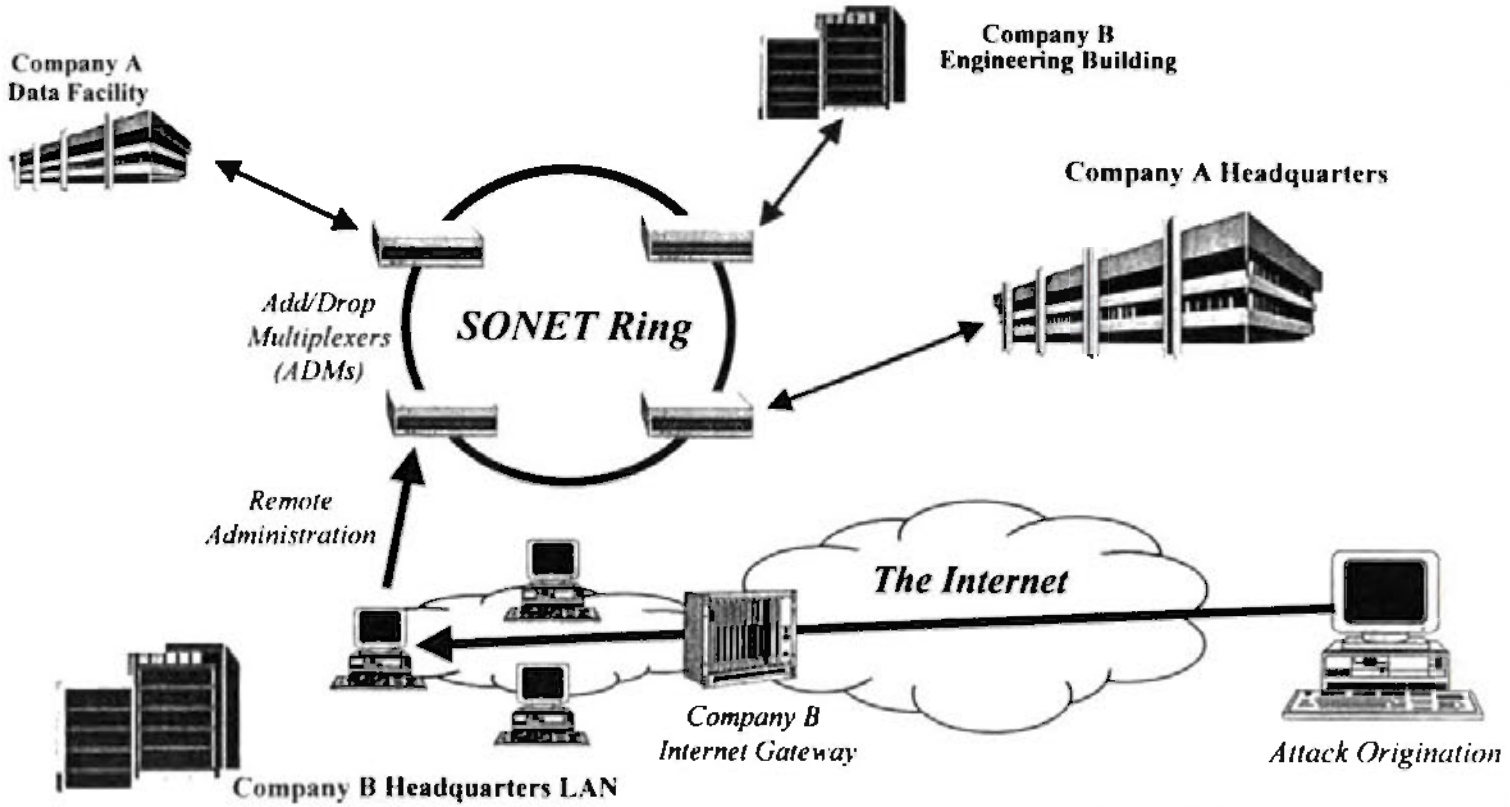


Understanding the Risks

Outsourcing And Vendor Issues

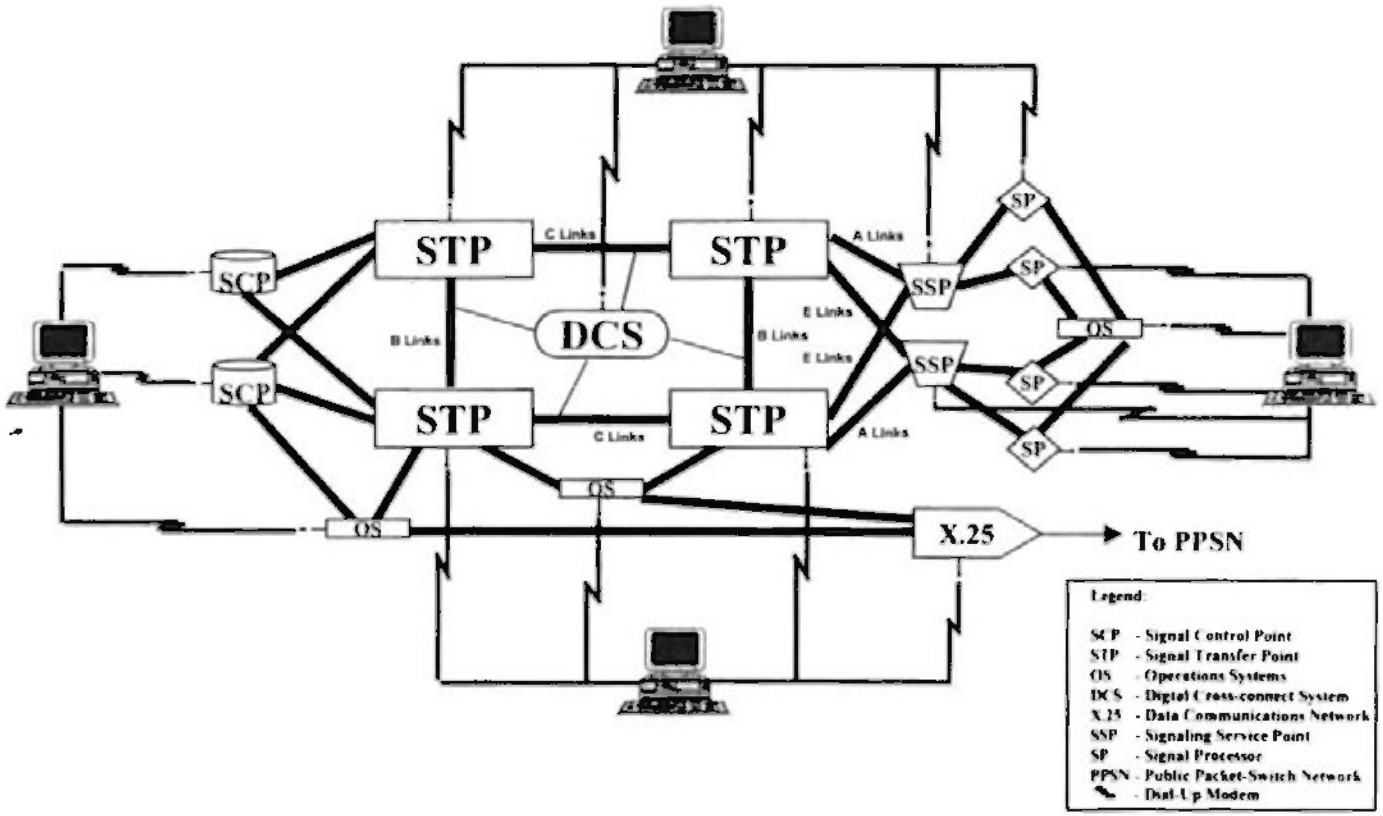


SONET Vulnerabilities



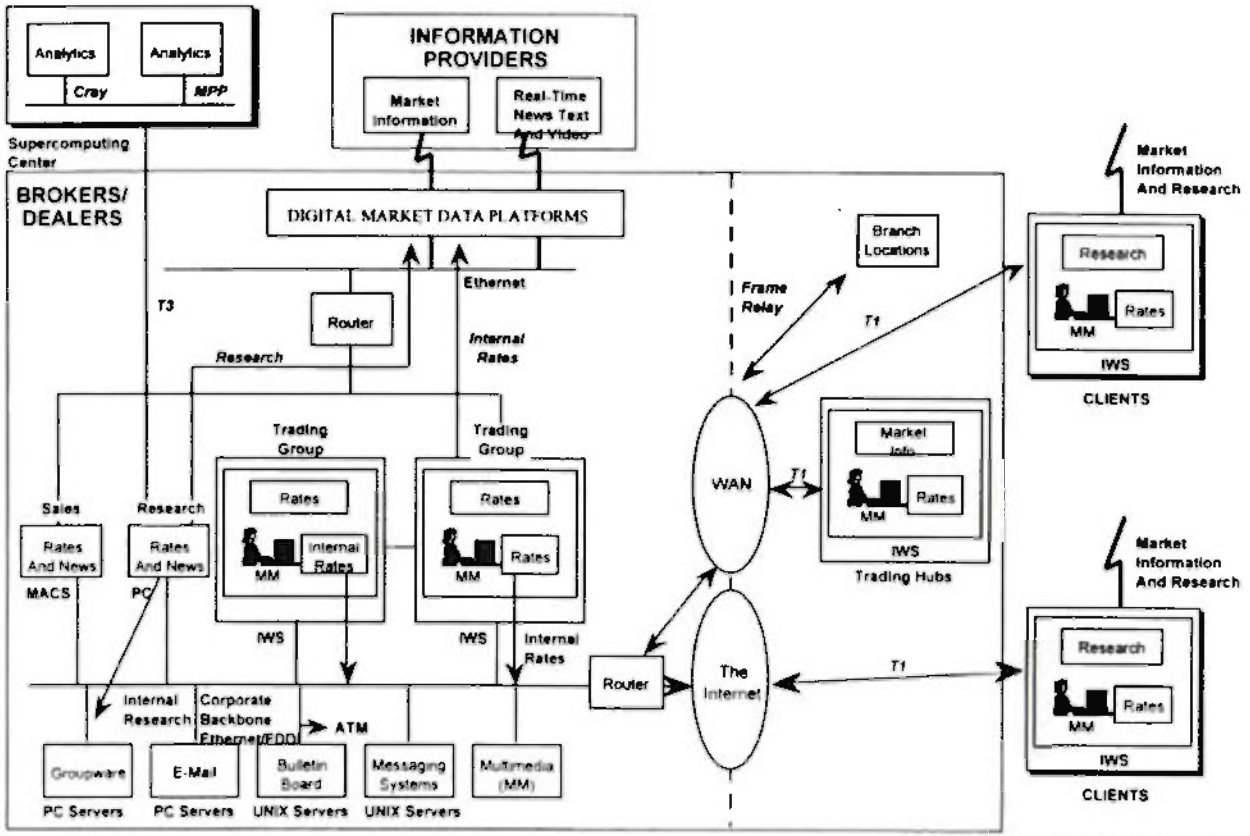
Understanding the Risks

Signaling System 7 (SS7) And Intelligent Network Vulnerabilities



Understanding the Risks

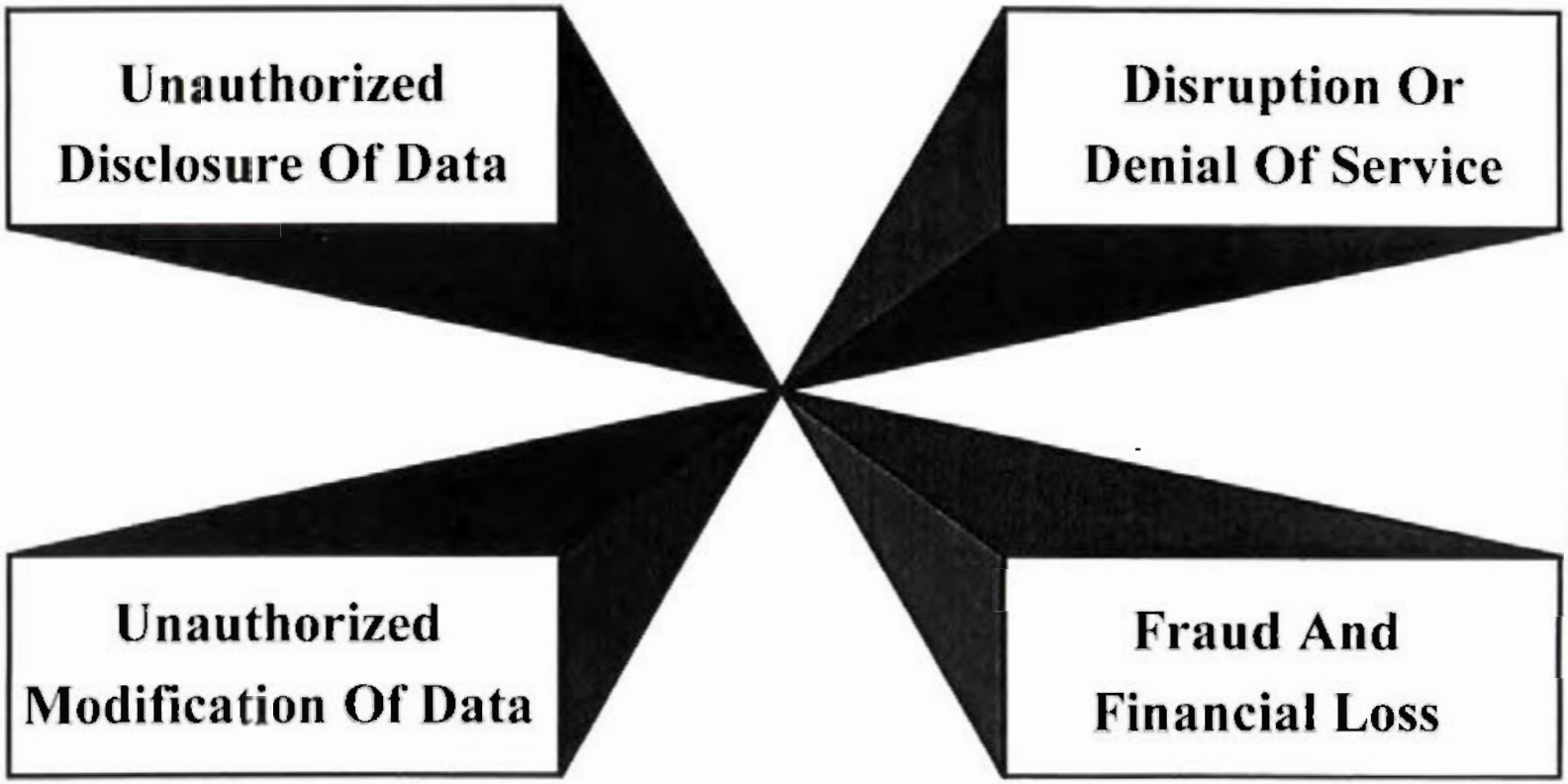
Financial Systems Are Completely Dependent On Networks



THREATS AND CASE HISTORIES

Threats And Case Histories

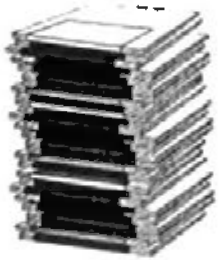
The Primary Threats To Network Technologies



Hacker Toolkits

Include:

- Highly targeted, custom scripted attacks
- Automated attack tools
- Sophisticated surveillance & data gathering tools
- Offensive use of network management tools
- Complex stealth & evasion techniques
- Password cracking tools
- Network element attack techniques



Case Histories

- Masters Of Deception (MOD)
- Kevin Poulsen
- Kevin Mitnick
- Legion Of Doom (LOD)
- The Posse And Internet Attacks
- Shadowhawk

+ Countries With Significant Hacker Activity

Masters Of Deception (MOD)

- Developed And Unleashed "Programmed Attacks" On Telephone Company Computers
- Monitored Data Transmissions On Packet Data Networks
- Created New Telephone Circuits And Add Services With No Billing Records
- Changed An Adversary's Long Distance Carrier To Illegally Obtain Calling Records
- Sold Passwords, Access Codes, and Other Illegally-Obtained Information
- Destroyed Data In Computer Systems

Threats And Case Histories

Kevin Poulsen

aka "Dark Dante"

Allegedly. . .

- **Hacked Into Phone Company Computers Hundreds Of Times**
- **Used Stolen Access Codes To Access Government Information And Sold Access Codes For Money**
- **Compromised Several Ongoing Law Enforcement Investigations**
- **Eavesdropped On Telephone Company Investigators**
- **Sold Untraceable, Unbilled Circuits To Criminals**
- **Illegally Entered Telephone Company Offices And Stole Data And Equipment**

Threats And Case Histories

Kevin Mitnick

aka "Condor"

Allegedly. . .

- **Attacked Telephone Central Offices**
- **Stole Telco Equipment & Manuals**
- **Attacked DEC's Software Development ComputerAnd Copied Proprietary Source Code Programs For The VAX/VMS Operating System**
- **Modified This Stolen Source Code To Introduce A "Trap Door"**
- **Compromised Cellular Telephone Network Equipment**
- **Implemented IP Spoofing Attack**

Legion Of Doom (LOD)

- Planted Software Time Bombs In Telephone Switching Centers
- Corrupted Pointer Tables In Signaling Switches

- Changed Circuit Routing Tables In Traffic Switches
- Electronically Eavesdropped On Telephone Conversations
- Traded Stolen Credit Card Numbers, Calling Card Numbers, And Computer System Information

The Posse And Internet Attacks

Allegedly. . .

- **Attacked Internet With "Sniffer" Programs Designed To Record Login IDs and Passwords**
- **Penetrated The Primary Internet Backbone Networks**
- **In First 6 Months, Sniffer Programs Were Discovered On Over 500,000 Internet Hosts—The Number May Now Be Over 1 Million**
- **Individual Sniffer Programs Have Captured Over 40,000 Passwords Per Day**
- **The Sniffer Is Now Part Of The Standard Hacker Toolkit, Along With Scanner Programs And The "Rootkit" Software**

Shadowhawk

- Illegally Copied The 5ESS Switching System Source Code Valued Between $28,000 And $40,000
- Illegally Copied Source Code Files Worth Over $1 Million
- Attacked A Telephone Carrier's Computers And Installed A "Trap Door" Password Allowing SysAdmin Access
- Accessed A Military Computer And Destroyed Diagnostic Files Reflecting The Operation Of The Military Base's Communication System
- Published Entry Codes To 27 Computers As Well As Legitimate Names, Telephone Numbers, Account Names, And Passwords

Threats And Case Histories

Countries With Significant Hacker Activity *

- Netherlands
- England
- Germany
- Belgium
- France
- Austria
- Sweden
- Switzerland
- Malaysia
- South Africa
- United States
- Canada
- Brazil
- Israel
- Australia
- Italy
- Greece
- Korea
- PRC
- Japan
- Hungary
- Czech Republic
- Bulgaria
- Russia
- Belarus
- Turkmenistan
- South Africa
- Spain
- Philippines
- Argentina

* Based On Unclassified Open Source Information

STRATEGIES TO REDUCE YOUR RISK EXPOSURE

Conclusions

- → All Aspects Of Worldwide Communications Networks Are At Risk From Electronic Intruders
- → Electronic Intrusions Are Escalating In Frequency & Severity
- → New Technologies And Other Industry Trends Are Increasing Risks To Both End Users And System Operators

Risk Management

- **Risk Can Not Be Eliminated Entirely, But It Can Be *Effectively Managed***
- **Your Risk Exposure Can Be Dramatically Reduced By Developing and Implementing An *Organizational Security Strategy***
  - **Organizational Security Policy**
  - **System Specific Security Policies**
  - **Detailed Seeurity Procedures**

- **Your Security Posture Should Reflect Management's Position On Security *Costs and Benefits.***

Risk Can Be Reduced By Implementing New Procedures

- Establish Security Awareness Programs
- Improve Security Staff Skills
- Perform Regular Security Audits
- Control Proprietary Information
- Use Existing Security Features In Equipment
- Implement Dial Access Control
- Identify and Close Security "Holes"
- Design & Implement A Security Architecture
- Implement Advanced Security Technologies

Less Complex

More Complex