Vulnerability Management:

Mitigating Your Company's Security Risks

Matt Tolbert, CISSP

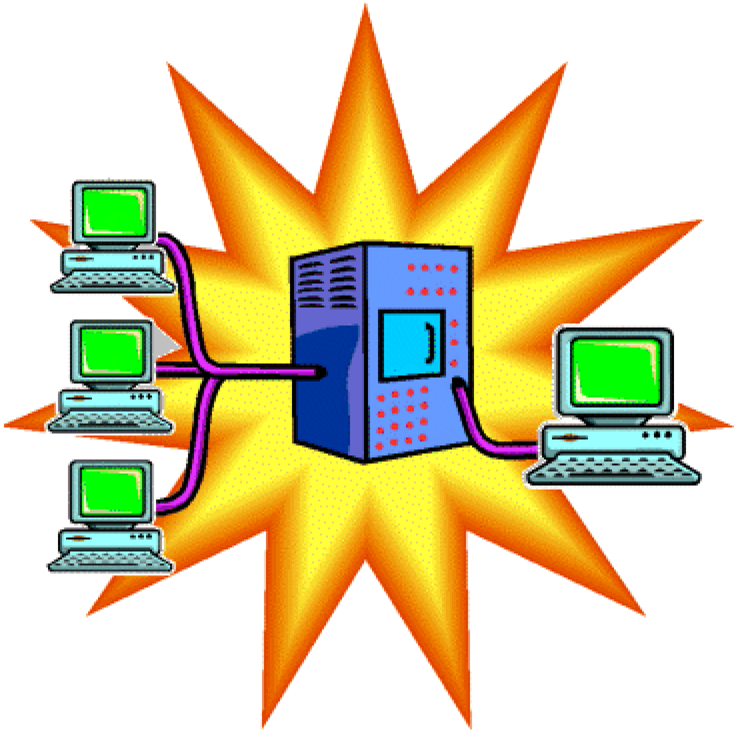
Senior Manager, Ernst & Young Security & Technology Solutions Group, New York City

HP WORLD 2002 Conference & Expo

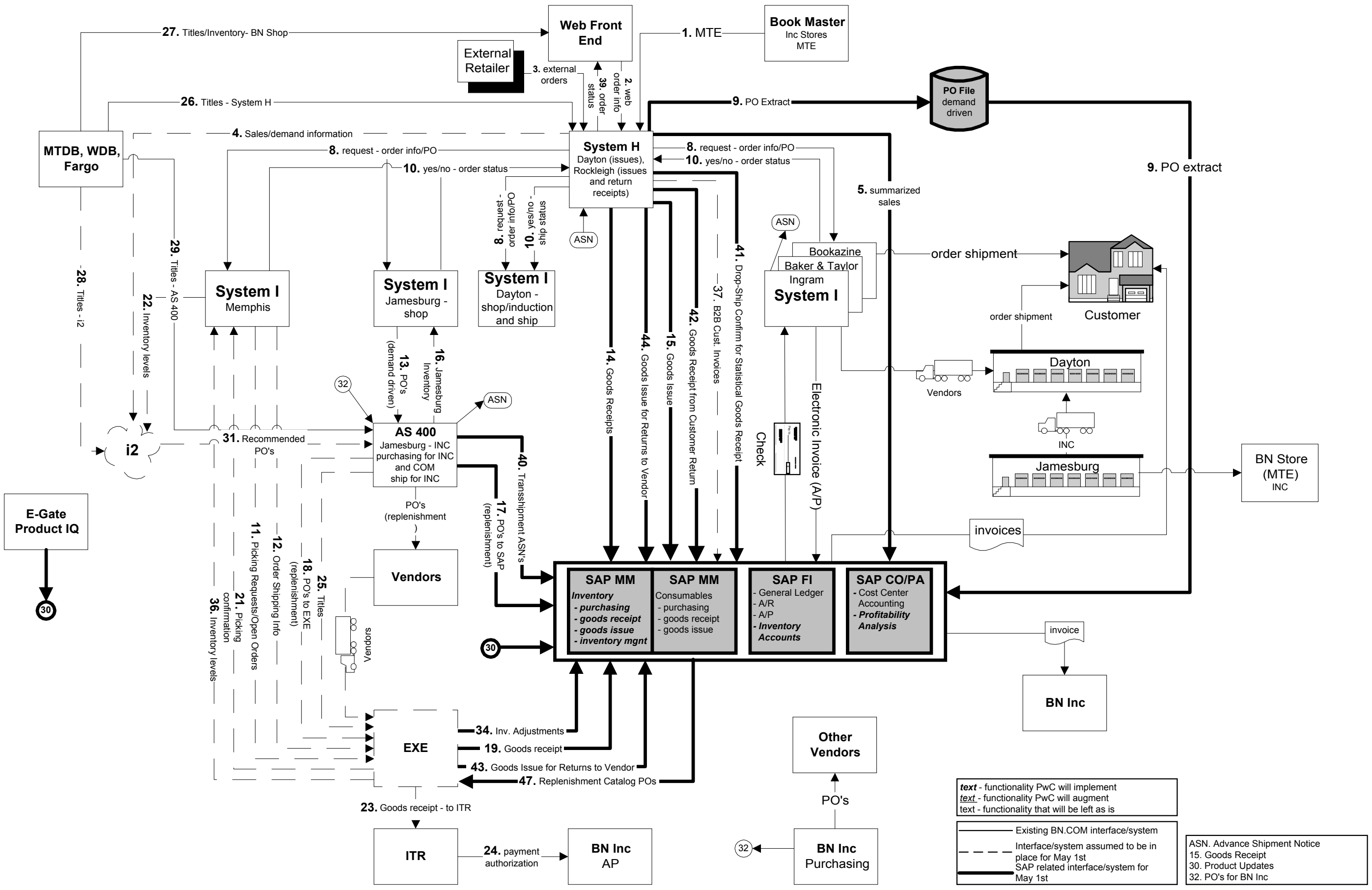
AGENDA:

1. Where are today’s security risks?
2. What are today’s solutions to mitigate risk?
3. How are others managing their security vulnerabilities?
4. How do I manage my company’s vulnerabilities?

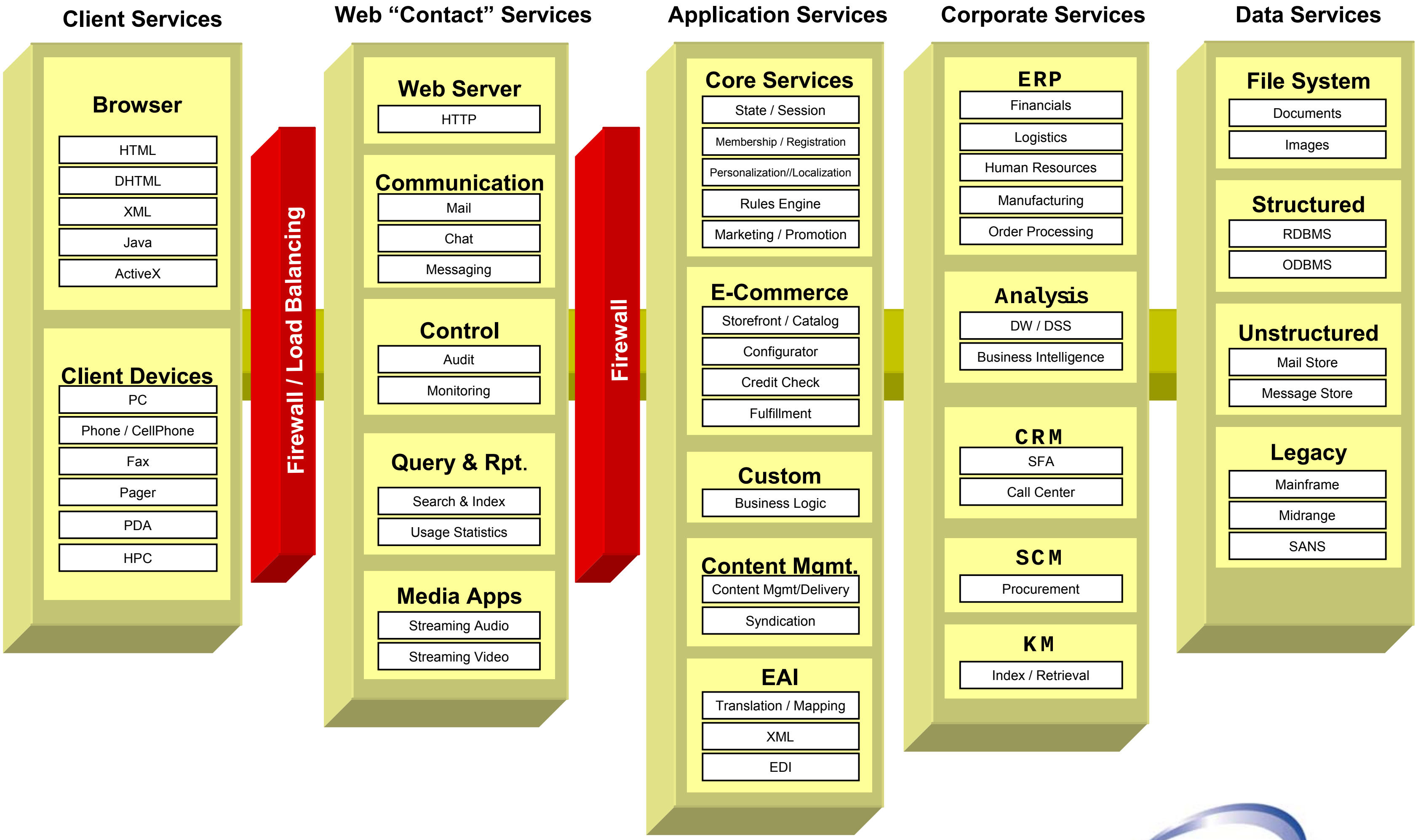
While simple is desirable…



…business processes are complex…



…application architectures are extensive…



Client Services

- **Browser**
  - HTML
  - DHTML
  - XML
  - Java
  - ActiveX
- **Client Devices**
  - PC
  - Phone / CellPhone
  - Fax
  - Pager
  - PDA
  - HPC

Firewall / Load Balancing

Web "Contact" Services

- **Web Server**
  - HTTP
- **Communication**
  - Mail
  - Chat
  - Messaging
- **Control**
  - Audit
  - Monitoring
- **Query & Rpt.**
  - Search & Index
  - Usage Statistics
- **Media Apps**
  - Streaming Audio
  - Streaming Video

Firewall

Application Services

- **Core Services**
  - State / Session
  - Membership / Registration
  - Personalization//Localization
  - Rules Engine
  - Marketing / Promotion
- **E-Commerce**
  - Storefront / Catalog
  - Configurator
  - Credit Check
  - Fulfillment
- **Custom**
  - Business Logic
- **Content Mgmt.**
  - Content Mgmt/Delivery
  - Syndication
- **EAI**
  - Translation / Mapping
  - XML
  - EDI

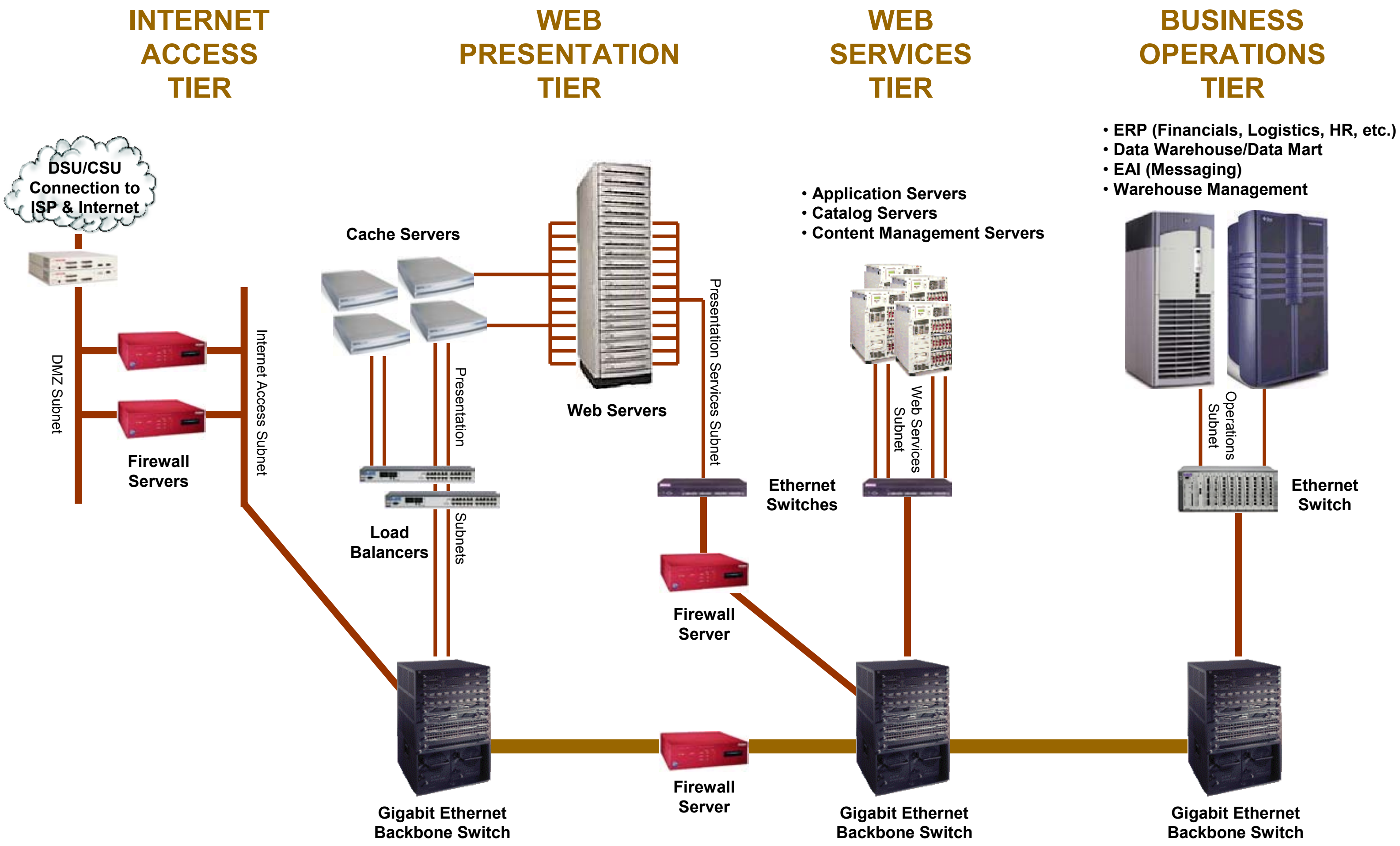
Corporate Services

- **ERP**
  - Financials
  - Logistics
  - Human Resources
  - Manufacturing
  - Order Processing
- **Analysis**
  - DW / DSS
  - Business Intelligence
- **CRM**
  - SFA
  - Call Center
- **SCM**
  - Procurement
- **KM**
  - Index / Retrieval

Data Services

- **File System**
  - Documents
  - Images
- **Structured**
  - RDBMS
  - ODBMS
- **Unstructured**
  - Mail Store
  - Message Store
- **Legacy**
  - Mainframe
  - Midrange
  - SANS

…and IT infrastructures are nontrivial…



HP WORLD 2002 Conference & Expo

…so the risk of exposure to security vulnerabilities are greater than ever.

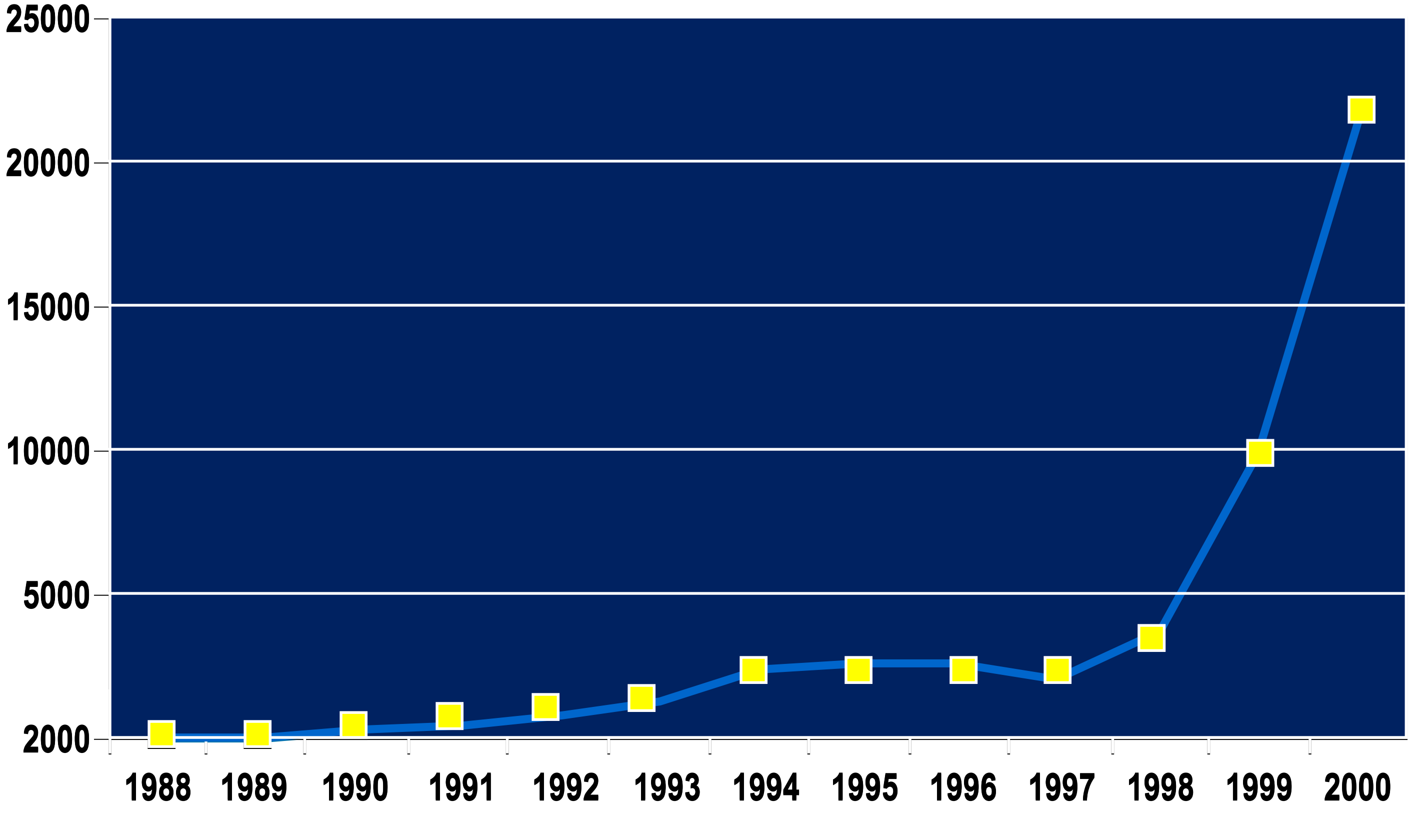
1. TODAY'S SECURITY RISKS

Where are Today's Security Risks?

- Malevolent actions and attacks—internal and external
- Unintended consequences due to lack of internal controls
- Non-compliance with government regulations
- Competitive intelligence
- Pervasive computing
- Integration of systems and applications

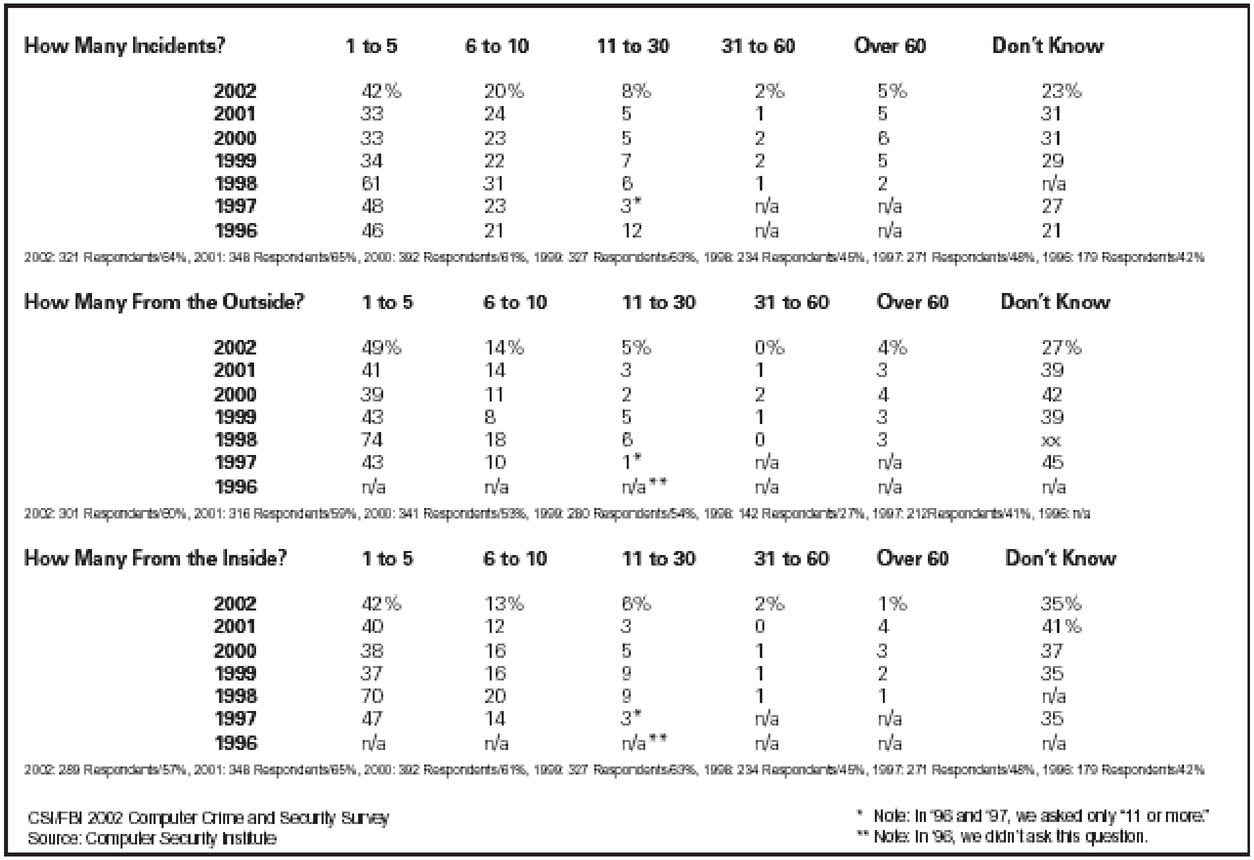
1.2 Today's Security Risks

Reported Security Incidents Growing



©2001 Carnegie Mellon University

Where Do These Incidents Originate?



How Many Incidents?	1 to 5	6 to 10	11 to 30	31 to 60	Over 60	Don't Know
2002	42%	20%	8%	2%	5%	23%
2001	33	24	5	1	5	31
2000	33	23	5	2	6	31
1999	34	22	7	2	5	29
1998	61	31	6	1	2	n/a
1997	48	23	3*	n/a	n/a	27
1996	46	21	12	n/a	n/a	21

2002: 321 Respondents/64%, 2001: 348 Respondents/65%, 2000: 392 Respondents/61%, 1999: 327 Respondents/63%, 1998: 234 Respondents/45%, 1997: 271 Respondents/48%, 1996: 179 Respondents/42%

How Many From the Outside?	1 to 5	6 to 10	11 to 30	31 to 60	Over 60	Don't Know
2002	49%	14%	5%	0%	4%	27%
2001	41	14	3	1	3	39
2000	39	11	2	2	4	42
1999	43	8	5	1	3	39
1998	74	18	6	0	3	xx
1997	43	10	1*	n/a	n/a	45
1996	n/a	n/a	n/a**	n/a	n/a	n/a

2002: 301 Respondents/60%, 2001: 316 Respondents/59%, 2000: 341 Respondents/53%, 1999: 280 Respondents/54%, 1998: 142 Respondents/27%, 1997: 212Respondents/41%, 1996: n/a

How Many From the Inside?	1 to 5	6 to 10	11 to 30	31 to 60	Over 60	Don't Know
2002	42%	13%	6%	2%	1%	35%
2001	40	12	3	0	4	41%
2000	38	16	5	1	3	37
1999	37	16	9	1	2	35
1998	70	20	9	1	1	n/a
1997	47	14	3*	n/a	n/a	35
1996	n/a	n/a	n/a**	n/a	n/a	n/a

2002: 289 Respondents/57%, 2001: 348 Respondents/65%, 2000: 392 Respondents/61%, 1999: 327 Respondents/63%, 1998: 234 Respondents/45%, 1997: 271 Respondents/48%, 1996: 179 Respondents/42%

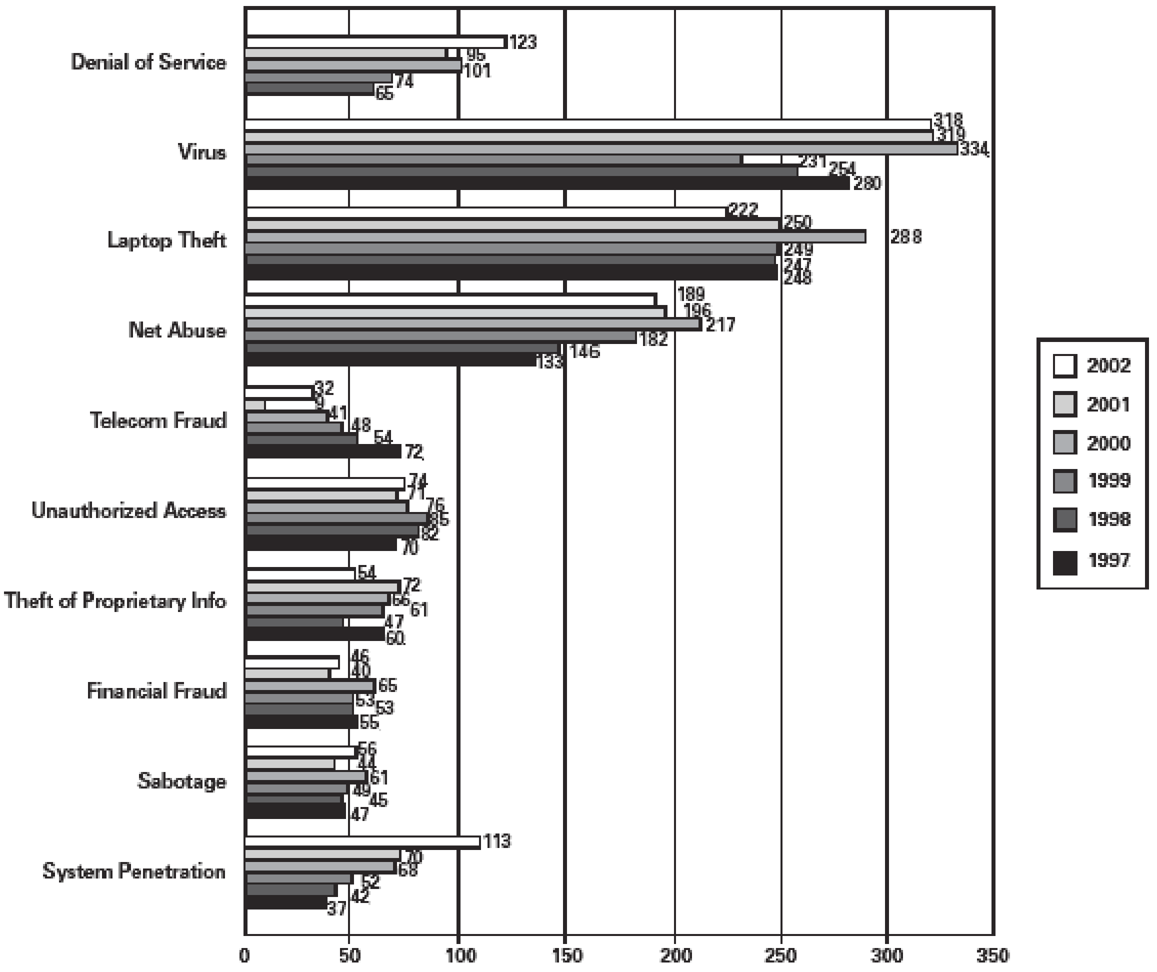
CSI/FBI 2002 Computer Crime and Security Survey
Source: Computer Security Institute

* Note: In '96 and '97, we asked only "11 or more."
** Note: In '96, we didn't ask this question.

Internal & external sources of risks are nearly equivalent

1.4 *Today's Security Risks*

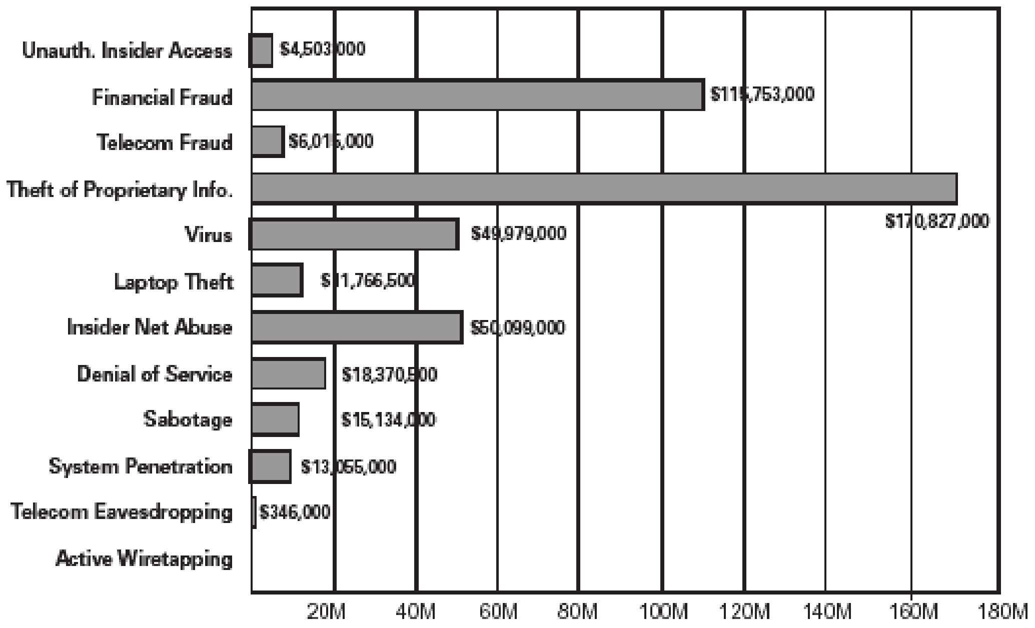
Cited Security Vulnerabilities



What are the Consequences?

- Financial losses
  - Direct loss of revenue
  - Costs to recover and remedy
  - Insurance recovery and premiums
- Public perception and brand recognition
- Customer impact
- Government regulatory compliance
  - Fines
  - Imprisonment

Financial Impact of Security Vulnerabilities



Dollar Amount of Losses by Type

CSI/FBI 2002 Computer Crime and Security Survey
Source: Computer Security Institute

2002: 223 respondents/44%

Attack Trends

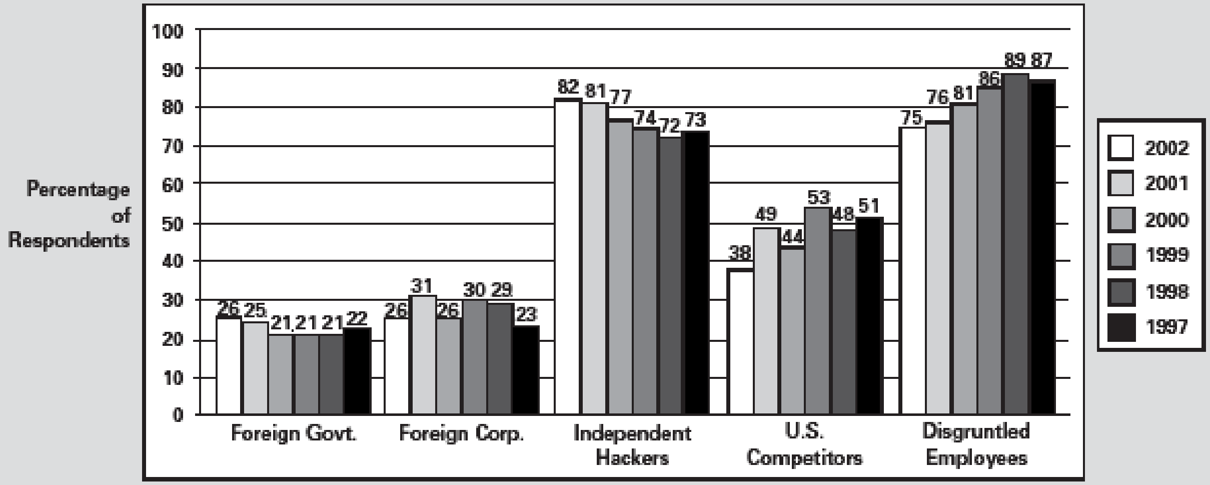
- Automated attacks through new tools
- Increasing sophistication of attack tools
- Faster discovery of vulnerabilities
- Increasing permeability of firewalls
- Increasingly asymmetric threats
- Increasing threat from infrastructure attacks

Speed of Attack: Honeypot Findings

- Server discovered in under 20 minutes
- Vulnerability scans commence in under 2 hours
- Concerted intrusion attempts in under 2-3 days
- Discovery of vulnerability after initial intrusion on average of 5 minutes

1.9 *Today’s Security Risks*

Likely Sources of Attack

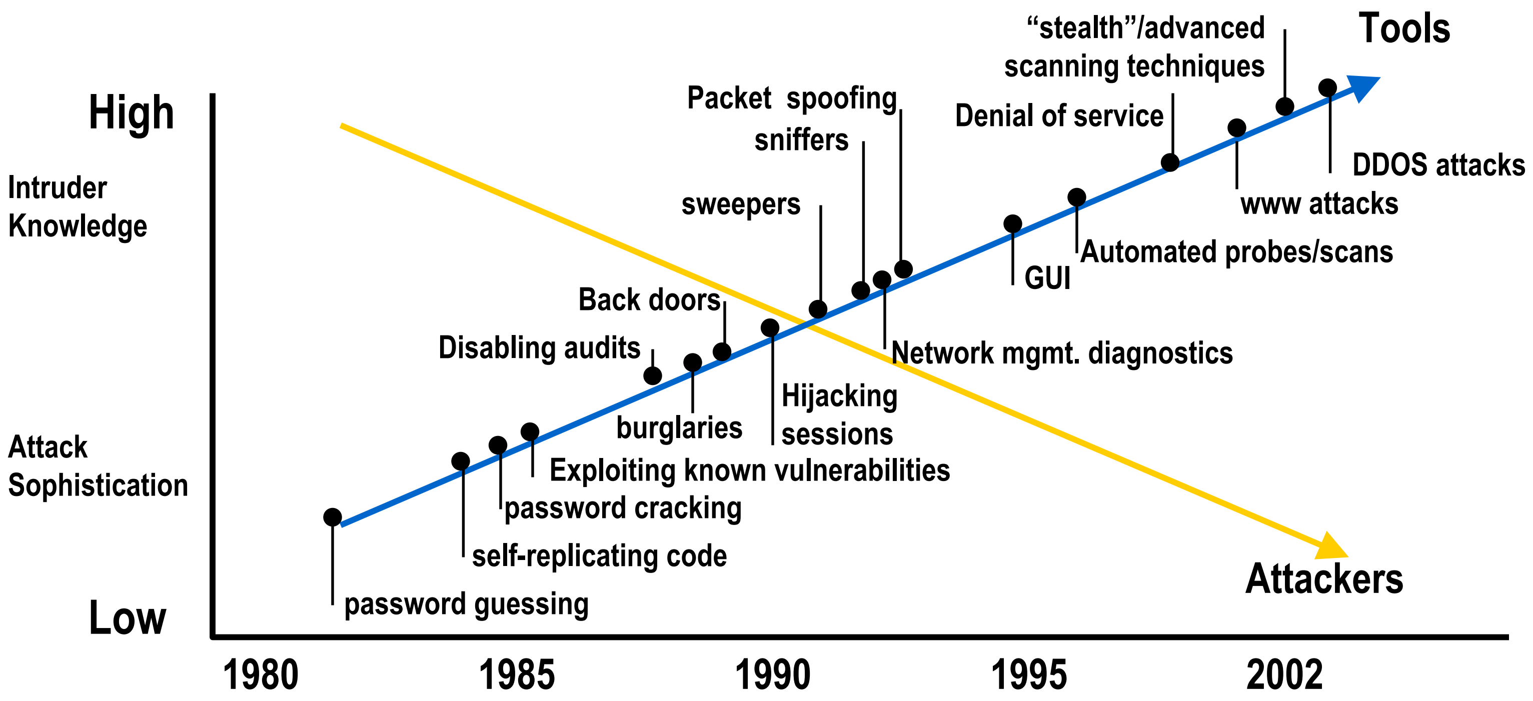


2002: 414 Respondents/82%
2001: 484 Respondents/91%
2000: 583 Respondents/90%
1999: 460 Respondents/88%
1998: 428 Respondents/54%
1997: 503 Respondents/89%

CSI/FBI 2002 Computer Crime and Security Survey
Source: Computer Security Institute

1.10 Today's Security Risks

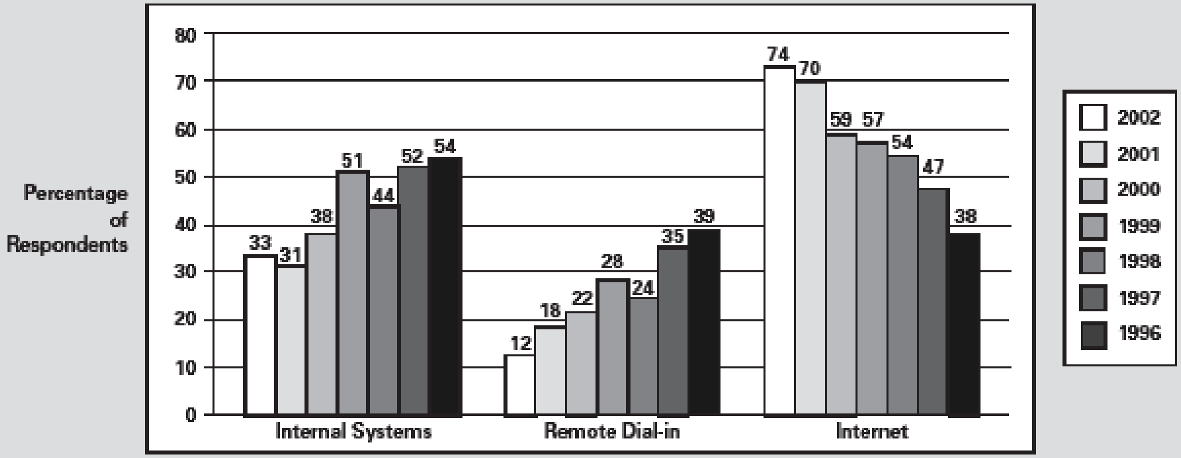
Sophistication of Attacks Increasing



©2001 Carnegie Mellon University

1.11 Today’s Security Risks

Internet the Most Common Point of Attack

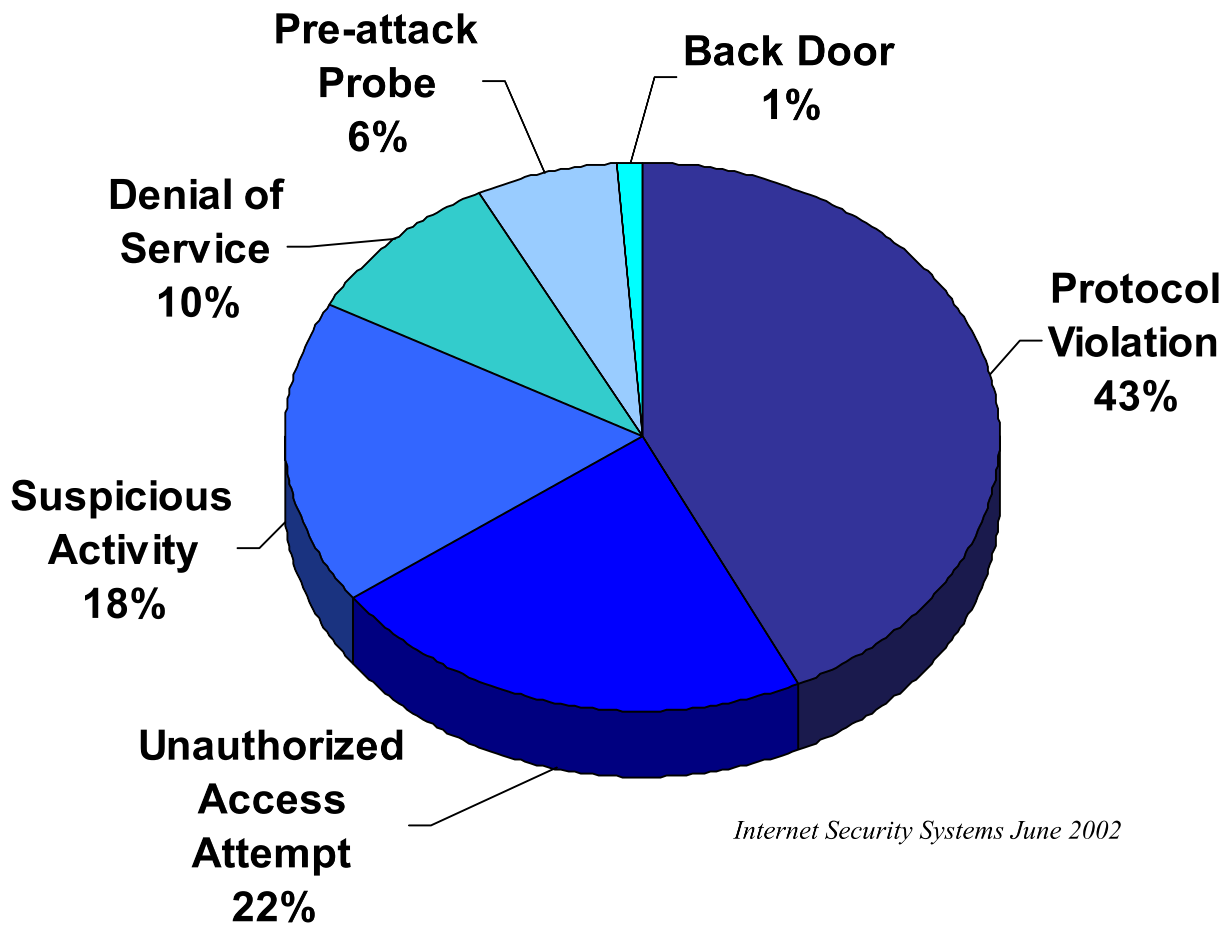


2002: 481 Respondents/96%
2001: 384 Respondents/72%
2000: 443 Respondents/68%
1999: 324 Respondents/62%
1998: 279 Respondents/54%
1997: 391 Respondents/69%
1996: 174 Respondents/40%

CSI/FBI 2002 Computer Crime and Security Survey
Source: Computer Security Institute

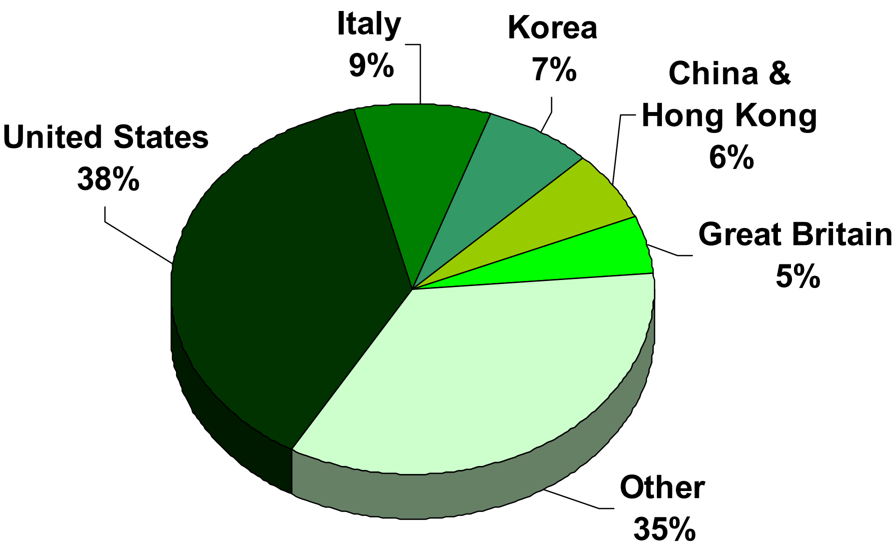
HP WORLD 2002
Conference & Expo

Attack Trends: Top Attack Categories

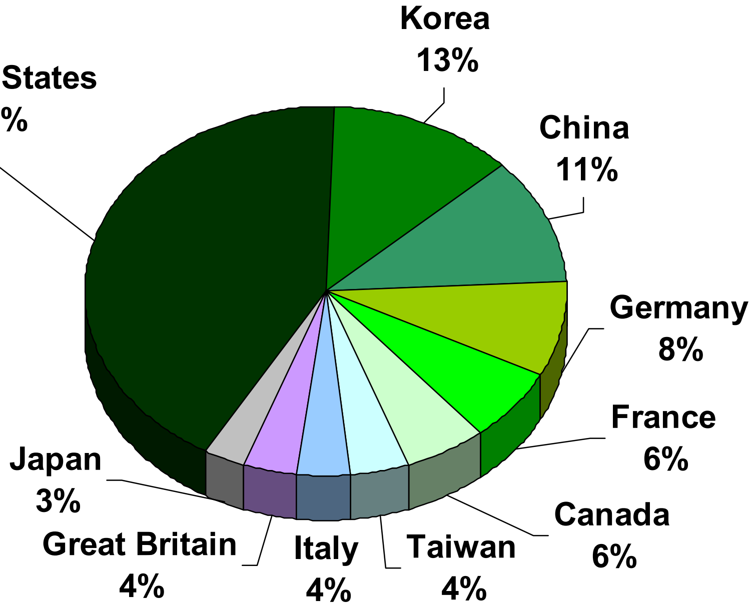


Internet Security Systems June 2002

Attack Trends: Top Attack Sources

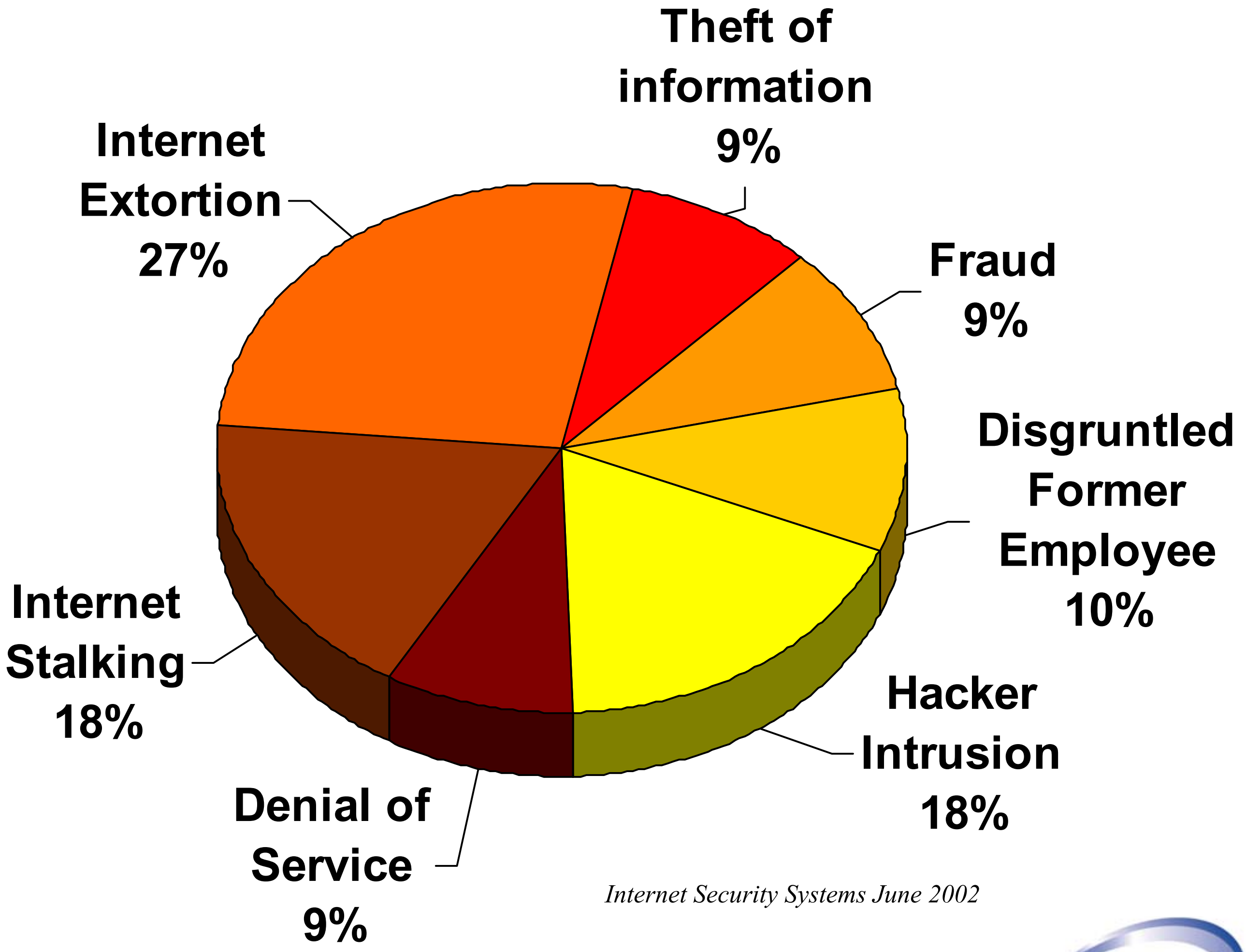


Internet Security Systems June 2002



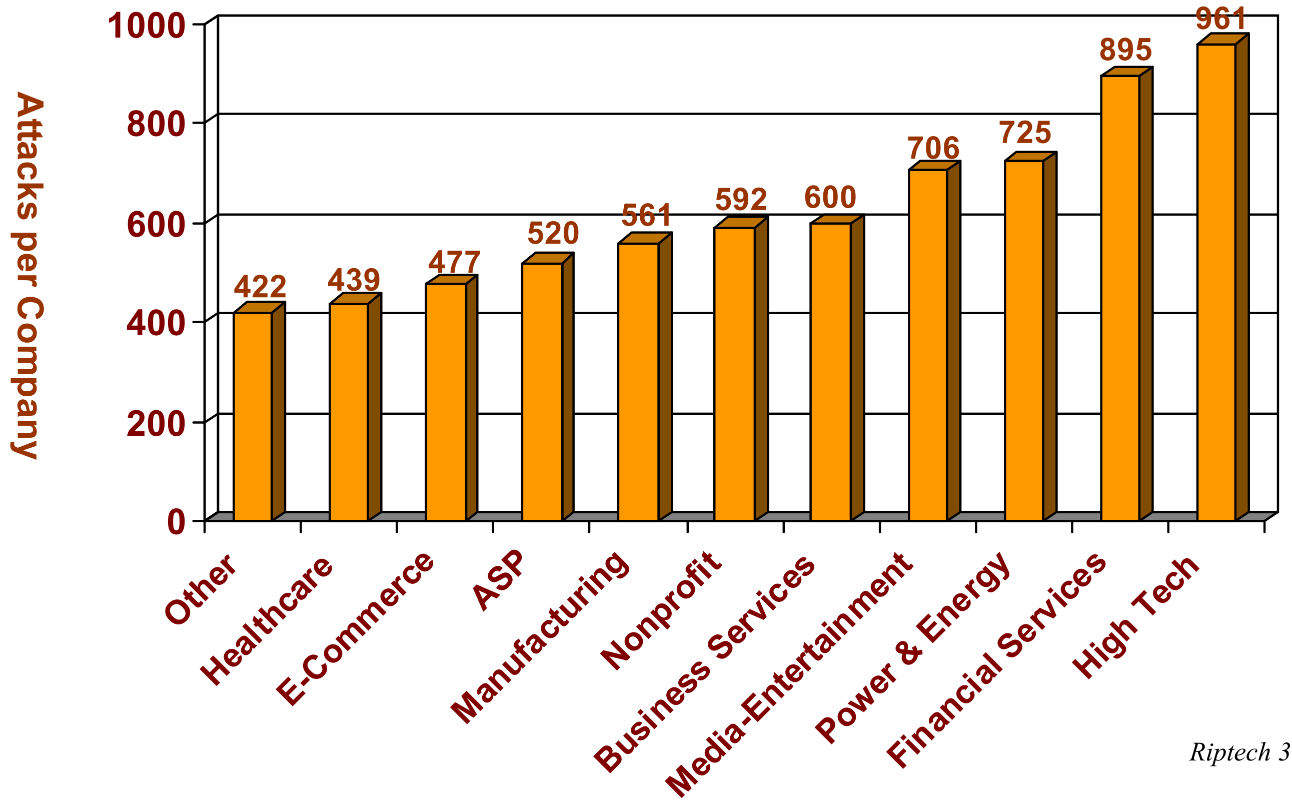
Riptech 3-4Q2001

Attack Trends: Top Declared Emergencies



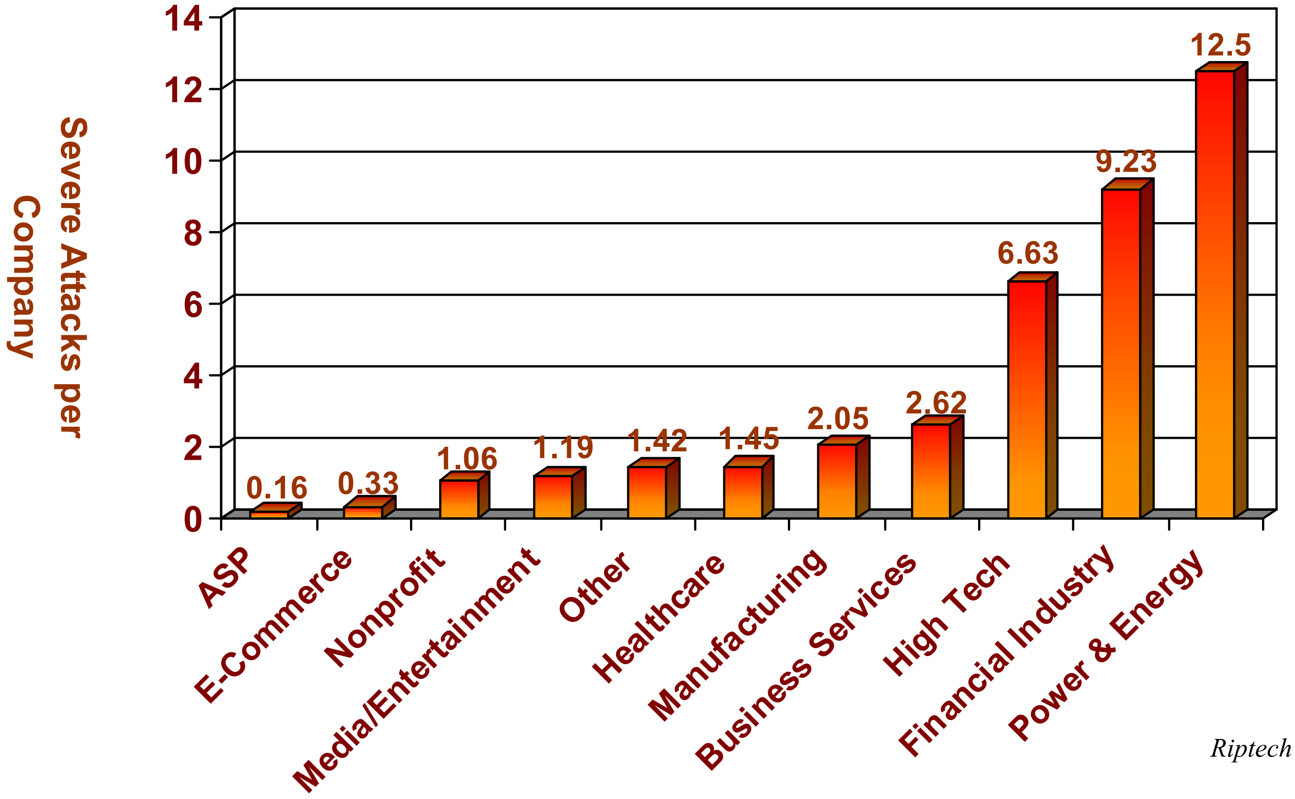
Internet Security Systems June 2002

Attack Trends: Attacks by Industry



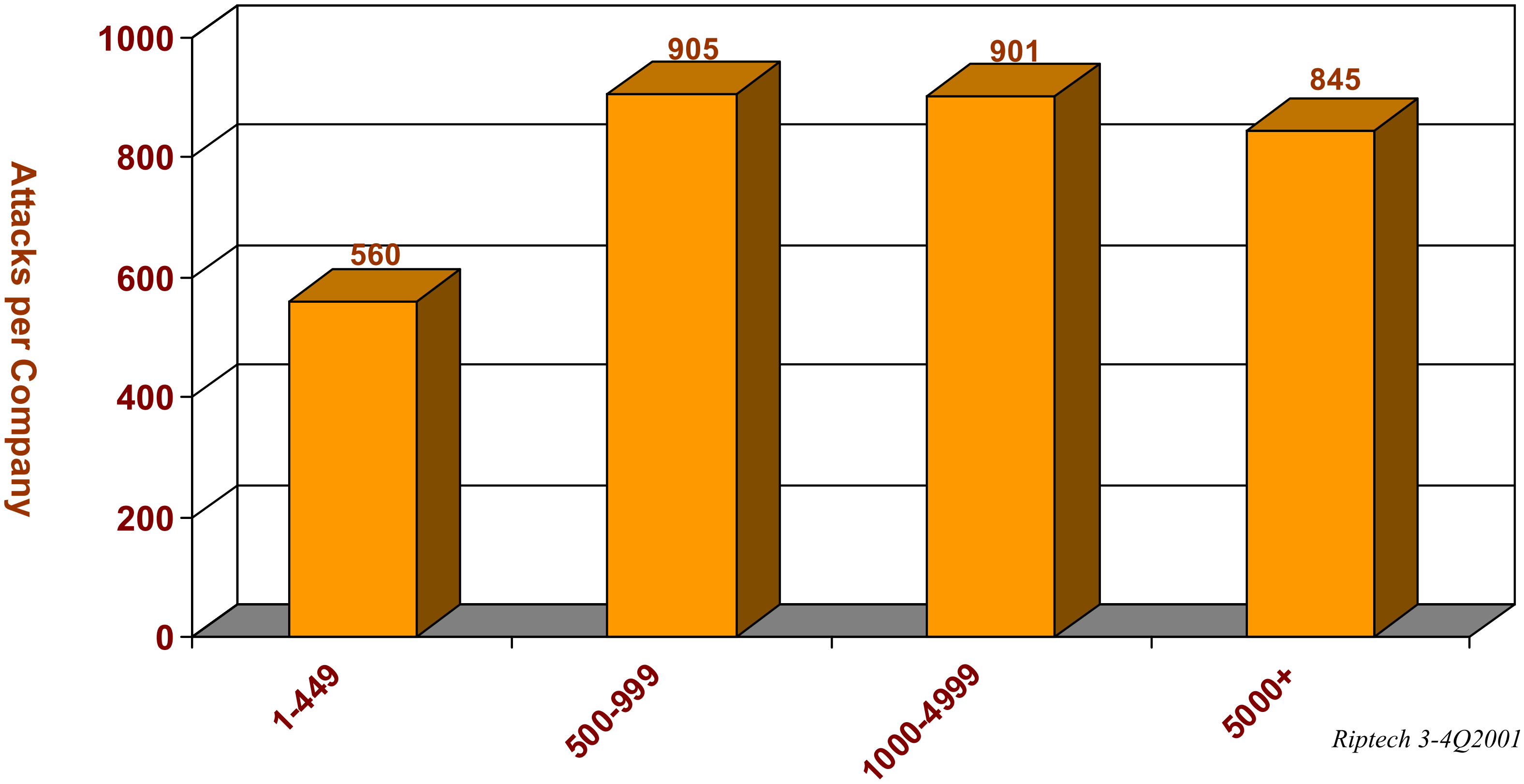
Riptech 3-4Q2001

Attack Trends: Severe Attacks by Industry



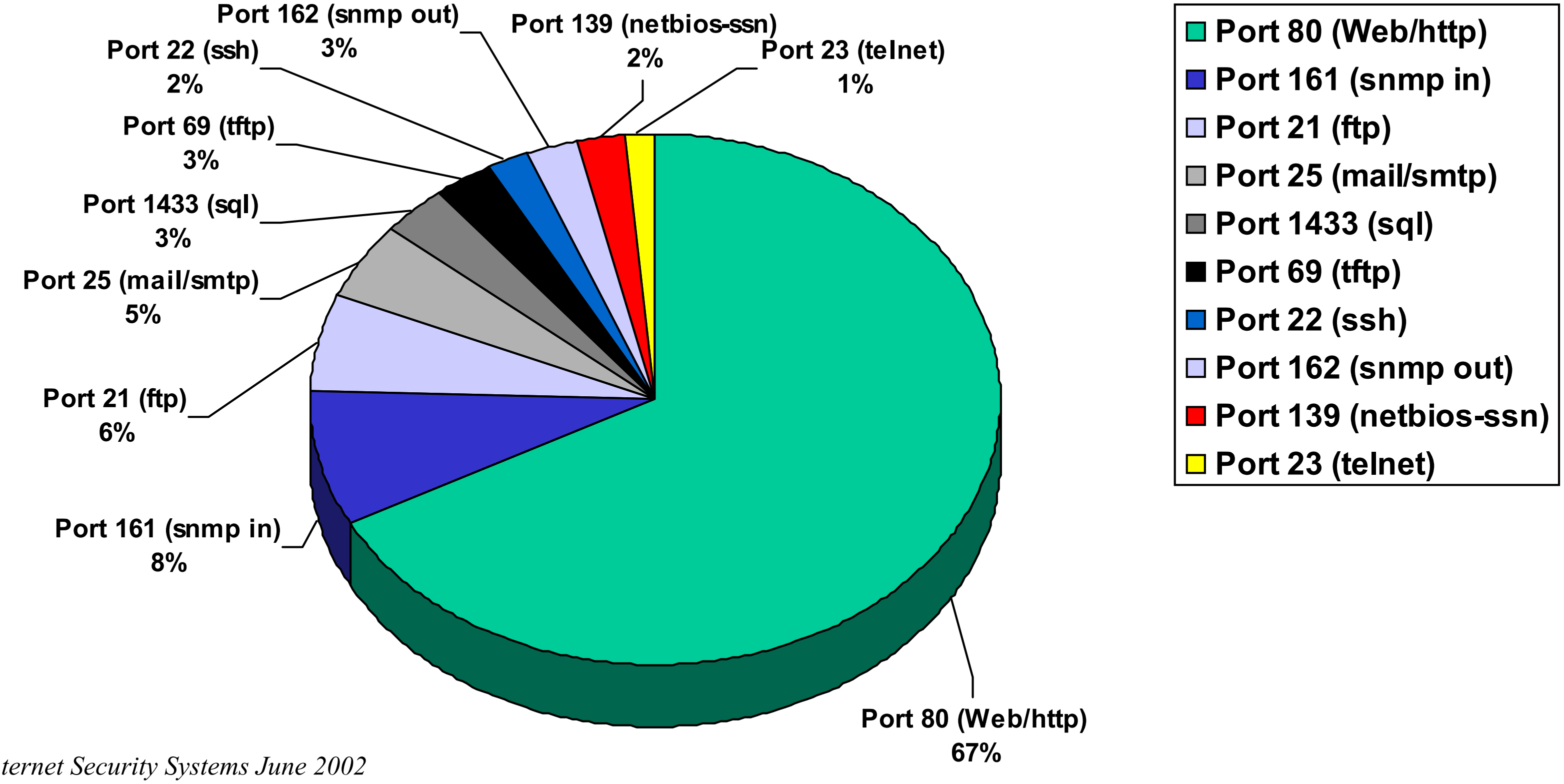
Riptech 3-4Q2001

Attack Trends: Attacks by Company Size



Riptech 3-4Q2001

Attack Trends: Top Destination Ports



Internet Security Systems June 2002

Regulatory Compliance

- Electronic Signatures in Global & National Commerce Act ("E-Sign")
- FDA 21 CFR Part 11
- Gramm-Leach-Bliley (GLB) Act of 1999
- Health Insurance Portability & Accountability Act (HIPAA) of 1996
- Uniform Computer Information Transactions Act (UCITA)
- USA Patriot Act of 2001
- U.S. Safe Harbor

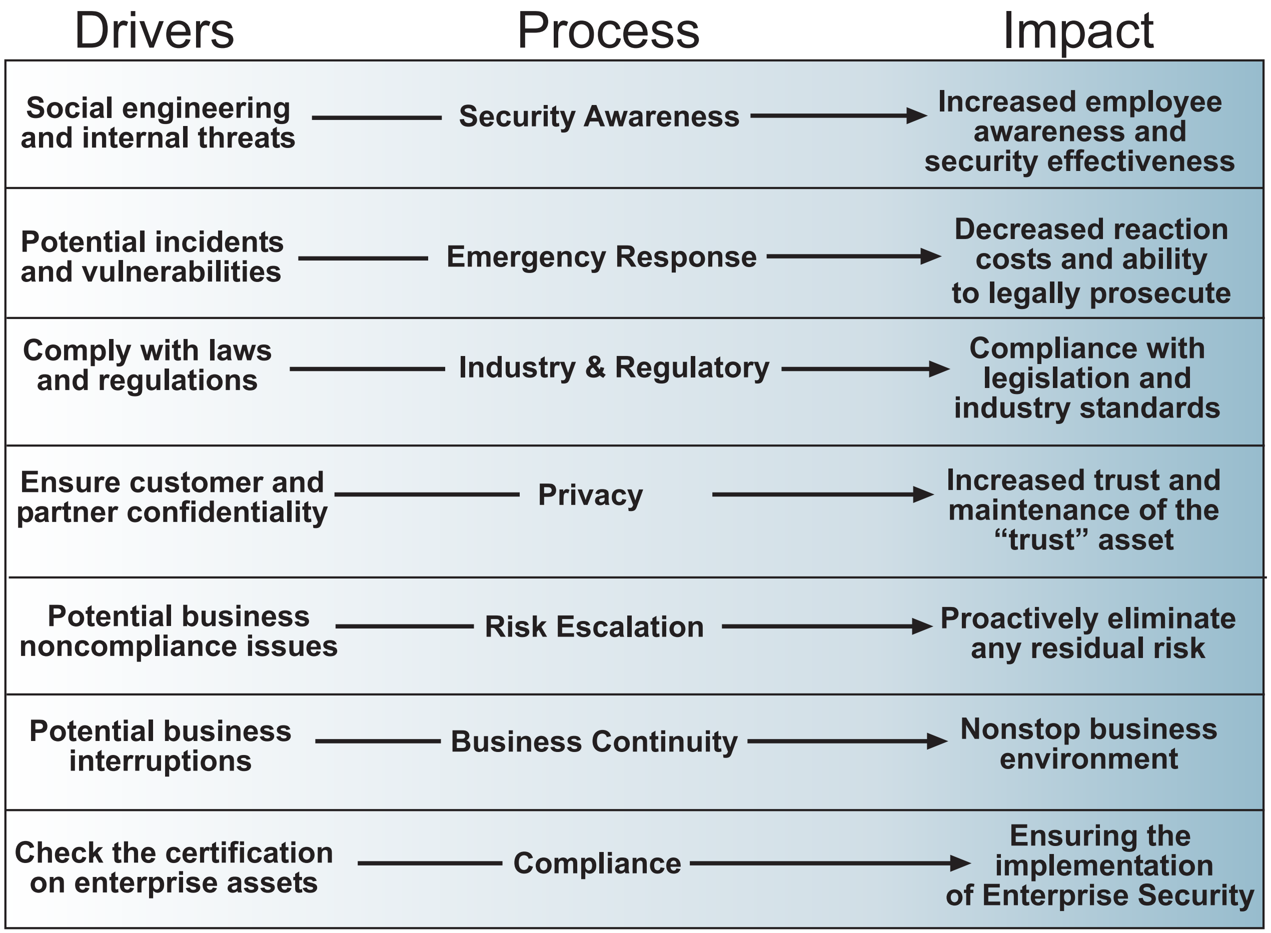
Consequences of Non-Compliance

- Significant fines
- Imprisonment
- Increased insurance premiums
- Additional legal costs
- Higher costs for reacting to compliance audits
- Direct and indirect business loss

2. TODAY'S SOLUTIONS FOR MITIGATING RISK

2.1 Today's Solutions for Mitigating Risk

Resolving Security Risks



Drivers	Process	Impact
Social engineering and internal threats	Security Awareness	Increased employee awareness and security effectiveness
Potential incidents and vulnerabilities	Emergency Response	Decreased reaction costs and ability to legally prosecute
Comply with laws and regulations	Industry & Regulatory	Compliance with legislation and industry standards
Ensure customer and partner confidentiality	Privacy	Increased trust and maintenance of the "trust" asset
Potential business noncompliance issues	Risk Escalation	Proactively eliminate any residual risk
Potential business interruptions	Business Continuity	Nonstop business environment
Check the certification on enterprise assets	Compliance	Ensuring the implementation of Enterprise Security

0002-00111620.19

2.2 Today's Solutions for Mitigating Risk

Vulnerability Alerts

- CERT: www.cert.org
- eSecurityOnline: www.eSecurityOnline.com
- SecurityFocus: www.SecurityFocus.com

Security Technology Enablers

- Network
  - Firewalls
  - Intrusion detection (IDS)
  - Internal/external VPN
  - Wireless encryption
- Server
  - Intrusion detection (IDS)
  - Secure shell
  - Trusted system configuration
  - Enterprise antivirus software
- Entitlement Management
  - Directory services (LDAP)
  - Single sign-on (SSO)
  - Biometrics
- Integration
  - Encrypted EDI
  - Public key infrastructure (PKI)
  - IPSec

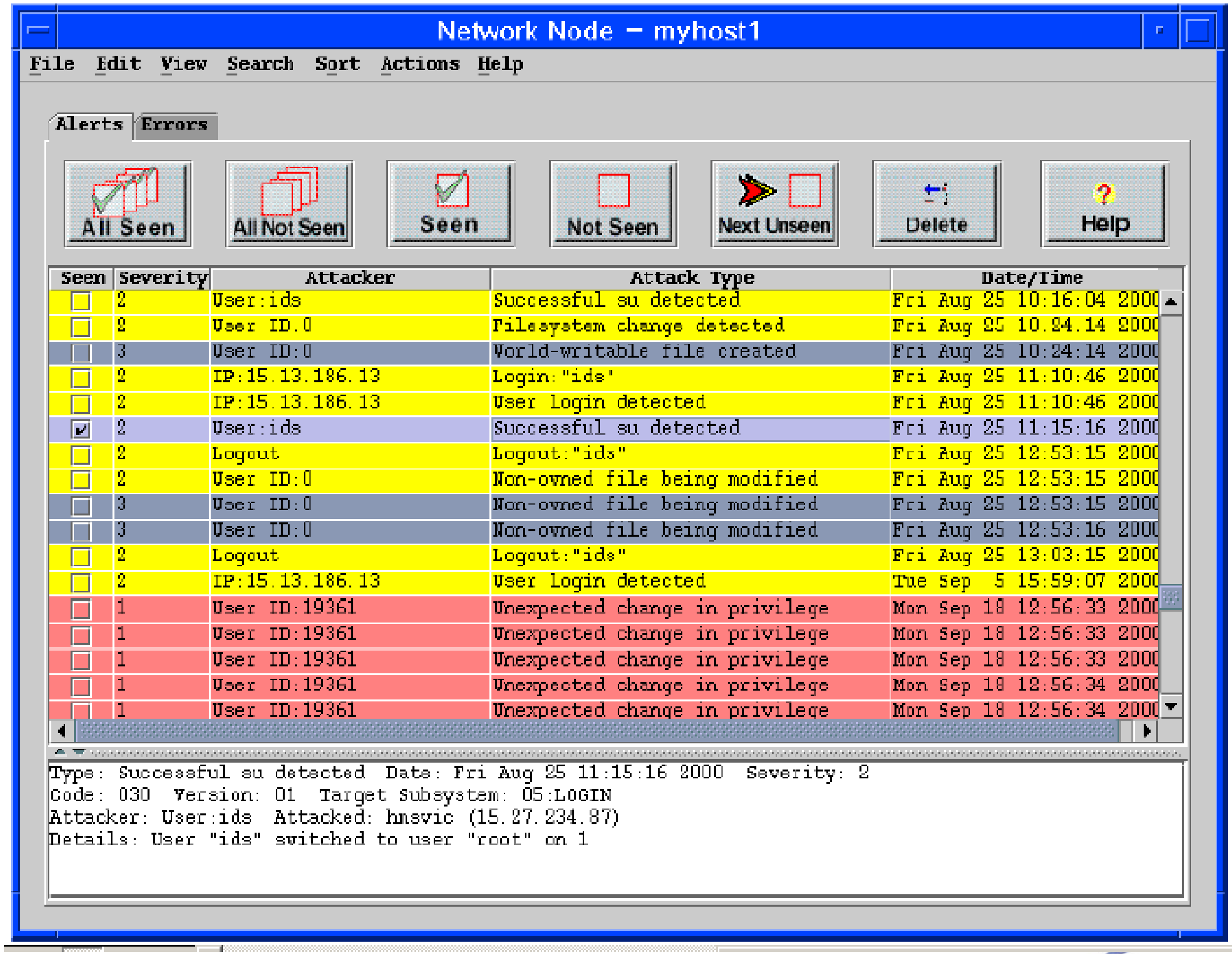
HP Security Solutions

- Atalla Network Security Processors
  For secure financial transactions (ATM, POS, EFT)
- HP-UX AAA
  authentication, authorization & accounting based on RADIUS protocol
- HP-UX Secure Shell
- HP-UX Trusted System
- HP Toptools Remote Security Management
- HP IDS/9000
  System-level intrusion detection
- Proliant-based VPN/Firewall
  Based on CheckPoint VPN-1 and Firewall-1 software
- HP-UX IPSec/9000
- HP-UX IP Filter
  Stateful firewall server

www.hp.com/security

2.5 Today’s Solutions for Mitigating Risk

HP IDS/9000 Example



Seen	Severity	Attacker	Attack Type	Date/Time
□	2	User:ids	Successful su detected	Fri Aug 25 10:16:04 2000
□	2	User ID.0	Filesystem change detected	Fri Aug 25 10.24.14 2000
□	3	User ID:0	World-writable file created	Fri Aug 25 10:24:14 2000
□	2	IP:15.13.186.13	Login:"ids'	Fri Aug 25 11:10:46 2000
□	2	IP:15.13.186.13	User login detected	Fri Aug 25 11:10:46 2000
☑	2	User:ids	Successful su detected	Fri Aug 25 11:15:16 2000
□	2	Logout	Logout:"ids"	Fri Aug 25 12:53:15 2000
□	2	User ID:0	Non-owned file being modified	Fri Aug 25 12:53:15 2000
□	3	User ID:0	Non-owned file being modified	Fri Aug 25 12:53:15 2000
□	3	User ID:0	Non-owned file being modified	Fri Aug 25 12:53:16 2000
□	2	Logout	Logout:"ids"	Fri Aug 25 13:03:15 2000
□	2	IP:15.13.186.13	User login detected	Tue Sep 5 15:59:07 2000
□	1	User ID:19361	Unexpected change in privilege	Mon Sep 18 12:56:33 2000
□	1	User ID:19361	Unexpected change in privilege	Mon Sep 18 12:56:33 2000
□	1	User ID:19361	Unexpected change in privilege	Mon Sep 18 12:56:33 2000
□	1	User ID:19361	Unexpected change in privilege	Mon Sep 18 12:56:34 2000
□	1	User ID:19361	Unexpected change in privilege	Mon Sep 18 12:56:34 2000

```
Type: Successful su detected  Date: Fri Aug 25 11:15:16 2000  Severity: 2
Code: 030  Version: 01  Target Subsystem: 05:LOGIN
Attacker: User:ids  Attacked: hnsvic (15.27.234.87)
Details: User "ids" switched to user "root" on 1
```

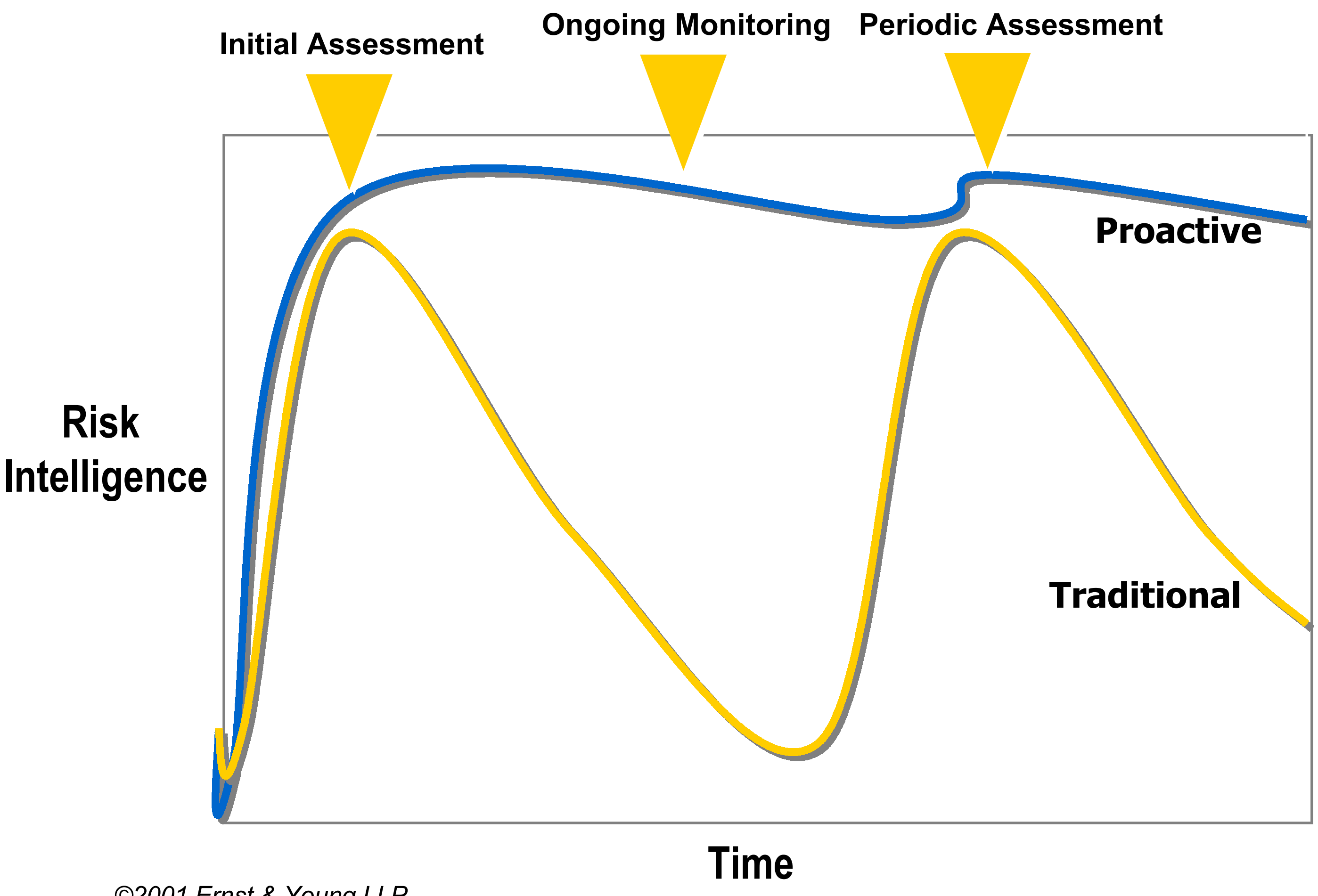
3. HOW OTHERS MANAGE THEIR SECURITY VULNERABILITIES

Characteristics of World-Class Vulnerability Management

1. Business and security objectives are aligned
2. Security programs are enterprise-wide
3. Vulnerability management is continuous
4. Response to vulnerabilities are proactive
5. Security programs are validated
6. Security frameworks are formalized

3.2 How Others Manage their Security Vulnerabilities

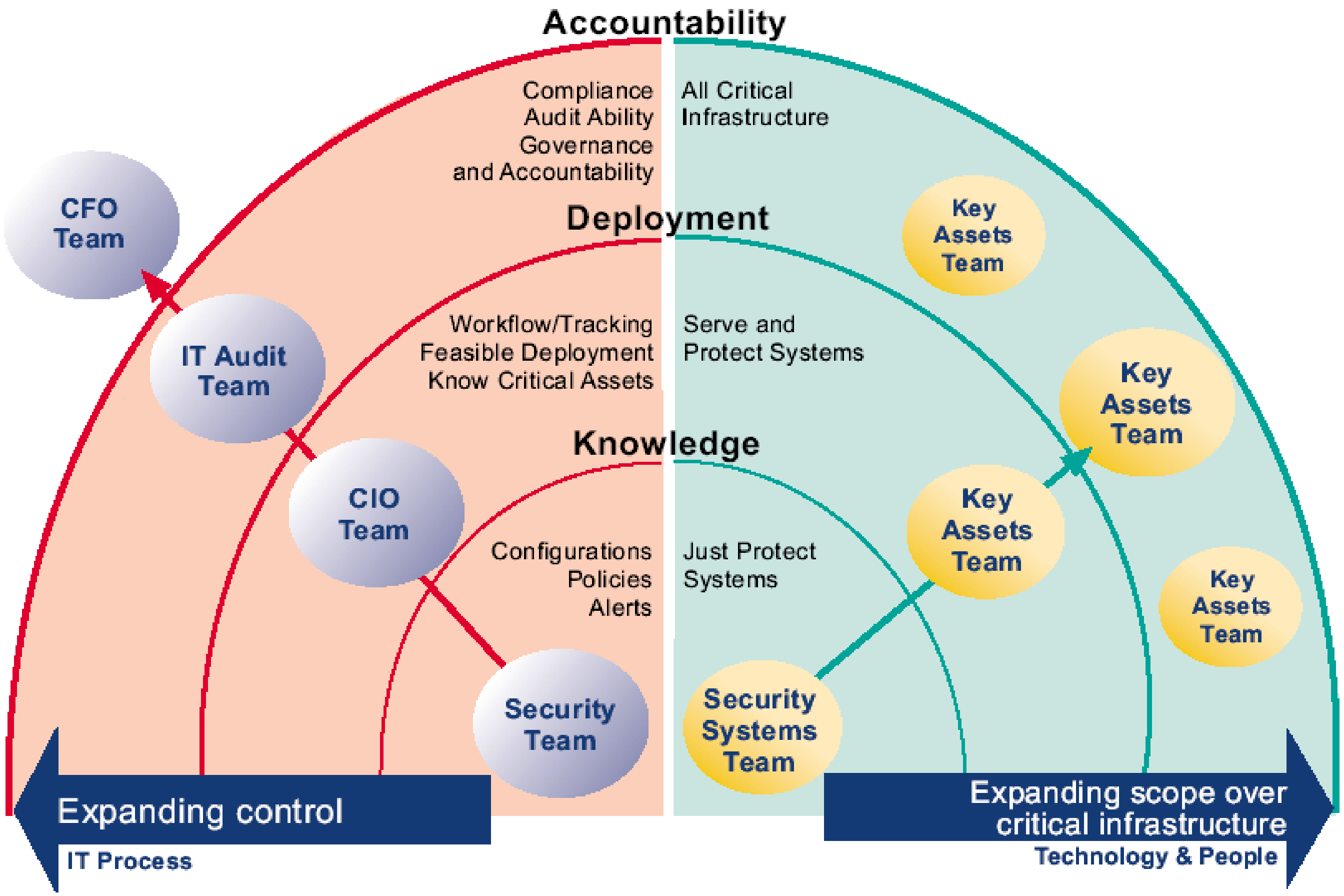
Security Readiness



©2001 Ernst & Young LLP

3.3 *How Others Manage their Security Vulnerabilities*

Vulnerability Management Model

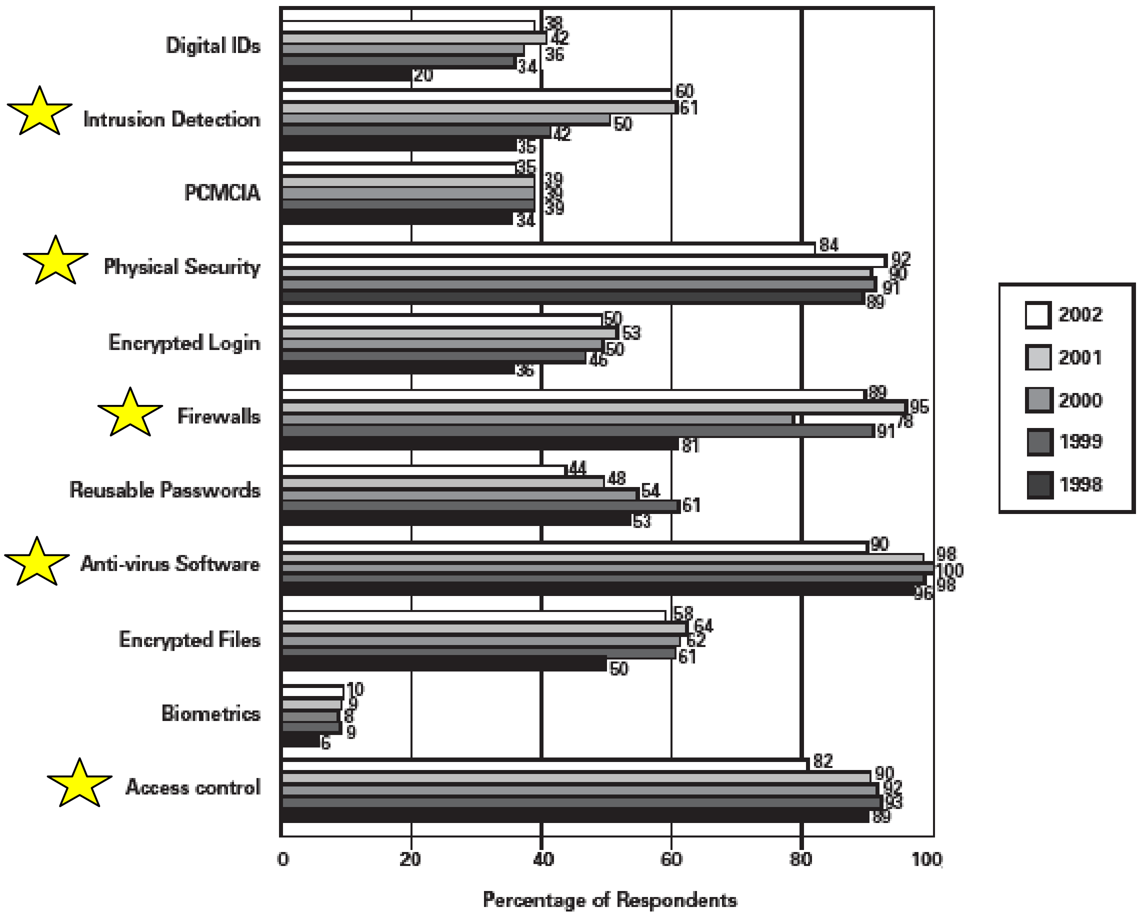


©2001 Ernst & Young LLP

3.4 How Others Manage their Security Vulnerabilities

Security Technologies Used

Security Technologies Used



4. MANAGING MY ORGANIZATION'S VULNERABILITY

4.1 Managing My Organization's Vulnerability

Vulnerability Scorecard

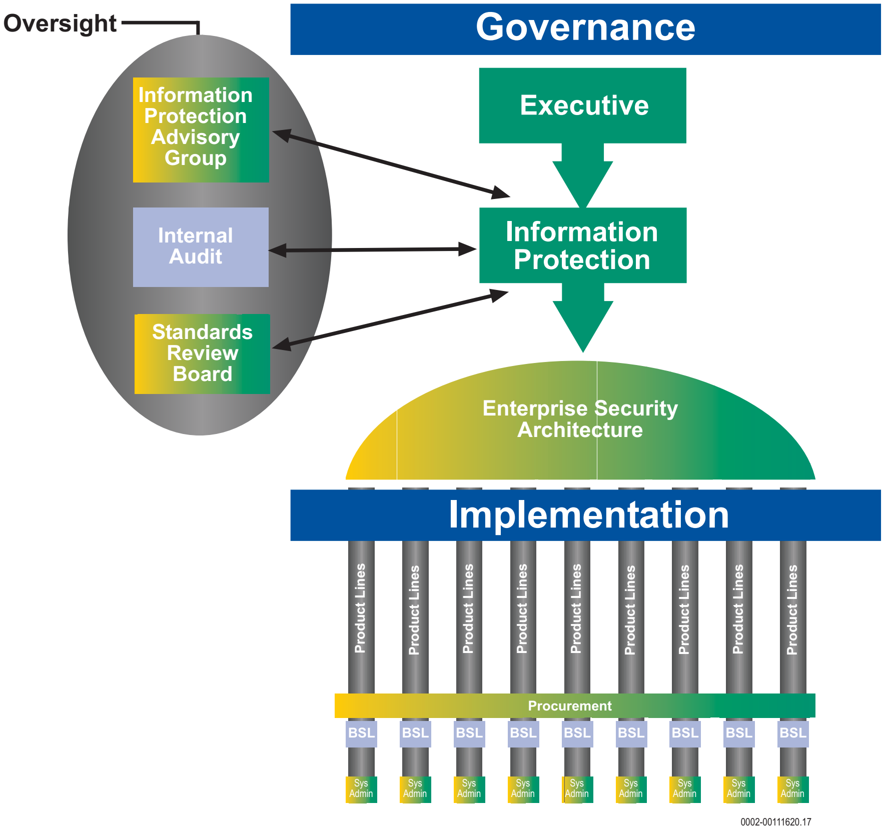
	YES	NO
1. *Do I know of all the IT assets I have?*	□	□
2. *Am I confident my critical IT assets are secure?*	□	□
3. *Am I monitoring my assets to detect virus attacks, external hacks, and internal intrusions?*	□	□
4. *Do I have updated policies and procedures addressing IT security?*	□	□
5. *Do I have current disaster and business continuity planning?*	□	□
6. *Do I know what my Business Partners are doing?*	□	□
7. *Does my Internal Audit group assess and validate my risk profile?*	□	□
8. *Am I fully compliant with government regulations?*	□	□

Approach to Vulnerability Management

1. Security Governance
2. IT Asset Management
3. Vulnerability Assessment
4. Vulnerability Management

4.3 Managing My Organization’s Vulnerability

Step 1: Security Governance



©2001 Ernst & Young LLP

Step 2: IT Asset Management

- Continuous process for managing IT assets
- Automated asset discovery software
- Detailed asset management database
- Change controls processes in place
- Integration with helpdesk services
- Self-service functions

Step 3: Vulnerability Assessment

- Implement a continuous assessment process
- Leverage detailed asset management database
- Business impact assessment to organization if vulnerability is realized
- Prioritization & alignment with organization goals and requirements

Step 4: Vulnerability Management

- Enterprise security strategy and standards
- Centralized management of monitoring and testing
- Proactive identification of vulnerabilities specific to your organization
  - Asset management database
  - eSecurityOnline-type customized notification
- Computer Emergency Response Program (CERP)
- Mitigation of risks through technology enablers
  - Firewalls
  - Enterprise antivirus software and mail filters
  - Enterprise entitlement management
  - Intrusion detection systems

SUMMARY

- Know your risks so as to make informed decisions
- Align with business goals and requirements
- Establish security governance
- Enterprise-wide consistent approach
- Implement proactive and continuous processes as well as security technologies to manage vulnerabilities

Matt Tolbert, CISSP

Ernst & Young, LLP   Security & Technology Solutions Group

(212) 773-5967   Matthew.Tolbert@ey.com