Directives and Legislation

• The National Strategy to Secure Cyberspace, Priority II: A National Cyberspace Security Threat and Vulnerability Reduction Program:

  “DOJ and other appropriate agencies will develop and implement efforts to reduce cyber attacks and cyber threats through . . . developing better data about victims of cybercrime and intrusions in order to understand the scope of the problem and to be able to track changes over time.” (A/R 2-1)

• Cyber Security Research and Development Act, P.L. 107-305
Partnerships

• DHS
  – National Cyber Security Division
  – U.S. Secret Service

• DOJ
  – Computer Crime and Intellectual Property
  – FBI Cyber Security Squad

• Other supporters

• Data collection agents
  – RAND Corporation
  – Market Strategies, Inc.

National Computer Security Survey

• Measure nature and prevalence of cybercrime
• Quantify losses
• Reveal vulnerabilities
• Identify best security practices
• Inform resource allocation
• Reduce cyber threats
NCSS Universe, Sample, and Response

NCSS Universe, Sample, and Response, by Company Size, 2005

<table>
<thead>
<tr>
<th>Number of employees</th>
<th>Number of businesses</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Universe</td>
<td>Sample</td>
</tr>
<tr>
<td>All businesses</td>
<td>7,278,109</td>
<td>35,596</td>
</tr>
<tr>
<td>2 to 24</td>
<td>6,771,026</td>
<td>11,479</td>
</tr>
<tr>
<td>25 to 99</td>
<td>396,355</td>
<td>5,601</td>
</tr>
<tr>
<td>100 to 999</td>
<td>98,585</td>
<td>11,472</td>
</tr>
<tr>
<td>1,000 or more</td>
<td>12,143</td>
<td>7,044</td>
</tr>
</tbody>
</table>

Highest and Lowest Response Rates

- Utilities
- Social Svcs
- Health Care
- Telecom
- Hotels
- Recording

Percent of companies
NCSS Data

• Represents more than 8,000 businesses
• Covers 36 economic sectors
• Is the most comprehensive data available on—
  – Nature of computer security incidents
  – Prevalence by industry and type of incident
  – Monetary losses
  – Downtime
  – Types of offenders
  – Reporting incidents to authorities
  – Vulnerabilities leading to breaches

The Nature of Cybercrime

• Cyber attacks
  – All or part of the computer system is the target
• Cyber theft
  – A computer was used to illegally obtain money, goods, or services
• Other computer security incidents
  – Spyware, adware, other malware
  – Phishing, spoofing
  – Hacking
  – Pinging, scanning, sniffing
  – Theft of other information
**Prevalence of Cybercrime**

**Prevalence of computer security incidents among businesses, by type of incident, 2005**

<table>
<thead>
<tr>
<th>Type of incident</th>
<th>All companies</th>
<th>Number</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>All incidents</td>
<td>7,636</td>
<td>5,081</td>
<td>67 %</td>
</tr>
<tr>
<td>Cyber attack</td>
<td>7,626</td>
<td>4,398</td>
<td>58 %</td>
</tr>
<tr>
<td>Computer virus</td>
<td>7,538</td>
<td>3,937</td>
<td>52 %</td>
</tr>
<tr>
<td>Denial of service</td>
<td>7,517</td>
<td>1,215</td>
<td>16 %</td>
</tr>
<tr>
<td>Vandalism</td>
<td>7,500</td>
<td>350</td>
<td>5 %</td>
</tr>
<tr>
<td>Cyber theft</td>
<td>7,561</td>
<td>839</td>
<td>11 %</td>
</tr>
<tr>
<td>Other</td>
<td>7,492</td>
<td>1,792</td>
<td>24 %</td>
</tr>
</tbody>
</table>

**Prevalence of Cybercrime**

Percent of companies

![Bar chart showing the prevalence of cybercrime among companies, with categories for All, Cyber attack, Cyber theft, and Other, indicating the percentage of companies affected by each type of incident.](chart_image)
Total Monetary Loss

Monetary Loss (in thousands of dollars)

- All
- Cyber attack
- Cyber theft
- Other

Total System Downtime

System downtime (in hours)

- All
- Cyber attack
- Cyber theft (not collected)
- Other
Unknown Cyber Offenders

Percent of companies

Suspected Cyber Offenders

Percent of companies
Networks Most Commonly Accessed

Percent of companies

- Internet
- Local Area Network
- Wide Area Network
- Business laptop

- All
- Cyber attack
- Cyber theft
- Other

Computer Virus Sources

Percent of companies

- 25 to 99 employees
- 100 to 999 employees
- 1,000 or more employees

- E-mail
- Internet
- Portable media
- Other
Most Common Computer Security—

<table>
<thead>
<tr>
<th>In House</th>
<th>Outsourced</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Disaster recovery plan</td>
<td>• Intrusion testing</td>
</tr>
<tr>
<td>• Corporate security policy</td>
<td>• Vulnerability/risk assessment</td>
</tr>
<tr>
<td>• Physical security</td>
<td>• Disaster recovery plan</td>
</tr>
<tr>
<td>• Personnel policy</td>
<td>• Periodic audits</td>
</tr>
<tr>
<td>• Business continuity plan</td>
<td>• Network watch center</td>
</tr>
</tbody>
</table>

In-House Versus Outsourced Security

<table>
<thead>
<tr>
<th>Percent of companies detecting an incident</th>
<th>Physical security</th>
<th>Equipment decommissioning</th>
<th>Personnel policy</th>
<th>Network watch center</th>
</tr>
</thead>
<tbody>
<tr>
<td>In-house</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Outsourced</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[Bar chart showing comparison between in-house and outsourced security for different areas: Physical security, Equipment decommissioning, Personnel policy, Network watch center]
Future Plans

- Scale down questionnaire
- Survey a sample of industries each year
- Explore mandatory reporting requirements

Contact

Ramona Rantala
Statistician
Bureau of Justice Statistics
Department of Justice

(202) 307-6170
Ramona.Rantala@usdoj.gov
For Your Reference

Risk Levels

- Critical infrastructure
  - Agriculture
  - Chemical and drug mfg
  - Computer system design
  - Finance
  - Health care
  - Internet service providers
  - Petroleum mining and manufacturing

- Publications and broadcasting
- Real estate
- Telecommunications
- Transportation and pipelines
- Utilities
Risk Levels (continued)

• High risk
  – Manufacturing, durable
  – Manufacturing, non-durable goods
  – Motion picture and sound recording
  – Retail
  – Scientific research and development
  – Wholesale

• Moderate risk
  – Accounting
  – Advertising
  – Architecture and engineering
  – Business and technical schools
  – Insurance
  – Legal services

Risk Levels (continued)

• Low risk
  – Accommodations
  – Administrative support
  – Arts & entertainment
  – Construction
  – Food services
  – Forestry, fishing, and hunting

• Management of companies
  – Mining
  – Rental services
  – Social services
  – Other services
  – Warehousing
Highest Prevalence of Cybercrime

• Telecommunications (82%)
• Computer system design (79%)
• Manufacturing, durable goods (75%)
• Chemical and drug manufacturing (73%)
• Manufacturing, non-durable goods (72%)
• Business and technical schools (72%)
• Publications and broadcasting (71%)

Highest Prevalence of Cyber Attacks

• Telecommunications (74%)
• Computer system design (72%)
• Manufacturing, durable goods (68%)
• Chemical and drug manufacturing (66%)
• Publications and broadcasting (65%)
• Business and technical schools (64%)
• Manufacturing, non-durable goods (61%)
Highest Prevalence of Cyber Theft

- Finance (33%)
- Internet service providers (21%)
- Telecommunications (17%)
- Computer system design (15%)
- Manufacturing, durable goods (15%)
- Publications and broadcasting (14%)
- Accommodations (14%)

Highest Prevalence of Other Incidents

- Telecommunications (32%)
- Manufacturing, durable goods (32%)
- Architecture and engineering (31%)
- Chemical and drug manufacturing (27%)
- Wholesale (27%)
- Legal services (27%)
Lowest Prevalence of Cybercrime

• Forestry, fishing, and hunting (44%)
• Agriculture (51%)
• Food services (54%)
• Accounting (55%)
• Petroleum mining and manufacturing (56%)

Lowest Prevalence of Cyber Attacks

• Agriculture (40%)
• Forestry, fishing, and hunting (40%)
• Accounting (47%)
• Food services (48%)
• Finance (49%)
Lowest Prevalence of Cyber Theft

- Forestry, fishing, and hunting (3%)
- Warehousing (4%)
- Social services (5%)
- Agriculture (6%)
- Advertising (6%)
- Legal services (6%)

Lowest Prevalence of Other Incidents

- Food services (15%)
- Forestry, fishing, and hunting (16%)
- Accommodations (16%)
- Warehousing (16%)
- Agriculture (17%)