CSI/FBI 2000
COMPUTER CRIME AND SECURITY SURVEY
Statement of intent

• This survey was conducted by the Computer Security Institute (CSI) in association with the San Francisco Computer Crime Squad of the Federal Bureau of Investigation (FBI). The purpose of this joint effort is threefold:

• To provide statistical data on the current state of both computer crime and computer security;

• To help law enforcement agencies and information security professionals deal with the threat more effectively;

• To further cooperation between law enforcement agencies and organizations by encouraging organizations to report computer crimes to appropriate authorities.
Methodology

- Questionnaires were distributed to 4,284 information security professionals, 643 responses were received for a response rate of 15%. In 1999, 521 responses were received for a response rate of 14%. In 1998, 520 responses were received (13% of 3,890). In 1997, 563 responses were returned (11.49% of 4,899). In 1996, 428 responses were received (8.6% of 4,971).
- The responses were anonymous
- Job titles of respondents ranged from corporate information security manager and data security officer to senior systems analyst
- Organizations surveyed included corporations, financial institutions, government agencies and universities
Respondents by industry sector

- Financial: 17%
- Manufacturing: 10%
- Telecomm: 4%
- Medical: 7%
- Telecomm: 4%
- Local Gov.: 2%
- Other: 12%
- Federal Gov.: 9%
- Education: 5%
- Retail: 4%
- Medical: 7%
- High-Tech: 17%
- Transportation: 2%
- State Gov.: 7%
- Utility: 4%

Source: Computer Security Institute
2000: 643 Respondents/100%
Respondents by number of employees

- 1 to 99: 12%
- 100 to 499: 11%
- 500 to 999: 9%
- 1000 to 5000: 26%
- 5001 to 9999: 12%
- 10,000 or more: 30%

Source: Computer Security Institute
2000: 640 Respondents/99%
Respondents by gross income

- Over $1 billion: 43%
- Under $10 million: 17%
- $501 million to $1 billion: 11%
- 11-99 million: 15%
- $100-500 million: 14%
- $501 million to $1 billion: 11%

Source: Computer Security Institute

2000: 422 Respondents/65%
Security technologies used

Source: Computer Security Institute

1998: 512 Respondents/98%
1999: 501 Respondents/96%
2000: 629 Respondents/97%
Unauthorized use of computer systems within the last 12 months?

Percentage of Respondents

<table>
<thead>
<tr>
<th>Year</th>
<th>YES (%)</th>
<th>NO (%)</th>
<th>DON'T KNOW (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1996</td>
<td>42</td>
<td>64</td>
<td>70</td>
</tr>
<tr>
<td>1997</td>
<td>37</td>
<td>33</td>
<td></td>
</tr>
<tr>
<td>1998</td>
<td>18</td>
<td>17</td>
<td>16</td>
</tr>
<tr>
<td>1999</td>
<td>21</td>
<td>19</td>
<td>21</td>
</tr>
<tr>
<td>2000</td>
<td>18</td>
<td>18</td>
<td>12</td>
</tr>
</tbody>
</table>

2000: 585 Respondents/91%
1999: 512 Respondents/98%
1998: 515 Respondents/99%
1997: 391 Respondents/69%
1996: 410 Respondents/96%

Source: Computer Security Institute
### How many incidents? How many from outside? How many from inside?

#### How many incidents?

<table>
<thead>
<tr>
<th></th>
<th>1 TO 5</th>
<th>6 to 10</th>
<th>11 to 30</th>
<th>31 to 60</th>
<th>Over 60</th>
<th>Don’t Know</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000:</td>
<td>33%</td>
<td>23%</td>
<td>5%</td>
<td>2%</td>
<td>6%</td>
<td>31%</td>
</tr>
<tr>
<td>1999:</td>
<td>34%</td>
<td>22%</td>
<td>7%</td>
<td>2%</td>
<td>5%</td>
<td>29%</td>
</tr>
<tr>
<td>1998:</td>
<td>61%</td>
<td>31%</td>
<td>6%</td>
<td>1%</td>
<td>2%</td>
<td>n/a</td>
</tr>
<tr>
<td>1997:</td>
<td>47.60%</td>
<td>22.50%</td>
<td>2.9% (*)</td>
<td>n/a</td>
<td>n/a</td>
<td>26.93%</td>
</tr>
<tr>
<td>1996:</td>
<td>45.8%</td>
<td>20.6%</td>
<td>12.2% (*)</td>
<td>n/a</td>
<td>n/a</td>
<td>21.2%</td>
</tr>
</tbody>
</table>


#### How many from the outside?

<table>
<thead>
<tr>
<th></th>
<th>1 TO 5</th>
<th>6 to 10</th>
<th>11 to 30</th>
<th>31 to 60</th>
<th>Over 60</th>
<th>Don’t Know</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000:</td>
<td>39%</td>
<td>11%</td>
<td>2%</td>
<td>2%</td>
<td>4%</td>
<td>42%</td>
</tr>
<tr>
<td>1999:</td>
<td>43%</td>
<td>8%</td>
<td>5%</td>
<td>1%</td>
<td>3%</td>
<td>39%</td>
</tr>
<tr>
<td>1998:</td>
<td>74%</td>
<td>18%</td>
<td>6%</td>
<td>0%</td>
<td>3%</td>
<td>xx%</td>
</tr>
<tr>
<td>1997:</td>
<td>43.10%</td>
<td>9.91%</td>
<td>1.21% (*)</td>
<td>n/a</td>
<td>n/a</td>
<td>45.28%</td>
</tr>
<tr>
<td>1996:</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a (**)</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
</tbody>
</table>


#### How many from the inside?

<table>
<thead>
<tr>
<th></th>
<th>1 TO 5</th>
<th>6 to 10</th>
<th>11 to 30</th>
<th>31 to 60</th>
<th>Over 60</th>
<th>Don’t Know</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000:</td>
<td>38%</td>
<td>16%</td>
<td>5%</td>
<td>1%</td>
<td>3%</td>
<td>37%</td>
</tr>
<tr>
<td>1999:</td>
<td>37%</td>
<td>16%</td>
<td>9%</td>
<td>1%</td>
<td>2%</td>
<td>35%</td>
</tr>
<tr>
<td>1998:</td>
<td>70%</td>
<td>20%</td>
<td>9%</td>
<td>1%</td>
<td>1%</td>
<td>n/a</td>
</tr>
<tr>
<td>1997:</td>
<td>47.20%</td>
<td>13.76%</td>
<td>3.21% (*)</td>
<td>n/a</td>
<td>n/a</td>
<td>35.32%</td>
</tr>
<tr>
<td>1996:</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a (**)</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
</tbody>
</table>


---

*Note: In ‘96 and ‘97, we asked only “11 or more.”

**Note: In ‘96, we didn’t ask this question.
Internet connection is increasingly cited as a frequent point of attack

Percentage of Respondents

<table>
<thead>
<tr>
<th>Year</th>
<th>INTERNAL SYSTEMS</th>
<th>REMOTE DIAL-IN</th>
<th>INTERNET</th>
</tr>
</thead>
<tbody>
<tr>
<td>1996</td>
<td>53.5%</td>
<td>44%</td>
<td>51%</td>
</tr>
<tr>
<td>1997</td>
<td>51.7%</td>
<td>38%</td>
<td>47%</td>
</tr>
<tr>
<td>1998</td>
<td>51.6%</td>
<td>34.9%</td>
<td>37.5%</td>
</tr>
<tr>
<td>1999</td>
<td>51.7%</td>
<td>28%</td>
<td>54%</td>
</tr>
<tr>
<td>2000</td>
<td>51.7%</td>
<td>22%</td>
<td>57%</td>
</tr>
</tbody>
</table>

2000: 443 Respondents/68%
1999: 324 Respondents/62%
1998: 279 Respondents/54%
1997: 391 Respondents/69%
1996: 174 Respondents/40%

Source: Computer Security Institute
Likely sources of attack

Percentage of Respondents

- **Foreign gov.**
  - 1997: 22%
  - 1998: 21%
  - 1999: 22%
  - 2000: 21%

- **Foreign corp.**
  - 1997: 22%
  - 1998: 23%
  - 1999: 29%
  - 2000: 30%

- **Independent hackers**
  - 1997: 73%
  - 1998: 72%
  - 1999: 74%
  - 2000: 77%

- **U.S. competitors**
  - 1997: 51%
  - 1998: 48%
  - 1999: 53%
  - 2000: 44%

- **Disgruntled employees**
  - 1997: 87%
  - 1998: 89%
  - 1999: 86%
  - 2000: 81%

Source: Computer Security Institute


2000: 583 Respondents/90%
1999: 460 Respondents/88%
1998: 428 Respondents/83%
1997: 503 Respondents/89%
Types of attack or misuse detected within the last 12 months

- Denial of Service
- Laptop
- Active wiretap
- Telecom fraud
- Unauthorized access by insiders
- Virus
- Financial fraud
- Insider abuse of Net access
- System penetration
- Telecom eavesdropping
- Sabotage
- Theft of proprietary info

Source: Computer Security Institute

2000: 581 Respondents/90%
1999: 405 Respondents/78%
1998: 458 Respondents/89%
1997: 492 Respondents/87%
Types of attack or misuse detected in the last 12 months (by percent)


Source: Computer Security Institute

2000: 581 Respondents/90%
1999: 405 Respondents/78%
1998: 458 Respondents/89%
1997: 492 Respondents/87%
Financial losses by type of attack or misuse

Number of Respondents

- 2000: 477 Respondents/74%
- 1999: 265 Respondents/51%
- 1998: 376 Respondents/73%
- 1997: 422 Respondents/75%

Source: Computer Security Institute
Financial losses by type of attack or misuse

Percentage of Respondents


Source: Computer Security Institute

2000: 477 Respondents/74%
1999: 265 Respondents/51%
1998: 376 Respondents/73%
1997: 422 Respondents/75%
Dollar amount of losses by type

<table>
<thead>
<tr>
<th>Type</th>
<th>Loss Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauth. insider access</td>
<td>$22,554,500</td>
</tr>
<tr>
<td>Theft of proprietary info</td>
<td>$55,996,000</td>
</tr>
<tr>
<td>Telecom fraud</td>
<td>$4,028,000</td>
</tr>
<tr>
<td>Financial fraud</td>
<td>$29,171,700</td>
</tr>
<tr>
<td>Virus</td>
<td>$10,404,300</td>
</tr>
<tr>
<td>Laptop theft</td>
<td>$27,984,740</td>
</tr>
<tr>
<td>Insider net abuse</td>
<td>$27,148,000</td>
</tr>
<tr>
<td>Denial of service</td>
<td>$8,247,500</td>
</tr>
<tr>
<td>Sabotage</td>
<td>$27,148,000</td>
</tr>
<tr>
<td>System penetration</td>
<td>$7,104,000</td>
</tr>
<tr>
<td>Telecom eavesdropping</td>
<td>$991,200</td>
</tr>
<tr>
<td>Active wiretapping</td>
<td>$5,000,000</td>
</tr>
</tbody>
</table>

Source: Computer Security Institute


2000: 273 Respondents/42%
Financial losses aggregated
Financial losses summary

Cited financial losses due to security breaches:

Willing and/or able to quantify their losses:

Total dollar losses:
  1997: 249 respondents, US$100,119,555
  1998: 241 respondents, US$136,822,000
  1999: 163 respondents, US$123,779,000
  2000: 273 respondents, US$265,589,940
Has your WWW site suffered unauthorized access or misuse within the last 12 months?

Percentage of Respondents

Yes  No  Don't Know

20  47  33
19  49  32

95% of respondents have WWW sites, 43% provide electronic commerce services via their WWW sites, only 30% were doing e-commerce in 1999.

2000: 603 Respondents/93%
1999: 479 Respondents/92%

Source: Computer Security Institute
WWW site incidents:
If yes, how many incidents?

Percentage of Respondents

<table>
<thead>
<tr>
<th></th>
<th>1999</th>
<th>2000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Just 1</td>
<td>30</td>
<td>36</td>
</tr>
<tr>
<td>2 to 5</td>
<td>38</td>
<td>35</td>
</tr>
<tr>
<td>5 to 9</td>
<td>3</td>
<td>10</td>
</tr>
<tr>
<td>10 or more</td>
<td>26</td>
<td>19</td>
</tr>
</tbody>
</table>

Source: Computer Security Institute

2000: 120 Respondents/18%
1999: 92 Respondents/18%
WWW site incidents:
Did the attacks come from inside or outside?

Percentage of Respondents

<table>
<thead>
<tr>
<th>Inside</th>
<th>Outside</th>
<th>Both</th>
<th>Don't Know</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>38</td>
<td>41</td>
<td>14</td>
</tr>
<tr>
<td>5</td>
<td>49</td>
<td>24</td>
<td>21</td>
</tr>
</tbody>
</table>

2000: 153 Respondents/23%
1999: 125 Respondents/24%

Source: Computer Security Institute
WWW site incidents:
What type of unauthorized access or misuse?

Percentage of Respondents

- Vandalism: 98 (1999) vs. 64 (2000)
- Denial of Service: 93 (1999) vs. 60 (2000)

Source: Computer Security Institute

2000: 93 Respondents/14%
1999: 44 Respondents/8%
If your organization has experienced computer intrusion(s) within the last 12 months, which of the following actions did you take?

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Patched holes</td>
<td>50</td>
<td>44</td>
<td>50</td>
<td>48</td>
<td>96</td>
</tr>
<tr>
<td>Did not report</td>
<td>85</td>
<td>48</td>
<td>44</td>
<td>32</td>
<td>23</td>
</tr>
<tr>
<td>Reported to law enforcement</td>
<td>96</td>
<td>26</td>
<td>26</td>
<td>16</td>
<td>26</td>
</tr>
<tr>
<td>Reported to legal counsel</td>
<td>85</td>
<td>29</td>
<td>29</td>
<td>25</td>
<td>48</td>
</tr>
</tbody>
</table>

Source: Computer Security Institute

2000: 407 Respondents/63%
1999: 295 Respondents/57%
1998: 321 Respondents/72%
1997: 317 Respondents/56%
1996: 325 Respondents/76%
The reasons organizations did not report intrusions to law enforcement

Percentage of Respondents

- **Negative publicity:**
  - 1996: 84%
  - 1997: 83%
  - 1998: 74%
  - 1999: 79%
  - 2000: 85.1%

- **Competitors would use to advantage:**
  - 1996: 52%
  - 1997: 54.8%
  - 1998: 60%
  - 1999: 74%
  - 2000: 74.9%

- **Unaware that could report:**
  - 1996: 39%
  - 1997: 36%
  - 1998: 46%
  - 1999: 53.2%
  - 2000: 52.8%

- **Civil remedy seemed best:**
  - 1996: 13%
  - 1997: 13%
  - 1998: 13%
  - 1999: 13%
  - 2000: 13%

---

Source: Computer Security Institute

- **2000:** 209 Respondents/32%
- **1999:** 107 Respondents/20%
- **1998:** 96 Respondents/19%
- **1997:** 142 Respondents/25%
- **1996:** 64 Respondents/15%
Would your organization consider hiring reformed hackers as consultants?

Percentage of Respondents

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
<th>Don't know</th>
</tr>
</thead>
<tbody>
<tr>
<td>17</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>65</td>
<td>61</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>19</td>
<td></td>
</tr>
</tbody>
</table>

Source: Computer Security Institute
For further information, contact:

- Chris Beeson, Special Agent
  S.F. Regional FBI Computer Crime Squad
  22320 Foothill Blvd., Hayward, CA 94541
  Ph: 510-886-7447      Fax: 510-886-4981
  E-mail: nccs-sf@fbi.gov

- Richard Power, Editorial Director
  Computer Security Institute
  600 Harrison Street, San Francisco, CA 94107
  Ph: 415-905-2370      Fax: 415-905-2218
  E-mail: rpower@cmp.com