2001 COMPUTER SECURITY SURVEY

I. COMPUTER SECURITY CONCERNS

1. What are the top three computer security concerns for this company? Mark (X) three.

   Embezzlement  [101]
   Fraud  [02]
   Theft of proprietary information  [03]
   Denial of service (to Internet connection or e-mail service)  [04]
   Vandalism or sabotage (electronic)  [06]
   Computer virus  [06]
   Other intrusion or breach of computer systems  [07]
   Misuse of computers by employees (Internet, e-mail, etc.)  [08]
   Unlicensed use or copying (piracy) of digital products – software, music, motion pictures, etc. – developed for resale  [09]
   Other – Specify  [10]

RETURN COMPLETED FORM TO:

U.S. CENSUS BUREAU
1201 East 10th Street
Jeffersonville, IN 47132-0001

OR

FAX TO:
1–888–300–5192

FOR ASSISTANCE, CALL
1–800–227–1735
MONDAY THROUGH FRIDAY
8:00 A.M. TO 5:00 P.M. EDT
OR
E-MAIL: css@census.gov

NOTICE OF CONFIDENTIALITY – Your report to the Census Bureau is confidential by law (Title 13, Section 9 of the U.S. Code). It may be seen only by persons sworn to uphold the confidentiality of Census Bureau information and used only for statistical purposes from which no firm may be identified. The law also prohibits the sharing of your data with other agencies, exempts the information you provide from requests made under the Freedom of Information Act, and ensures that your responses are immune from legal process, including copies retained in your files.

SURVEY SCOPE – This survey collects data on the type and frequency of computer security incidents in which a computer was used as the means of committing a crime against the company.

REPORTING ENTITY – Report consolidated figures for DOMESTIC OPERATIONS of this company, including all DIVISIONS, SUBSIDIARIES and LOCATIONS. If this company changed its operational status prior to or during the reporting period, see instructions.

REPORTING PERIOD – The reporting period for this survey is calendar year 2001. If 2001 calendar year figures are not available, please use fiscal year 2001 data.

ESTIMATES are acceptable.
II. COMPUTER INFRASTRUCTURE AND SECURITY

2a. In 2001, what types of computer networks did this company use? For this survey, "company" means DOMESTIC OPERATIONS, including all DIVISIONS, SUBSIDIARIES and LOCATIONS. Mark (X) all that apply.

01 Local area network (LAN)
02 Wide area network (WAN)
03 Process control network (PCN)
04 Virtual private network (VPN)
05 Electronic Data Interchange (EDI)
06 Wireless network (e.g., 802.11)
07 Internet
08 Intranet
09 Extranet
10 Stand-alone PCs (not on LAN)
11 Company has no computers – (Skip to 20, page 8.)
12 Don’t know

b. In 2001, how many servers did this company have?

202 Number

c. In 2001, how many individual PCs and workstations did this company have?

203 Number

d. In 2001, which of the following types of access to its networks did this company support? Mark (X) all that apply.

01 Remote dial-in access
02 Access to networks through Internet
03 Wireless access to e-mail
04 Wireless access to Internet
05 Wireless access to this company’s other networks
06 Publicly accessible website WITHOUT e-commerce capabilities
07 Publicly accessible website WITH e-commerce capabilities
08 Other – Specify
09 None of the above
10 Don’t know

3a. In 2001, what types of computer system security technology did this company use? Mark (X) all that apply.

01 Anti-virus software
02 Biometrics
03 Digital certificates
04 E-mail logs/filters
05 System administrative logs
06 Encryption
07 Firewall
08 Intrusion detection system
09 One-time password generators (smartcards, tokens, keys)
10 Passwords (changed every 30 or 60 days, etc.)
11 Other – Specify
12 None; no computer security
13 Don’t know

3b. In 2001, how much did this company spend on the types of computer system security technology identified in 3a? EXCLUDE personnel costs. $ 

ESTIMATES are acceptable.

4a. In 2001, what types of computer security practices did this company have? Mark (X) all that apply.

01 Business continuity program for computer systems
02 Disaster recovery program for computer systems
03 Corporate policy on computer security
04 Regular review of system administrative logs
05 Periodic computer security audits
06 Formal computer security audit standards
07 Training employees in computer security practices
08 Other – Specify
09 None of the above
10 Don’t know

b. If this company had a computer system business continuity or disaster recovery program, was it tested, used in an emergency situation and/or updated in 2001? Mark (X) all that apply.

01 Tested
02 Used in emergency situation
03 Updated
04 None of the above
05 Don’t know
06 Not applicable

c. What percentage of this company’s total 2001 Information Technology budget did this company spend on the types of computer system security technology identified in 3a? Round to nearest whole percent.

207 %

ESTIMATES are acceptable.

FORM CS-1A (7-31-2002)
III. TYPES OF COMPUTER SECURITY INCIDENTS

The questions in this section pertain to computer security incidents against this company, where the word "incident" refers to any unauthorized access, intrusion, breach, compromise or use of this company’s computer systems.

Computer security incidents may be committed by people either inside or outside the company and include embezzlement, fraud, theft of proprietary information, denial of service, vandalism, sabotage, computer virus, etc.

EXCLUDE incidents of unlicensed use or copying (piracy) of digital products – software, music, motion pictures, etc. – developed by this company for resale. These should be reported in Question 18, page 8.

Please do NOT duplicate information. If an incident can be classified under multiple categories, report it under the FIRST applicable category. For example, if proprietary information was stolen or copied by means of computer fraud, report it under fraud and do NOT include it under theft of proprietary information.

ESTIMATES are acceptable.

5. EMBEZZLEMENT

Embezzlement is the unlawful misappropriation of money or other things of value, BY THE PERSON TO WHOM IT WAS ENTRUSTED (typically an employee), for his/her own use or purpose.

INCLUDE instances in which a computer was used to wrongfully transfer, counterfeit, forge or gain access to money, property, financial documents, insurance policies, deeds, use of rental cars, various services, etc., by the person to whom it was entrusted.

a. Did this company detect any incidents in which a computer was used to commit embezzlement against this company in 2001?

☐ Yes → How many incidents were detected? ______ Number
☐ No – (If “No,” skip to 6.)

b. How many of these incidents were reported to law enforcement, FedCIRC, ISAC or CERT? INCLUDE incidents reported to local, State or Federal law enforcement, the Federal Computer Incident Response Center, the Information Sharing and Analysis Center or the CERT® Coordination Center.

c. For the incidents in 5a, were any of the suspected offenders employed by this company at the time of the incident?

☐ Yes → In how many incidents? ______ Number
☐ No
☐ Don’t know

d. What was the dollar value of money or other things taken by embezzlement in 2001? ESTIMATES are acceptable.

$ ______

500 ______ 504 ______

6. FRAUD

Fraud is the intentional misrepresentation of information or identity to deceive others, the unlawful use of credit/debit card or ATM, or the use of electronic means to transmit deceptive information, in order to obtain money or other things of value. Fraud may be committed by someone inside or outside the company.

INCLUDE instances in which a computer was used by someone inside or outside the company in order to defraud this company of money, property, financial documents, insurance policies, deeds, use of rental cars, various services, etc., by means of forgery, misrepresented identity, credit card or wire fraud, etc. EXCLUDE incidents of embezzlement. Report these in 5.

a. Did this company detect any incidents in which someone inside or outside this company used a computer to commit fraud against this company in 2001?

☐ Yes → How many incidents were detected? ______ Number
☐ No – (If “No,” skip to 7, page 4.)

b. How many of these incidents were reported to law enforcement, FedCIRC, ISAC or CERT? INCLUDE incidents reported to local, State or Federal law enforcement, the Federal Computer Incident Response Center, the Information Sharing and Analysis Center or the CERT® Coordination Center.

c. For the incidents in 6a, were any of the suspected offenders employed by this company at the time of the incident?

☐ Yes → In how many incidents? ______ Number
☐ No
☐ Don’t know

d. What was the dollar value of money or other things taken by fraud in 2001? ESTIMATES are acceptable.

$ ______

500 ______ 506 ______
III. TYPES OF COMPUTER SECURITY INCIDENTS – Continued

6. FRAUD – Continued

e. What other monetary losses and costs were incurred in 2001 due to these incidents? ESTIMATES are acceptable. INCLUDE the cost of diagnosis, repair and replacement such as labor, hardware, software, etc. If possible, include the estimated value of downtime, lost productivity, income from lost sales, labor or fees for legal or investigative work, etc. EXCLUDE costs associated solely with the prevention of future incidents.

<table>
<thead>
<tr>
<th>Mil.</th>
<th>Thou.</th>
<th>Dol.</th>
</tr>
</thead>
<tbody>
<tr>
<td>$</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

7. THEFT OF PROPRIETARY INFORMATION

Theft of proprietary information is the illegal obtaining of designs, plans, blueprints, codes, computer programs, formulas, recipes, trade secrets, graphics, copyrighted material, data, forms, files, lists, personal or financial information, etc., usually by electronic copying.

EXCLUDE incidents which resulted in embezzlement or fraud. Report these in 5 or 6, page 3.

EXCLUDE incidents of unlicensed use or copying (piracy) of digital products – software, music, motion pictures, etc. – developed by this company for resale. Report these in 18, page 8.

For the incidents in 7a, were any of the suspected offenders employed by this company at the time of the incident?

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

8. DENIAL OF SERVICE

Denial of service is the disruption or degradation of an Internet connection or e-mail service that results in an interruption of the normal flow of information. Denial of service is usually caused by ping attacks, port scanning probes, excessive amounts of incoming data, etc.

EXCLUDE incidents in which a virus, worm or Trojan horse was the cause of the denial of service.

a. Did this company detect any incidents of denial of service (a noticeable interruption of its Internet connection or e-mail service) in 2001?

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

How many of these incidents were reported to local, State or Federal law enforcement, the Federal Computer Incident Response Center, the Information Sharing and Analysis Center or the CERT® Coordination Center.

b. In 2001, how many of these incidents of denial of service were caused by a virus, worm or Trojan horse?

<table>
<thead>
<tr>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

c. How many of these incidents in 8a were reported to law enforcement, FedCIRC, ISAC or CERT? INCLUDE incidents reported to local, State or Federal law enforcement, the Federal Computer Incident Response Center, the Information Sharing and Analysis Center or the CERT® Coordination Center.

<table>
<thead>
<tr>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

d. For the incidents in 8a, were any of the suspected offenders employed by this company at the time of the incident?

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

e. What was the total duration (in hours) of the incidents of denial of service indicated in 8a?

INCLUDE downtime needed for repairs.

<table>
<thead>
<tr>
<th>Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

f. How many of these incidents of denial of service resulted in the company taking some action to restore the level of service?

<table>
<thead>
<tr>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

g. How much was spent in 2001 to recover from these incidents of denial of service? ESTIMATES are acceptable. INCLUDE the cost – both internal and external – of diagnosis, repair and replacement such as labor, hardware, software, etc. EXCLUDE costs associated solely with the prevention of future incidents.

<table>
<thead>
<tr>
<th>Mil.</th>
<th>Thou.</th>
<th>Dol.</th>
</tr>
</thead>
<tbody>
<tr>
<td>$</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

h. What other monetary losses and costs were incurred in 2001 due to these incidents? ESTIMATES are acceptable. INCLUDE the estimated value of downtime, lost productivity, income from lost sales, labor or fees for legal or investigative work, etc.

<table>
<thead>
<tr>
<th>Mil.</th>
<th>Thou.</th>
<th>Dol.</th>
</tr>
</thead>
<tbody>
<tr>
<td>$</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

i. How many of the incidents in 8a resulted in recovery costs or other monetary losses and costs reported above?

<table>
<thead>
<tr>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>
III. TYPES OF COMPUTER SECURITY INCIDENTS – Continued

9. VANDALISM OR SABOTAGE (ELECTRONIC)
Vandalism or sabotage (electronic) is the deliberate or malicious damage, defacement, destruction or other alteration of electronic files, data, web pages, programs, etc.

INCLUDE incidents of destructive viruses, worms, Trojan horses, etc.

EXCLUDE incidents of alteration which resulted in fraud. Report these in 3, page 3.

a. Did this company detect any incidents in which files, data, web pages or any part of its computer systems were electronically vandalized or sabotaged in 2001?

Yes → How many incidents were detected?
No → (If "No," skip to 10.)

b. How many of these incidents of vandalism or sabotage were caused by a destructive virus, worm or Trojan horse?

c. How many of these incidents in 9a were reported to law enforcement, FedCIRC, ISAC or CERT? INCLUDE incidents reported to local, State or Federal law enforcement, the Federal Computer Incident Response Center, the Information Sharing and Analysis Center or the CERT® Coordination Center.

da. For the incidents in 9a, were any of the suspected offenders employed by this company at the time of the incident?
EXCLUDE incidents in which an employee inadvertently executed a virus.

Yes → In how many incidents?
No
Don’t know

e. How many of these incidents of vandalism or sabotage in 9a resulted in the downtime of this company’s servers, routers, switches, individual PCs/workstations or websites? INCLUDE downtime needed for repairs.

f. What was the total downtime (in hours) of each of the following due to these acts of vandalism or sabotage?
INCLUDE downtime needed for repairs.

1) Downtime of company websites/web servers
2) Downtime of servers, routers or switches
3) Downtime of individual PCs/workstations

EXCLUDE network-wide downtime reported above.

EXCLUDE costs associated solely with the prevention of future incidents.

9. VANDALISM OR SABOTAGE (ELECTRONIC) – Continued

h. What other monetary losses and costs were incurred in 2001 due to these incidents? ESTIMATES are acceptable.
INCLUDE the estimated value of

EXCLUDE costs associated solely with the prevention of future incidents.

i. How many of the incidents in 9a resulted in recovery costs or other monetary losses and costs reported above?

10. COMPUTER VIRUS
A computer virus is a hidden fragment of computer code which propagates by inserting itself into or modifying other programs.

INCLUDE viruses, worms, Trojan horses, etc.

EXCLUDE incidents in which viruses caused excessive amounts of incoming data, resulting in denial of service. Report these in 8, page 4.

EXCLUDE incidents of destructive viruses, worms, Trojan horses, etc. Report these in 9.

a. Did this company detect any viruses which infected any part of its computer systems in 2001?

EXCLUDE viruses already reported in this survey.

Yes – How many incidents were detected?
No – (If "No," skip to 10.)

b. What was the total number of machines (servers, routers, switches, individual PCs/workstations, etc.) infected by these computer viruses?

c. How many of these incidents were reported to law enforcement, FedCIRC, ISAC or CERT? INCLUDE incidents reported to local, State or Federal law enforcement, the Federal Computer Incident Response Center, the Information Sharing and Analysis Center or the CERT® Coordination Center.

d. For the incidents in 10b, were any of the suspected offenders employed by this company at the time of the incident?
EXCLUDE incidents in which an employee inadvertently executed a virus.

Yes → In how many incidents?
No
Don’t know

EXCLUDE incidents in which an employee inadvertently executed a virus.
10. COMPUTER VIRUS – Continued

e. What was the total downtime (in hours) for each of the following due to these virus infections?
   INCLUDE downtime needed for repairs.

   1) Downtime of servers, routers or switches
   2) Downtime of individual PCs/workstations
   EXCLUDE network-wide downtime reported above.

   f. What was the total number of person-hours spent by technical support staff to recover from these computer viruses?

   g. How much was spent in 2001 to recover from these computer viruses? ESTIMATES are acceptable.
   INCLUDE the cost – both internal and external – of diagnosis, repair and replacement such as labor, hardware, software, etc.
   EXCLUDE costs associated solely with the prevention of future incidents.

   h. What other monetary losses and costs were incurred in 2001 due to these incidents? ESTIMATES are acceptable.
   INCLUDE actual losses such as the value of lost information.
   INCLUDE the estimated value of downtime, lost productivity, income from lost sales, labor or fees for legal or investigative work, etc.

   i. How many of the incidents in 10b resulted in recovery costs or other monetary losses and costs reported above?

11. OTHER COMPUTER SECURITY INCIDENTS – Continued

b. Please briefly describe these computer security incidents.

   c. How many of these incidents were reported to law enforcement, FedCIRC, ISAC or CERT? INCLUDE incidents reported to local, State or Federal law enforcement, the Federal Computer Incident Response Center, the Information Sharing and Analysis Center or the CERT® Coordination Center.

   d. For the incidents in 11a, were any of the suspected offenders employed by this company at the time of the incident?

   e. How many of the other computer security incidents in 11a resulted in the downtime of this company’s servers, routers, switches, individual PCs/workstations or websites? INCLUDE downtime needed for repairs.

   f. What was the total downtime (in hours) of each of the following due to these other computer security incidents?

   1) Downtime of company websites/web servers
   2) Downtime of servers, routers or switches
   EXCLUDE downtime of websites/web servers.
   3) Downtime of individual PCs/workstations
   EXCLUDE network-wide downtime reported above.

   g. How much was spent in 2001 to recover from these other computer security incidents? ESTIMATES are acceptable.
   INCLUDE the cost – both internal and external – of diagnosis, repair and replacement such as labor, hardware, software, etc.
   EXCLUDE costs associated solely with the prevention of future incidents.

   h. What other monetary losses and costs were incurred in 2001 due to these incidents? ESTIMATES are acceptable.
   INCLUDE actual losses such as the value of lost information.
   INCLUDE the estimated value of downtime, lost productivity, income from lost sales, labor or fees for legal or investigative work, etc.

   i. How many of the incidents in 11a resulted in recovery costs or other monetary losses and costs reported above?
For Questions 12–15, please report for the single most significant computer security incident for this company in 2001. If there were multiple similar incidents, choose ONE representative incident.

12. For the incidents reported in this survey, in what month did this company’s single most significant computer security incident occur?

13a. Which of this company’s computer networks were affected in this particular incident? Mark (X) all that apply.

13b. Which of the following were used to access this company’s networks in this particular incident? Mark (X) all that apply.

13c. If this particular incident resulted in any downtime, what was the total duration (in hours) of each of the following? INCLUDE downtime needed for repairs.

13d. How much was spent in 2001 to recover from this particular incident? ESTIMATES are acceptable.

13e. In this particular incident, what was the dollar value of money or other things taken or lost (by embezzlement, fraud, theft, vandalism, sabotage, etc.)? ESTIMATES are acceptable.

14a. To which of the following organizations was this incident reported? Mark (X) all that apply.

14b. If this incident was not reported to any of the organizations listed in 14a, what were the reasons? Mark (X) only one.

14c. What other monetary losses and costs were incurred in 2001 due to this incident? ESTIMATES are acceptable. INCLUDE the estimated value of downtime, lost productivity, income from lost sales, labor or fees for legal or investigative work, etc.

14d. In this particular incident, what was the dollar value of other tangible assets (such as inventory, equipment, products, etc.) taken or lost (by embezzlement, fraud, theft, vandalism, sabotage, etc.)? ESTIMATES are acceptable.

15. What was the relationship between the suspected offender and this company at the time of this particular incident? Mark (X) only one. If there were multiple offenders, answer for the one viewed as the principal offender.
V. OTHER TRENDS IN COMPUTER SECURITY

16. In 2001, was the overall number of computer security incidents detected by this company more, less or about the same compared to the number detected in 2000? Mark (X) only one.

01 More
02 Less
03 About the same/did not change
04 Don’t know

17. In 2001, did this company have a separate insurance policy or rider to cover losses due specifically to computer security breaches?

01 Yes
02 No
03 Don’t know

18a. In 2001, which of the following types of digital products did this company develop for resale? Mark (X) all that apply.

01 Software
02 Music
03 Motion pictures
04 Other – Specify
05 None; company did not produce digital products for resale in 2001 – (If “None,” skip to 19a.)

b. In 2001, did this company experience any unlicensed use or copying (piracy) of digital products which it developed for resale?

01 Yes
02 No – (Skip to 19a.)
03 Don’t know – (Skip to 19a.)

c. What was the estimated revenue lost in 2001 due to this unlicensed use or copying?

VI. COMPANY INFORMATION

19a. In 2001, which of the following Internet services, if any, did this company provide? Mark (X) all that apply.

01 Internet Service Provider (ISP)
02 Web Search Portal
03 Internet Publishing
04 Internet Broadcasting
05 None of the above – (Skip to 20.)

b. In 2001, which of the following Internet services, if any, was the PRIMARY business activity for this company? Mark (X) only one.

01 Internet Service Provider (ISP)
02 Web Search Portal
03 Internet Publishing
04 Internet Broadcasting
05 None of the above

VI. COMPANY INFORMATION – Continued

20. What were the total sales, receipts and operating revenue for this company in 2001? Estimates are acceptable.

$ Mil. Thou. Dol.

21. What was the total number of employees on this company’s payroll for the pay period which includes March 12, 2001? Estimates are acceptable. Count EACH part-time employee as one. EXCLUDE contractors, leased and temporary employees.

604 Number

22. Does the information reported in this survey cover the calendar year 2001?

01 Yes
02 No – Specify period covered:

FROM

TO

Month Year

Month Year

23. What was this company’s operational status at the end of 2001? Mark (X) only one.

01 In operation
02 Under construction, development or exploration
03 Temporary or seasonally inactive
04 Ceased operation
05 Sold to another operator

609 Month Year

Successor company (if sold):

Company Name

Street address

City State Zip code

CONTACT INFORMATION

Person to contact regarding this report:

Name

Title

Telephone number Extension

Fax number

E-mail address

Please make a copy of this form for your records.

Use a separate sheet of paper for any explanations that may be essential in understanding your reported data.