FORM	CS-	<b>1A</b>
(7-31-2	002)	

# **2001 COMPUTER SECURITY SURVEY**

Economics and Statistics Administration U.S. CENSUS BUREAU Acting As Collecting Agent For BUREAU OF JUSTICE STATISTICS U.S. DEPARTMENT OF JUSTICE

**DUE DATE:** 

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** 

(Please correct any errors in name, address and ZIP Code)

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.

# Please refer to the enclosed instructions before completing the survey.

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.

#### I. COMPUTER SECURITY CONCERNS

- **1.** What are the top three computer security concerns for this company? *Mark* (*X*) *three.* 
  - 101 01 Cembezzlement

02 Fraud

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

<ul> <li>a) Tridues control tervision of the source of the</li></ul>	2a. In 2001, what types of computer networks did this	<b>3b.</b> In 2001, how much did this company spend on the types
LDCATIONS. Mark (X) all that apply.   an   an   an   an   bit Local area network (VAN)   bit Process control network (VPN)   compared the network (VPN) <t< th=""><th>company use? For this survey, "company" means DOMESTIC</th><th></th></t<>	company use? For this survey, "company" means DOMESTIC	
Sol Description   Sol EXCLUDE personnel costs   Sol Sol   Charles are network (LAN)   Sol Process control network (PN)   Sol Process control network (PN)   Sol Process control network (PN)   Sol Process control charl merchange (ED)   Sol Process control network (PN)   Sol Process control network (PN) <th></th> <th></th>		
e. Wide area network (WAx) C. What percentage of this company's total 2001 Information C. In 2001, what computer security association of union information in 2000 Information C. In 2001, what computer security association of union information in 2000 Information information in 2000 Information C. In 2001, what types of company is other n		
e. Wide area network (WAx) C. What percentage of this company's total 2001 Information C. In 2001, what computer security association of union information in 2000 Information C. In 2001, what computer security association of union information in 2000 Information information in 2000 Information C. In 2001, what types of company is other n	o1 Local area network (LAN)	
<ul> <li>process control network (PCN)</li> <li>process c</li></ul>		c. What percentage of this company's total 2001 Information
<ul> <li>or Urtual private network (VPN)</li> <li>clastronic Data Internet</li> <li>clastronic Data Internet</li></ul>		Technology budget did this company spend on the types of
<pre>c = Electronic Data Interchange (EDI) c = Compares shework (e.g., 802.11) c = Compares system security technology identified in 3 c = Compares system security technology identified in 3 c = Compares system security technology identified in 3 c = Compares system security technology identified in 3 c = Compares system security technology identified in 3 c = Compares system security technology identified in 3 c = Compares system security technology identified in 3 c = Compares system security technology identified in 3 c = Compares system security technology identified in 3 c = Compares system security technology identified in 3 c = Compares system security technology identified in 3 c = Compares system security tervices did this company have? c = In 2001, what oppes of access to its c = Conter - Specify c = Conter - Specify c = Compares security security program for computer security program for computer security c = Compares security audit standards c = Compares securit</pre>		
<ul> <li>windess network (e.g., 802.11)</li> <li>winternat</li> <li>b. In 2001, thermant</li> <li>company has no computers - (Skip to 20, page 8.)</li> <li>company has no computers - (Skip to 20, page 8.)</li> <li>company have?</li> <li>don't know</li> <li>company have?</li> <li>company have?</li></ul>		
a       In 2001, was the amount this company spent on the types of computer system security technology identified in 3a company has no computers - (Skip to 20, page 8.)         b       In 2001, how many servers did this company have?         c. In 2001, how many individual PCs and workstations did this company have?       Number         c. In 2001, how many individual PCs and workstations did this company have?       Number         c. In 2001, which of the following types of access to its networks did this company support? Mark (X) all that apply.       Image: Stand-did not change and Don't know         d. In 2001, which of the following types of access to its networks did this company support? Mark (X) all that apply.       Image: Stand-did not change and Don't know         d. In 2001, which of the following types of access to its onetworks through Internet       Don't know         a       Dytreless access to Internet       Don't know         a       Other - Specify       System administration of computer security and computer security and this apply.         a       Don't know       System administrative logs       Don't know         a       Intrusion detection system       Don't know       System administrative logs         a       Intrusion detection system       Don't know         a       Induction of the above       Don't know         a       Don't know       Specify       Don't know         a       <		
aintranet         aintranet         bistand-alone PCS (not on LAN)         1: Company has no computers - (Skip to 20, page 8.)         1: Don't know         bin 2001, how many servers did this company have?         c. In 2001, how many individual PCs and workstations did this company have?         c. In 2001, which of the following types of access to its networks did this company support? Mark (X) all that apply.         ci. In 2001, which of the following types of access to its networks did his company support? Mark (X) all that apply.         ci. In 2001, which of the following types of access to its networks did his company support? Mark (X) all that apply.         ci. In 2001, which of the following types of access to its networks did his company support? Mark (X) all that apply.         ci. In 2001, which of the following types of access to its networks did his company support? Mark (X) all that apply.         ci. In 2001, what yos conceptor security accessible website WITH e-commerce capabilities         ci. Don't know         ci. In 2001, what types of computer security was done in-house         ci. In 2001, what types of computer security accessible website WITH e-commerce capabilities         ci. Biometrics         ci. Biometrics         ci. Biometrics         ci. Biometrics         ci. Frail logs/filters         ci. Biometrics         ci. Biometrics         ci. Conther asystem		
a d_ Extranct   a d_ Extranct   a d_ Extranct   a d_ Don't know         b. in 2001, how many servers did this company have?   zom_ Number         c. in 2001, how many individual PCs and workstations did this company have?   zom, Number      c. in 2001, how many individual PCs and workstations did this company support? Mark (X) all that apply.   zom   d. in 2001, which of the following types of access to its metworks did this company support? Mark (X) all that apply.   a d_ Profile dal-in access   a d_ Wrieless access to Internet   a d_ Other - Specify   a d_ Other - Specify   a d_ Don't know		
<ul> <li>spent in 2007 Mark (X) only one.</li> <li>spent in 2007 Mark (X) only one.</li> <li>company has no computers - (Skip to 20, page 8.)</li> <li>company have no computers - (Skip to 20, page 8.)</li> <li>company have?</li> <li>company have?</li> <li>company have?</li> <li>contract out to a third party? Mark (X) all that apply.</li> <li>contract out to a third party? Mark (X) all that apply.</li> <li>contract out to a third party? Mark (X) all that apply.</li> <li>contract out to a third party? Mark (X) all that apply.</li> <li>contract out to a third party? Mark (X) all that apply.</li> <li>contract out to a third party? Mark (X) all that apply.</li> <li>contract out to a third party? Mark (X) all that apply.</li> <li>contract out to a third party? Mark (X) all that apply.</li> <li>contract out to a third party? Mark (X) all that apply.</li> <li>contract out to a third party? Mark (X) all that apply.</li> <li>contract out to a third party? Mark (X) all that apply.</li> <li>contract out to a third party? Mark (X) all that apply.</li> <li>contract out to a third party? Mark (X) all that apply.</li> <li>contract out to a third party? Mark (X) all that apply.</li> <li>contract out to a third party? Mark (X) all that apply.</li> <li>contract out to a third party? Mark (X) all that apply.</li> <li>contract out to a third party? Mark (X) all that apply.</li> <li>contract out to a third party? Mark (X) all that apply.</li> <li>contract out to a third party? Mark (X) all that apply.</li> <li>continuity of the following there is access to enail out the salue out</li></ul>	09 Extranet	
1       Company has no computers - (Skip to 20, page 8.)         1       Company has no computers - (Skip to 20, page 8.)         1       Company have?         2       Number         2       Number         2       In 2001, how many individual PCs and workstations did this company support? Mark (X) all that apply.         2       In 2001, which of the following types of access to its networks did this company support? Mark (X) all that apply.         2       Intrusion/penetration of computer security and therest access to its networks through Internet         0       Wireless access to internet         0       Ba In 2001, what types of computer system administrative logs         0       Charle Same did this company was? Mark (X) all that apply.         20       System administrative logs <td< th=""><th>—</th><th></th></td<>	—	
12 □ Don't know         b. In 2001, how many servers did this company have?         200         c. In 2001, how many individual PCs and workstations did this company have?         200         c. In 2001, which of the following types of access to its networks did this company support? Mark (X) all that apply.         200         200         200         201, which of the following types of access to its networks did this company support? Mark (X) all that apply.         201         202         203         204         Chin 2001, which of the following types of access to its networks did this company support? Mark (X) all that apply.         204         205         206         207         208         209         209         209         200         200         201         202         203         204         204         205         205         206         206         207         208         208         209         200         200         200		
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?       200       Number         c. In 2001, how many individual PCs and workstations did this company have?       200       Number         c. In 2001, which of the following types of access to its metworks did this company support? Mark (X) all that apply.       201       Publicly accessible website WITH of the retworks are publicly accessible website WITH of the acompany is other networks are publicly accessible website WITH of the acompany is other networks are publicly accessible website WITH of the apply.       200       Company have?       200         a. In 2001, what types of computer system security technology did this company use? Mark (X) all that apply.       200       200       200         a. In 2001, what types of computer system security technology did this company use? Mark (X) all that apply.       200       200       200         a. In 2001, what types of computer system security technology did this company use? Mark (X) all that apply.       200       200       200         a. In 2001, what types of computer system security technology did this company use? Mark (X) all that apply.       200       200       200         a. In 2001, what types of computer security audits       200       200       200       200         a. In 2001, what types of computer system security program for computer security audits       200       200 <th></th> <th>01 More</th>		01 More
Sompany have? Aumber C. In 2001, how many individual PCs and workstations did this company have? 203 Aumber C. In 2001, which of the following types of access to its networks did this company support? Mark (X) all that apply. 204 C. In 2001, which of the following types of access to its networks did this company support? Mark (X) all that apply. 205 C. In 2001, which of the following types of access to its order works through Internet C. In 2001, which of the following types of access to its order works through Internet C. In 2001, which of the following types of access to its company's other networks C. Wireless access to instructive security C. In 2001, what types of computer security C. In 2001, what types of computer security C. In 2001, what types of computer system security C. In 2001, what types of computer system security C. In 2001, what types of computer system security C. In 2001, what types of computer system security C. In 2001, what types of computer system security C. In 2001, what types of computer system security C. In 2001, what types of computer system security C. In 2001, what types of computer system security C. In 2001, what types of computer system security C. In 2001, what types of computer system security C. In 2001, what types of computer system security C. In 2001, what types of computer system security C. In 2001, what types of computer system security C. In 2001, what types of computer system security C. In 2001, what types of computer system security C. In 2001, what types of computer system security C. In 2001, what types of computer security C. In the iso of the above C. In 2001, what types of compu		
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.       203       203         204       Bemote diakin access       0       Company support? Mark (X) all that apply.         204       Company support? Mark (X) all that apply.       203         205       Company support? Mark (X) all that apply.       203         206       Company support? Mark (X) all that apply.         207       Company accessible website WITHOUT e-commerce capabilities         208       Company support? Mark (X) all that apply.         209       Company have? Mark (X) all that apply.         200       Company have? Mark (X) all that apply.         201       System administrative logs         202       Company have? Mark (X) all that apply.         203       Company have? Mark (X) all that apply.	<b>b.</b> In 2001, how many servers did this	03 About the same/did not change
workstations did this company have?       203       Number         contract out to a third party? Mark (X) all that apply.         ad. In 2001, which of the following types of access to its metworks did this company support? Mark (X) all that apply.       204         ad.       Contract out to a third party? Mark (X) all that apply.         ad.       Contract out to a third party? Mark (X) all that apply.         ad.       Contract out to a third party? Mark (X) all that apply.         ad.       Contract out to a third party? Mark (X) all that apply.         ad.       Contract out to a third party? Mark (X) all that apply.         ad.       Contract out to a third party? Mark (X) all that apply.         ad.       Contract out to a third party? Mark (X) all that apply.         ad.       Contract out to a third party? Mark (X) all that apply.         ad.       Contract out to a third party? Mark (X) all that apply.         ad.       Contract out to a third party? Mark (X) all that apply.         ad.       Contract out to a third party? Mark (X) all that apply.         ad.       Contract out to a third party? Mark (X) all that apply.         ad.       Contract out to a third party? Mark (X) all that apply.         ad.       Contract out to a third party? Mark (X) all that apply.         ad.       Contract out to a third party? Mark (X) all that apply.         ad. <th></th> <th>04 Don't know</th>		04 Don't know
workstations did this company have?       203       Number         contract out to a third party? Mark (X) all that apply.         ad. In 2001, which of the following types of access to its metworks did this company support? Mark (X) all that apply.       204         ad.       Contract out to a third party? Mark (X) all that apply.         ad.       Contract out to a third party? Mark (X) all that apply.         ad.       Contract out to a third party? Mark (X) all that apply.         ad.       Contract out to a third party? Mark (X) all that apply.         ad.       Contract out to a third party? Mark (X) all that apply.         ad.       Contract out to a third party? Mark (X) all that apply.         ad.       Contract out to a third party? Mark (X) all that apply.         ad.       Contract out to a third party? Mark (X) all that apply.         ad.       Contract out to a third party? Mark (X) all that apply.         ad.       Contract out to a third party? Mark (X) all that apply.         ad.       Contract out to a third party? Mark (X) all that apply.         ad.       Contract out to a third party? Mark (X) all that apply.         ad.       Contract out to a third party? Mark (X) all that apply.         ad.       Contract out to a third party? Mark (X) all that apply.         ad.       Contract out to a third party? Mark (X) all that apply.         ad. <th></th> <th></th>		
d. In 2001, which of the following types of access to its metworks did this company support? Mark (X) all that apply.         204         a:       Remote dial-in access         a:       Access to networks through Internet         a:       Wireless access to e-mail         a:       Wireless access to internet         b:       Wireless access to this company's other networks         o:       Publicly accessible website WITHOUT e-commerce capabilities         o:       Dubricly accessible website WITH e-commerce capabilities         o:       Don't know         3a. In 2001, what types of computer system security technology did this company use? Mark (X) all that apply.         a:       Don't know         3a. In 2001, what types of computer system security technology did this company use? Mark (X) all that apply.         a:       Don't know         a:       Don't know         a:       Don't know         a:       Don't know         b:       f this company had a computer security practices         a:       Don't know         b:       f 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.       Don't know         b:       f this company had a computer system bus		e. In 2001, what computer security services did this company contract out to a third party? Mark (X) all that apply
d. In 2001, which of the following types of access to its metworks did this company support? Mark (X) all that apply. <ul> <li>□ Evaluation of vulnerability</li> <li>□ Intrusion/petertation testing of computer security</li> <li>□ Intrusion detection system</li> <li>□ Intrusin detection system</li></ul>	workstations and this company have? 203 Number	
activities       activities       activities       activities       activities         activities       activities       activities       activities       activities       activities         activities       activities       activities       activities       activities       activities         acties       acti	d in 2001, which of the following types of eccess to its	
<ul> <li>204</li> <li>a Remote dial-in access</li> <li>b Remote dial-in access</li> <li>c Access to networks through Internet</li> <li>c Wireless access to e-mail</li> <li>c Wireless access to Internet</li> <li>c Wireless access to this company's other networks</li> <li>c Publicly accessible website WITHOUT e-commerce capabilities</li> <li>c Other - Specify</li> <li>c O</li></ul>	<b>a.</b> In 2001, which of the following types of access to its networks did this company support? Mark (X) all that apply.	
<ul> <li>access to networks through Internet</li> <li>Access to networks through Internet</li> <li>Access to networks through Internet</li> <li>Wireless access to networks to e-mail</li> <li>Wireless access to this company's other networks</li> <li>Publicly accessible website WITHOUT e-commerce capabilities</li> <li>Other - Specify</li> <li>None of the above</li> <li>Don't know</li> <li>a. In 2001, what types of computer system security technology did this company use? Mark (X) all that apply.</li> <li>Anti-virus software</li> <li>Biometrics</li> <li>Biometrics</li> <li>Biometrics</li> <li>Biometrics</li> <li>Biometrics</li> <li>System administrative logs</li> <li>Fermail logs/filters</li> <li>System administrative logs</li> <li>Corporate policy on computer security audits</li> <li>Formal computer security audits</li> <li>Biometrics</li> <li>System administrative logs</li> <li>Corporate policy on computer security audits</li> <li>Biometrics</li> <li>System administrative logs</li> <li>Corporate policy on computer security audits</li> <li>Biometrics</li> <li>System administrative logs</li> <li>Corporate policy on computer security audits</li> <li>Biometrics</li> <li>System administrative logs</li> <li>Corporate policy on computer security audits</li> <li>Biometrics</li> <li>System administrative logs</li> <li>Corporate policy on computer security audits</li> <li>Bi fit is company had a computer system business</li> <li>Continuity or disaster recovery program, was it tested, used in an emergency situation and/or updated in 2001?</li> <li>Mark (X) all that apply.</li> <li>Mark (X) all that apply.</li> </ul>		
<ul> <li>a Access to networks through Internet</li> <li>Wireless access to networks through Internet</li> <li>Wireless access to Internet</li> <li>Introving of computer system security</li> <li>Intrusion detection system</li> <li>Don't know</li> <li>Intrusion detection system</li> <li>Don't know</li> <li>Intrusion detection system</li> <li>Don't know</li> <li>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?</li> <li>Mark (X) all that apply.</li> <li>Wark (X) all that apply.</li> </ul>	o1 Remote dial-in access	
<ul> <li>wireless access to e-mail</li> <li>wireless access to e-mail</li> <li>wireless access to Internet</li> <li>wireless access to Internet</li> <li>wireless access to Internet</li> <li>wireless access to this company's other networks</li> <li>Publicly accessible website WITHOUT e-commerce capabilities</li> <li>Publicly accessible website WITHOUT e-commerce capabilities</li> <li>Publicly accessible website WITHOUT e-commerce capabilities</li> <li>o Don't know</li> <li>a. In 2001, what types of computer security practices did this company have? Mark (X) all that apply.</li> <li>a. In 2001, what types of computer system security</li> <li>technology did this company use? Mark (X) all that apply.</li> <li>Anti-virus software</li> <li>Biometrics</li> <li>Digital certificates</li> <li>Encryption</li> <li>Firewall</li> <li>Intrusion detection system</li> <li>One-time password generators (smartcards, tokens, keys)</li> <li>Passwords (changed every 30 or 60 days, etc.)</li> <li>Passwords (changed every 30 or 60 days, etc.)</li> <li>Don't know</li> <li>If this company have 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.</li> </ul>		
<ul> <li>ad Wireless access to Internet</li> <li>by Wireless access to this company's other networks</li> <li>cy Publicly accessible website WITHOUT e-commerce capabilities</li> <li>cy Publicly accessible website WITH e-commerce capabilities</li> <li>dy Publicly accessible website WITH e-commerce capabilities</li> <li>dy Publicly accessible website WITH e-commerce website webs</li></ul>	-	05 Other – Specify
<ul> <li>a. In 2001, what types of computer security practices did this company have? Mark (X) all that apply.</li> <li>a. In 2001, what types of computer system security technology did this company use? Mark (X) all that apply.</li> <li>a. In 2001, what types of computer system security technology did this company use? Mark (X) all that apply.</li> <li>a. In 2001, what types of computer system security technology did this company use? Mark (X) all that apply.</li> <li>a. In 2001, what types of computer system security technology did this company use? Mark (X) all that apply.</li> <li>b. If this company have? Mark (X) all that apply.</li> <li>b. If this company have? the above in computer security or disaster recovery program, was it tested, used in an emergency situation and/or updated in 2001? Mark (X) all that apply.</li> <li>b. If this company have? and the above incomputer security and it standards in a mergency situation and/or updated in 2001? Mark (X) all that apply.</li> <li>b. If this company have? and the above incomputer security and it standards incompany have? It apply.</li> <li>b. If this company have? and the above incomputer security and it standards incompany have? It apply.</li> <li>b. If this company have? and the above incomputer security and it standards incompany have? It apply.</li> <li>b. If this company have? It apply.</li> <li>company ha</li></ul>		06 None; all computer security was done in-house
<ul> <li>a. In 2001, what types of computer security practices did this company have? Mark (X) all that apply.</li> <li>a. In 2001, what types of computer system security technology did this company use? Mark (X) all that apply.</li> <li>a. In 2001, what types of computer system security technology did this company use? Mark (X) all that apply.</li> <li>a. In 2001, what types of computer system security technology did this company use? Mark (X) all that apply.</li> <li>a. In 2001, what types of computer system security technology did this company use? Mark (X) all that apply.</li> <li>b. Formal computer security audits</li> <li>c. Digital certificates</li> <li>c. Digital certificates</li> <li>c. Don't know</li> <li>c. Done-time password generators (smartcards, tokens, keys)</li> <li>c. Deswords (changed every 30 or 60 days, etc.)</li> <li>c. Don't know</li> <li>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.</li> <li>211</li> <li>other - Specify</li> <li>211</li> <li>other - Specify</li> <li>2211</li> <li>other - Specify</li> <li>2211</li> <li>other - Specify</li> <li>2212</li> <li>2213</li> <li>2214</li> <li>2214</li> <li>2214</li> <li>2215</li> <li>2216</li> <li>2216</li> <li>2216</li> <li>2217</li> <li>2218</li> <li>2218</li> <li>2218</li> <li>2219</li> <li>2219</li> <li>2210</li> <li>2210</li> <li>2210</li> <li>2211</li> <li>2211</li> <li>2211</li> <li>2211</li> <li>2211</li> <li>2212</li> <li>2214</li> <li>2214</li> <li>2214</li> <li>2215</li> <li>2216</li> <li>2216</li> <li>2217</li> <li>2218</li> <li>2218</li> <li>2219</li> <li>2219</li> <li>2210</li> <li>2210</li> <li>2211</li> <li>2211</li> <li>2211</li> <li>2211</li> <li>2212</li> <li>2214</li> <li>2214</li> <li>2214</li> <li>2215</li> <li>2216</li> <li>2216</li> <li>2216</li> <li>2217</li> <li>2218</li> <li>2218</li> <li>2218</li> <li>2219</li> <li>2219</li> <li>2210</li> <li>2210</li> <li>2211</li> <li>2211</li> &lt;</ul>	05 Wireless access to this company's other networks	07 Don't know
<ul> <li>a. In 2001, what types of computer security practices did this company have? Mark (X) all that apply.</li> <li>a. In 2001, what types of computer system security rechnology did this company use? Mark (X) all that apply.</li> <li>a. In 2001, what types of computer system security technology did this company use? Mark (X) all that apply.</li> <li>a. In 2001, what types of computer system security technology did this company use? Mark (X) all that apply.</li> <li>b. If this company have? Mark (X) all that apply.</li> <li>b. If this company have? Mark (X) all that apply.</li> <li>cos</li> <licos< li=""> <li>cos</li> <li< th=""><th></th><th></th></li<></licos<></ul>		
06       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.       Disaster recovery program for computer systems         205       On Anti-virus software       Digital certificates         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 passwords (changed every 30 or 60 days, etc.)         11       Other - Specify         12       None, no computer security         13       Don't know		4a. In 2001, what types of computer security practices did
<ul> <li>None of the above</li> <li>Don't know</li> <li>a. In 2001, what types of computer system security technology did this company use? Mark (X) all that apply.</li> <li>Anti-virus software</li> <li>Biometrics</li> <li>Digital certificates</li> <li>Biometrics</li> <li>Digital certificates</li> <li>Encryption</li> <li>System administrative logs</li> <li>Encryption</li> <li>System administrative logs</li> <li>Encryption</li> <li>Dirt know</li> <li>Don't know</li> <li>Dirt specify</li> <li>Other - Specify</li> <li>Other - Specify</li> <li>Don't know</li> <li>Dirt show</li> <li>Don't know</li> <li>Don't know</li> <li>Don't know</li> <li>Don't know</li> <li>Don't know</li> <li>Don't know</li> <li>Digital certificates</li> <li>Digital cerificates<!--</th--><th></th><th>this company have? Mark (X) all that apply.</th></li></ul>		this company have? Mark (X) all that apply.
10       Don't know         3a. In 2001, what types of computer system security technology did this company use? Mark (X) all that apply.       Disaster recovery program for computer systems         205       Image: Computer system security technology did this company use? Mark (X) all that apply.         206       Image: Computer system security technology did this company use? Mark (X) all that apply.         206       Image: Computer security audits that apply.         206       Image: Computer security audits that apply.         207       Training employees in computer security audits that adds         208       Other - Specify         209       None of the above         209       None of the above         209       None of the above         209       One-time password generators (smartcards, tokens, keys)         201       Passwords (changed every 30 or 60 days, etc.)         211       Other - Specify         22       None; no computer security         23       Don't know         24       None; no computer security         25       Used in emergency situation         26       Used in emergency situation         27       Tested         28       Updated         29       None of the above		210
3a. In 2001, what types of computer system security technology did this company use? Mark (X) all that apply.       Image: Computer security audits apply.         205       Image: Computer security audit standards and the security and the security practices are provided in the security and the security practices are provided in the security and the security practices are provided in the security and the security practices are provided in the security and the security practices are provided in the security are provided are prov		01 Business continuity program for computer systems
3a. In 2001, what types of computer system security technology did this company use? Mark (X) all that apply.         205         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	10 Don't know	02 Disaster recovery program for computer systems
technology did this company use? Mark (X) all that apply.         205         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		03 Corporate policy on computer security
205       05       Periodic computer security audits         01       Anti-virus software       05       Periodic computer security audits         02       Biometrics       06       Formal computer security audits         03       Digital certificates       07       Training employees in computer security practices         04       E-mail logs/filters       08       Other - Specify       09         05       System administrative logs       08       Other - Specify       09         06       Encryption       10       Don't know         07       Firewall       08       Intrusion detection system       09         08       One-time password generators (smartcards, tokens, keys)       10       Don't know         10       Other - Specify       03       ad a computer system business continuity or disaster recovery program, was it tested, used in an emergency situation and/or updated in 2001?         11       Other - Specify       01       Tested         12       None; no computer security       02       Used in emergency situation         13       Don't know       03       Updated         04       None of the above       04		04 Regular review of system administrative logs
01 Anti-virus software   02 Biometrics   03 Digital certificates   04 E-mail logs/filters   05 System administrative logs   06 Encryption   07 Firewall   08 Other - Specify   09 None of the above   10 Don't know <b>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. 211 01 Tested 02 Used in emergency situation 03 Updated 04 None of the above 05 06 10 10 10 10 11 01 11 01 12 None; no computer security 13 10 13 10 14 14 15 16 16 17 17 18 18 19 19 10 10 10 10 10 10 10 10 11 10 11 10 11 11 11 11 12 12 13 14 14 15 16 16 17 17 18 18 19 19 10 19 10 10 10 10 11 10 11 10 11 10 11 10 11 10 11 10 11 10 11 10 11 10 11 10 11 11 10 12 12 13 13 14 14 15 16 16 16 17 17 17 18 18 18 18 19 19 19 10 10 10 10 10 10 10 10 10 10 10 10<!--</b--></b>		05 Periodic computer security audits
<ul> <li>Biometrics</li> <li>Digital certificates</li> <li>E-mail logs/filters</li> <li>System administrative logs</li> <li>Encryption</li> <li>Firewall</li> <li>Intrusion detection system</li> <li>One-time password generators (smartcards, tokens, keys)</li> <li>Passwords (changed every 30 or 60 days, etc.)</li> <li>Other - Specify</li> <li>None; no computer security</li> <li>Don't know</li> <li>Don't know</li> <li>Ubed in emergency situation</li> <li< th=""><th>01 Anti-virus software</th><th><math>_{06}\square</math>Formal computer security audit standards</th></li<></ul>	01 Anti-virus software	$_{06}\square$ Formal computer security audit standards
<ul> <li>Digital certificates</li> <li>E-mail logs/filters</li> <li>System administrative logs</li> <li>System administrative logs</li> <li>Encryption</li> <li>Firewall</li> <li>Intrusion detection system</li> <li>One-time password generators (smartcards, tokens, keys)</li> <li>Passwords (changed every 30 or 60 days, etc.)</li> <li>Other - Specify</li> <li>Other - Specify</li> <li>Tested</li> <li>Used in emergency situation and/or updated in 2001?</li> <li>Mark (X) all that apply.</li> <li>Tested</li> <li>Used in emergency situation</li> <li>Updated</li> <li>Updated</li> <li>None of the above</li> </ul>	_	07 Training employees in computer security practices
<ul> <li>04 E-mail logs/filters</li> <li>05 System administrative logs</li> <li>06 Cother - Specify</li> <li>09 None of the above</li> <li>10 Don't know</li> <li>09 None of the above</li> <li>10 Don't know</li> <li>09 None of the above</li> <li>10 Don't know</li> <li>01 Don't know</li> <li>02 None; no computer security</li> <li>12 None; no computer security</li> <li>13 Don't know</li> </ul>		
<ul> <li>05 System administrative logs</li> <li>09 None of the above</li> <li>10 Don't know</li> <li>09 One-time password generators (smartcards, tokens, keys)</li> <li>10 Passwords (changed every 30 or 60 days, etc.)</li> <li>11 Other - Specify</li> <li>12 None; no computer security</li> <li>13 Don't know</li> <li>09 None of the above</li> <li>10 Don't know</li> <li>09 One-time password generators (smartcards, tokens, keys)</li> <li>10 Tested</li> <li>02 Used in emergency situation</li> <li>03 Updated</li> <li>04 None of the above</li> </ul>	5	
<ul> <li>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.</li> <li>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.</li> <li>continuity or disaster recovery program, was it tested, used in an emergency situation and/or updated in 2001? Mark (X) all that apply.</li> <li>continuity or disaster recovery program, was it tested, used in an emergency situation and/or updated in 2001? Mark (X) all that apply.</li> <li>continuity or disaster recovery program, was it tested, used in an emergency situation and/or updated in 2001? Mark (X) all that apply.</li> <li>continuity or disaster recovery program, was it tested, used in an emergency situation and/or updated in 2001? Mark (X) all that apply.</li> <li>continuity or disaster recovery program, was it tested, used in an emergency situation and/or updated in 2001? Mark (X) all that apply.</li> </ul>	<b>U</b>	
<ul> <li>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.</li> <li>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.</li> <li>continuity or disaster recovery program, was it tested, used in an emergency situation and/or updated in 2001? Mark (X) all that apply.</li> <li>continuity or disaster recovery program, was it tested, used in an emergency situation and/or updated in 2001? Mark (X) all that apply.</li> <li>continuity or disaster recovery program, was it tested, used in an emergency situation and/or updated in 2001? Mark (X) all that apply.</li> <li>continuity or disaster recovery program, was it tested, used in an emergency situation and/or updated in 2001? Mark (X) all that apply.</li> <li>continuity or disaster recovery program, was it tested, used in an emergency situation and/or updated in 2001? Mark (X) all that apply.</li> <li>continuity or disaster recovery program, was it tested, used in an emergency situation and/or updated in 2001? Mark (X) all that apply.</li> <li>continuity or disaster recovery program, was it tested, used in emergency situation and/or updated in 2001? Mark (X) all that apply.</li> </ul>		10 <b>⊡Don't know</b>
<ul> <li>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.</li> <li>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.</li> <li>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.</li> <li>continuity or disaster recovery program, was it tested, used in an emergency situation and/or updated in 2001? Mark (X) all that apply.</li> <li>continuity or disaster recovery program, was it tested, used in an emergency situation and/or updated in 2001? Mark (X) all that apply.</li> <li>continuity or disaster recovery program, was it tested, used in an emergency situation and/or updated in 2001? Mark (X) all that apply.</li> <li>continuity or disaster recovery program, was it tested, used in an emergency situation and/or updated in 2001? Mark (X) all that apply.</li> <li>continuity or disaster recovery program, was it tested, used in an emergency situation and/or updated in 2001? Mark (X) all that apply.</li> <li>continuity or disaster recovery program, was it tested, used in emergency situation and/or updated or local distance of the above.</li> </ul>		
<ul> <li>One-time password generators (smartcards, tokens, keys)</li> <li>Passwords (changed every 30 or 60 days, etc.)</li> <li>Other - Specify</li> <li>None; no computer security</li> <li>Don't know</li> <li>Other - Specify</li> <li>Other - Spe</li></ul>		
10       Passwords (changed every 30 or 60 days, etc.)         11       Other - Specify         12       None; no computer security         13       Don't know		
11       Other - Specify       01       Tested         12       None; no computer security       02       Used in emergency situation         13       Don't know       03       Updated         04       None of the above       04		Mark (X) all that apply.
12       None; no computer security       02       Used in emergency situation         13       Don't know       03       Updated         04       None of the above		
12     None; no computer security     02     Used in emergency situation       13     Don't know     03     Updated       04     None of the above		01 Tested
13 Don't know   03 Updated     04 None of the above		
04 None of the above	13 Don't know	
		•
03 Bont know		05 Don't know

06 Not applicable

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. See page 1 of this survey for more details.

#### **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?

301	
o₁ ☐ Yes → How many incidents were detected?	Number
02 🗌 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. 303 Number
- **c.** For the incidents in 5a, were any of the suspected offenders employed by this company at the time of the incident?

004			
01 ☐ Yes →	In how many	incidents?	
02 No			

	Dawl	t know	
03	 DOD	τκηριλι	

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

	Mil.	Thou.	Dol.
306	\$		
306	φ		

305

Number

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.

	Mil.	Thou.	Dol.
307	\$		

#### 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?

of $\Box$ Yes $\rightarrow$ How many incidents were detected?	 Number
02 🗌 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. 310 Number
- c. For the incidents in 6a, were any of the suspected offenders employed by this company at the time of the incident?

,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,		
o1	312	
02 🗌 No		
os 🗌 Don't know		

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

	Mil.	Thou.	Dol.
313	¢		
313	φ		

Number

### 6. FRAUD - Continued

- FRAOD - Continued				
e. What other monetary losses and 2001 due to these incidents? ES INCLUDE the cost of diagnosis, repa labor, hardware, software, etc. If po	TIM air a ssik	ATES are and replace	acceptat	ole. Ich as
value of downtime, lost productivity income from lost sales, labor or fee for legal or investigative work, etc.		Mil.	Thou.	Dol.
EXCLUDE costs associated solely with the prevention of future incidents.	314	\$	inou.	201.
THEFT OF PROPRIETARY INFOR	MA	TION		
Theft of proprietary information is the plans, blueprints, codes, computer p trade secrets, graphics, copyrighted lists, personal or financial information copying.	orog ma	grams, foi iterial, da	rmulas, re ta, forms,	cipes, files,
EXCLUDE incidents which resulted i Report these in 5 or 6, page 3.	in e	mbezzlem	nent or fra	aud.
EXCLUDE incidents of unlicensed us products – software, music, motion this company for resale. Report thes	pict	ures, etc.	- develo	
a. Did this company detect any inc inside or outside this company u obtain proprietary information f 315	ISe	d a comp	outer in c mpany ii	order to
o1 ☐ Yes → How many incidents we o2 $\square$ No – (If "No," skip to 8.)	ere	detected?	-	Number
b. How many of these incidents we enforcement, FedCIRC, ISAC or reported to local, State or Federal la Computer Incident Response Center and Analysis Center or the	CEI aw e	RT? INCL enforceme	UDE incid ent, the Fe	ederal
CERT® Coordination Center.		317		Number
Section 2. For the incidents in 7a, were an offenders employed by this com incident?				the
318 o1 ☐ Yes → In how many incident o2 ☐ No o3 ☐ Don't know	s?	319		Number
d. What was the dollar value of proprietary information taken	1	Mil.	Thou.	Dol.
by theft in 2001?	320	\$		
What other monetary losses and due to these incidents? ESTIMATI INCLUDE the cost of diagnosis, repa labor, hardware, software, etc. If pos value of downtime, lost productivity income from lost sales, labor or fees	ES a iir a ssib ,	are accep <sup>:</sup> nd replac	table. ement su	ch as
for legal or investigative work, etc. EXCLUDE costs associated solely		Mil.	Thou.	Dol.
with the prevention of future incidents.	321	\$		

## 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 ncoming data, etc.

INCLUDE 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?

22 323	
I ☐ Yes → How many incidents were detected?	 Number
2 🗌 No – (If "No," skip to 9, page 5.)	

Number

- b. In 2001, how many of these incidents of denial of service were caused by a virus, worm or Trojan horse?
- 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. 325 Number
- **d.** For the incidents in 8a, were any of the suspected offenders employed by this company at the time of the incident?

of ☐Yes → In how many incidents?	3	327		_	Number
₀₃ 🗌 Don't know					
What was the total duration (in ho denial of service indicated in 8a?	urs) of t	he	incide	nts	s of
INCLUDE downtime needed for repair	s. :	328			Hours
				_	
How many of these incidents of de		ser	vice re	su	lted
in the company taking some actio to restore the level of service?					
to restore the level of service?	3	329		_	Number
How much was spent in 2001 to re incidents of denial of service? EST					0
INCLUDE the cost – both internal and					
repair and replacement such as					-,
labor, hardware, software, etc.	Mil.	1	Thou.		Dol.
EXCLUDE costs associated solely with the prevention of future		Т			2011
incidents. 330	\$				
What other monetary losses and co				l iı	n 2001
due to these incidents? ESTIMATES INCLUDE the estimated value of	are acce	epta			
downtime, lost productivity, income	Mil.	·	Thou.		Dol.
from lost sales, labor or fees for	\$		I		
legal or investigative work, etc. 331	Ψ				
Usur monu of the incidents in Qo w					
How many of the incidents in 8a re or other monetary losses and cost		in I	ecover	y	COSTS
reported above?		332			Number

9.	VANDALISM OR SABOTAGE (ELECTRONIC)	9	. VANDALISM OR SABOTAGE (ELECTRONIC) – Continued
	Vandalism or sabotage (electronic) is the deliberate or malicious damage, defacement, destruction or other alteration of electronic files, data, web pages, programs, etc.	h	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 incidents of destructive viruses, worms, Trojan horses, etc.		INCLUDE the estimated value of downtime, lost productivity, income Mil. Thou. Dol.
	EXCLUDE incidents of alteration which resulted in fraud. Report these in 6, page 3.		from lost sales, labor or fees for legal or investigative work, etc. 344
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?	i	i. How many of the incidents in 9a resulted in recovery costs or other monetary losses and costs reported above? 345 Number
	<sup>333</sup> <sup>334</sup> 01 □ Yes → How many incidents were detected? Number		
	02 🗌 No – (If "No," skip to 10.)	10	A computer virus is a hidden fragment of computer code which
b	How many of these incidents of vandalism or		propagates by inserting itself into or modifying other programs.
	sabotage were caused by a destructive virus, worm or Trojan horse?335Number		INCLUDE viruses, worms, Trojan horses, etc.
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		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
	Computer Incident Response Center, the Information Sharing and Analysis Center or the CERT® Coordination Center.		horses, etc. Report these in 9.
	CERI® Coordination Center. 336 Number	8	a. Did this company detect any viruses which infected any
d.	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. <sup>337</sup> o1 ☐ Yes → In how many incidents? <sup>338</sup> Number o2 ☐ No		part of its computer systems in 2001?         EXCLUDE viruses already reported in this survey.         700         01 Yes - How many incidents were detected?         Count each different virus as one incident.         701 Number         02 No - (If "No," skip to 11, page 6.)
	03 Don't know	ŀ	p. What was the total number of
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		machines (servers, routers, switches, individual PCs/workstations, etc.) infected by these computer viruses? 702 Number
	for repairs. 339 Number	C	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
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.		Computer Incident Response Center, the Information Sharing and Analysis Center or the CERT® Coordination Center. 349 Number
	1) Downtime of company websites/ web servers	c	d. For the incidents in 10b, were any of the suspected
	2) Downtime of servers, routers or switches EXCLUDE downtime of websites/ web servers. 341 Hours		offenders employed by this company at the time of the incident? EXCLUDE incidents in which an employee inadvertently executed a virus.
	<b>3) Downtime of individual PCs/workstations</b> EXCLUDE network-wide downtime reported above. 342 Hours		01 ☐ Yes → In how many incidents? 351 Number 02 ☐ No 03 ☐ Don't know
g	How much was spent in 2001 to recover from these incidents of vandalism or sabotage? 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.		

# III. TYPES OF COMPUTER SECURITY INCIDENTS - Continued

10.	<b>COMPUTER VIRUS – Continued</b>	b				11.	OTHER CON
e.	What was the total downtime (in following due to these virus inference) INCLUDE downtime needed for repart	ections		ich of	the	b.	Please briefly
	1) Downtime of servers, routers or switches		354		Hours		
	2) Downtime of individual PCs/w EXCLUDE network-wide downtim		ations				
	above.				Hours		
f.	What was the total number of person-hours spent by technical support staff to recover from th					c.	How many or enforcement reported to loc Computer Inci and Analysis (
	computer viruses?		703		Hours		CERT® Coord
g.	How much was spent in 2001 t computer viruses? ESTIMATES a INCLUDE the cost – both internal a repair and replacement such as labor, hardware, software, etc. EXCLUDE costs associated solely	are acc	eptable. ernal – o	f diag		d.	For the incid offenders en incident? <sup>363</sup> o1 □Yes →
	with the prevention of future 356	\$					02 🗌 No
	incluents.						03 🗌 Don't kno
h.	What other monetary losses and 2001 due to these incidents? ES INCLUDE actual losses such as the INCLUDE the estimated value of	TIMATI	ES are a	ccepta	ıble.	e.	How many or resulted in the switches, inco or websites? for repairs.
	downtime, lost productivity, income from lost sales, labor	Mil.	Tho	ou.	Dol.		
	or fees for legal or investigative work, etc. 357	\$	 				What was the following du INCLUDE dow
i.	How many of the incidents in 10 costs or other monetary losses a costs reported above?		Ited in	recov	<b>ery</b> Numbe	er l	1) Downtime web serve
							2) Downtime EXCLUDE of web server
11.	OTHER COMPUTER SECURITY	INCID	ENTS				3) Downtime EXCLUDE r reported ab
	INCLUDE all other intrusions, breaches and compromises of this company's computer systems (such as hacking or sniffing) regardless of whether or not damage or loss were sustained as a result. EXCLUDE incidents already reported in this survey.						How much w computer se INCLUDE the o repair and rep labor, hardwa
a.	Did this company detect any o				urity		EXCLUDE cost with the preve incidents.
	incidents in 2001?		360			h	What other n
	o1 Yes → How many incidents we o2 No – (If "No," skip to 12, page				_ Numbe		due to these INCLUDE actu INCLUDE the e downtime, los from lost sales legal or invest
						i.	How many of or other mon costs reporte

## **11. OTHER COMPUTER SECURITY INCIDENTS – Continued**

**b.** Please briefly describe these computer security incidents.

361			
			_
c. How many of these incidents were enforcement, FedCIRC, ISAC or CI reported to local, State or Federal law	ERT? INCLU	JDE incid	
Computer Incident Response Center, t			
and Analysis Center or the CERT® Coordination Center.			
CENT® Coordination Center.	362		Number
d. For the incidents in 11a, were any offenders employed by this compa incident? 363			the
$_{01}$ $\Box$ Yes $\rightarrow$ In how many incidents?	364		Number
02 No			-
$03 \square Don't know$			
e. How many of the other computer a resulted in the downtime of this c switches, individual PCs/workstat	ompany's ions		
or websites? INCLUDE downtime ne for repairs.	eded 365		Number
			_
f. What was the total downtime (in h following due to these other comp INCLUDE downtime needed for repai	<b>outer secu</b> rs.		
1) Downtime of company websites web servers	<b>5/</b>		Hours
<ol> <li>Downtime of servers, routers or EXCLUDE downtime of websites/ web servers.</li> </ol>	switches		Hours
3) Downtime of individual PCs/wo	rkstations		-
EXCLUDE network-wide downtime	Rotationo		
reported above.			Hours
g. How much was spent in 2001 to re computer security incidents? ESTIN INCLUDE the cost – both internal and or repair and replacement such as labor, hardware, software, etc.	MATES are	acceptab	le.
EXCLUDE costs associated solely	IVIII.	Thou.	DOI.
with the prevention of future	\$		
<ul> <li>incidents.</li> <li>h. What other monetary losses and conduct to these incidents? ESTIMATES INCLUDE actual losses such as the val</li> </ul>	osts were are accept	able.	
<ul> <li>incidents.</li> <li>h. What other monetary losses and conduct to these incidents? ESTIMATES INCLUDE actual losses such as the val INCLUDE the estimated value of</li> </ul>	osts were are accept	able.	
<ul> <li>incidents.</li> <li>h. What other monetary losses and conduct to these incidents? ESTIMATES INCLUDE actual losses such as the val</li> </ul>	osts were are accept ue of lost ir	able. Iformatio	n.
incidents. 369 <b>h. What other monetary losses and co due to these incidents?</b> ESTIMATES INCLUDE actual losses such as the val INCLUDE the estimated value of downtime, lost productivity, income from lost sales, labor or fees for legal or investigative work, etc. 370	osts were are accept ue of lost in Mil. \$	able. nformatio Thou.	n. Dol.
incidents. 369 <b>h. What other monetary losses and co due to these incidents?</b> ESTIMATES INCLUDE actual losses such as the val INCLUDE the estimated value of downtime, lost productivity, income from lost sales, labor or fees for	osts were are accept ue of lost in Mil. \$	able. nformatio Thou.	n. Dol.

	IV. SPECI	FIC INCID	DENT INFORMATION				
For Questions 12–15, please report for the single n computer security incident for this company in 200 multiple similar incidents, choose ONE representation	<b>3f. What other monetary losses and costs were incurred in</b> <b>2001 due to this incident?</b> ESTIMATES are acceptable. INCLUDE the estimated value of downtime, lost productivity, income from lost sales, labor						
12. For the incidents reported in this survey did this company's single most signification operative constructions and the second secon	<b>/, in what i</b> ant 401	month Month	or fees for legal or investigative work, etc.				
computer security incident occur? <b>13a.</b> Which of this company's computer netw in this particular incident? Mark (X) all t	<b>vorks were</b> hat apply.		g. Which of the following types describes this particular incident? <i>Mark (X) only one.</i> 411				
02       Wide area network (WAN)       11       In         03       Process control network (PCN)       0         04       Virtual private network (VPN)       12	xtranet dividual wo on LAN) tand-alone F not on LAN ther – <i>Speci</i>	PC )	01 Embezzlement       06 Computer virus         02 Fraud       07 Other computer security         03 Theft of proprietary information       04 Denial of service (to Internet connection or e-mail service)				
o6	on't know		<ul> <li>05 Vandalism or sabotage 08 Not applicable (electronic)</li> <li>14a. To which of the following organizations was this</li> </ul>				
09 🗆 Intranet 15 🗌 N	ot applicabl		<b>incident reported?</b> <i>Mark</i> (X) all that apply.				
<ul> <li>b. Which of the following were used to accent accentaccent accent accent accent accent accent accente accent accent</li></ul>	cess this c	<ul> <li>a12</li> <li>b1 Local law enforcement</li> <li>b2 State law enforcement</li> <li>b3 FBI (Federal Bureau of Investigation)</li> <li>b4 FedCIRC (Federal Computer Incident Response Center)</li> </ul>					
02 Remote dial-in access 03 Access to networks through Internet		<ul> <li>05 Other government agency – Specify</li> <li>06 ISAC (Information Sharing and Analysis Center)</li> </ul>					
04 Wireless access to e-mail 05 Wireless access to Internet 06 Wireless access to this company's othe		<ul> <li>07 CERT® Coordination Center</li> <li>08 None of the above</li> <li>b. If this incident was not reported to any of the</li> </ul>					
<ul> <li>07 Publicly accessible website WITHOUT e- 08 Publicly accessible website WITH e-com</li> <li>09 Other - Specify</li> </ul>		organizations listed in 14a, what were the reasons? Mark (X) all that apply. 413					
10 None of the above 11 Don't know 12 Not applicable		<ul> <li>Negative publicity</li> <li>Lower customer/client/investor confidence</li> <li>Competitor advantage</li> <li>Insident outside invisidiction of law enforcement</li> </ul>					
c. If this particular incident resulted in an was the total duration (in hours) of eacl INCLUDE downtime needed for repairs.			<ul> <li><sup>04</sup> Incident outside jurisdiction of law enforcement</li> <li><sup>05</sup> Reported elsewhere – <i>Specify</i></li> <li><sup>06</sup> Did not want data/hardware seized as evidence</li> </ul>				
1) Denial of service (to Internet connection or e-mail services)	404	Hours	07 ☐ Did not know who to contact 08 ☐ Did not think to report				
2) Downtime of company websites/ web servers	405	Hours	<sup>03</sup> Nothing to be gained/nothing worth pursuing 10 Other – Specify $\swarrow$				
3) Downtime of servers, routers or switt EXCLUDE downtime of websites/ web servers.	406	Hours					
4) Downtime of individual PCs/workstate EXCLUDE network-wide downtime reported above.	407	Hours	<b>15.</b> What was the relationship between the suspected offender and this company at the time of this particular incident? <i>Mark (X) only one.</i>				
d. How much was spent in 2001 to recove particular incident? ESTIMATES are acception INCLUDE the cost – both internal and extern repair and replacement such as labor, hardwork EXCLUDE costs associated solely	otable. nal – of diag vare, softwa	nosis, are, etc.	If there were multiple offenders, answer for the one viewed as the principal offender. 414 01 Current employee, contractor, temporary worker, etc. 02 Former employee, contractor, temporary worker, etc.				
with the prevention of future incidents. 408	Thou.	Dol.	03 Domestic competitor 04 Foreign competitor – <i>Specify country</i>				
e. In this particular incident, what was the money or other things taken or lost (by	dollar valu embezzlem	$_{05}$ Foreign hacker – <i>Specify country</i> $_{06}$ Hacker (no known association with this company)					
fraud, theft, vandalism, sabotage, etc.)? ESTIMATES		Dol.	07 🗌 Other – Specify				
are acceptable. 409 \$			08 🗌 Don't know				

V. OTHER TRENDS IN COMPUTER SECURITY			VI. COMPANY INFORMATION – Continued				
16.	In 2001, was the overall number incidents detected by this comp	of computer s	ecurity or about	20. What were the total sales, receipts and operating			
	the same compared to the numb Mark (X) only one.	per detected in	2000?	revenue for this company Bil.	Mil. Thou.	Dol.	
	501			are acceptable. 603 \$			
	01 More						
	02 Less	~ ~		21. What was the total number of employ company's payroll for the pay period	yees on this	1	
	o3 ☐ About the same/did not chang o4 ☐ Don't know	ye		March 12, 2001? Estimates are accepta Count EACH part-time employee as one.	ible.	, 	
17.	In 2001, did this company have a separate insurance policy or rider to cover losses due specifically to computer security breaches?			EXCLUDE contractors, leased and temporary employees. 604			
	502			22. Does the information reported in this	e eurvov		
	01 Yes			cover the calendar year 2001?	survey		
	03 Don't know			605			
40-		<b></b>		01			
18a	In 2001, which of the following did this company develop for res	types of digita sale? Mark (X) a	all that apply.		Aonth Year		
	503		,	FROM TO	/		
	o1 Software			606 / 607	/		
	02 Music 03 Motion pictures						
	$_{04}$ Other – <i>Specify</i>			23. What was this company's operationa end of 2001? Mark (X) only one.	I status at the		
	05 □ None; company did not produc	ce digital produc	ts for resale	608			
	in 2001 – (If "None," skip to 19a	a.)		01 In operation			
b	In 2001, did this company exper	ience any unli	censed	02 Under construction, development or	exploration		
	use or copying (piracy) of digital developed for resale?	l products whi	ch it	03 Temporary or seasonally inactive	Month Year		
	504			$04 \square$ Ceased operation $04 \square$ Sold to another operator	/		
	01 Yes			$_{05}$ Sold to another operator $\}$ $\rightarrow$ _	/		
	02 🗌 No – (Skip to 19a.)						
	03 Don't know – ( <i>Skip to 19a.</i> )			Successor company (if sold): Company Name			
С	What was the estimated	Mil. Tho	ı. Dol.				
	revenue lost in 2001 due to this unlicensed use or			Street address			
	copying? <sup>505</sup>	\$				_	
				City Sta	te Zip code		
	VI. COMPANY INFO	RMATION					
19a	In 2001, which of the following did this company provide? <i>Mark</i>	Internet servio (X) all that appl	<b>es, if any,</b> y.	CONTACT INFORMA	TION		
	601			Person to contact regarding this rep	oort:		
	01 Internet Service Provider (ISP 02 Web Search Portal	')		Name			
	03 Internet Publishing						
	₀₄ □ Internet Broadcasting			Title			
	05 None of the above – (Skip to .	20.)		Telephone number	Extensi	ion	
h	. In 2001, which of the following	Internet servic	es, if any	( )		511	
	was the PRIMARY business activ	vity for this co	mpany?	Fax number	I		
	Mark (X) only one.			( )			
	01 Internet Service Provider (ISP	)		E-mail address			
	02 Web Search Portal						
	03 Internet Publishing						
	o₄  Internet Broadcasting o₅  None of the above			Please make a copy of this form for	your records.		
						- 41- (	
				Use a separate sheet of paper for an may be essential in understanding y			