FORM	<b>CS-1</b>
(7-31-200	

# **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 Embezzlement
  - 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
  - 07 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>06 🗆 Formal computer security audit standards</th></li<></ul>	01 Anti-virus software	06 🗆 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	
on $\Box$ Yes $\rightarrow$ 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?

504			
01 □Yes →	In how many	incidents?	
02 No			

		D /.	know
03	L II	1)0n't	know

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

	Mil.	Thou.	Dol.
306	\$		

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.

30

EXCLUDE costs associated solely with the prevention of future incidents.

	Mil.	Thou.	Dol.
)7	\$		

#### 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?

511		
o1	312	
02 🗌 No		
03 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.
	<b>•</b>		
313	\$		

Number

#### 6. FRAUD - Continued

<b>2001 due to</b> INCLUDE the labor, hardw value of dow income from	monetary losses and of these incidents? EST e cost of diagnosis, repai vare, software, etc. If poss vntime, lost productivity, n lost sales, labor or fees nvestigative work, etc.	IMATES ar r and repla sible, inclu	e acceptab cement su	le. ch as	Denial of service is connection or e-ma normal flow of info ping attacks, port s incoming data, etc. INCLUDE incidents
EXCLUDE co	vention of future	Mil.	Thou.	Dol.	the cause of the de
	PROPRIETARY INFORM				a. Did this company (a noticeable inte e-mail service) in
plans, bluep trade secrets	prietary information is the rints, codes, computer pr s, graphics, copyrighted r al or financial information	rograms, fo material, da	ormulas, re ata, forms,	cipes, files,	322 01 ☐ Yes → How I 02 ☐ No - (If "No,"
copying. EXCLUDE in	cidents which resulted in in 5 or 6, page 3.				b. In 2001, how mai of denial of servid virus, worm or Tr
products – so	cidents of unlicensed use oftware, music, motion p y for resale. Report these	ictures, etc	. – develop		c. How many of the enforcement, Fed reported to local, S Computer Incident and Analysis Cente CERT® Coordinatio
inside or ou obtain prop 315	mpany detect any incid utside this company us prietary information fro How many incidents wer	sed a com om this co 31	puter in o ompany ir <sup>6</sup>	rder to	d. For the incidents offenders employ incident?
<b>b.</b> How many enforcement	f "No," skip to 8.) of these incidents wer nt, FedCIRC, ISAC or C ocal, State or Federal lav	ERT? INCL	UDE incid		01 ☐Yes → In hor 02 ☐No 03 ☐Don't know e. What was the tot
Computer In and Analysis	cident Response Center, s Center or the dination Center.		ation Shar		denial of service INCLUDE downtime f. How many of the
	idents in 7a, were any employed by this comp			the	in the company ta to restore the lev
318 01 ☐ Yes → 02 ☐ No 03 ☐ Don't ki	In how many incidents	<b>?</b> 31	9	Number	g. How much was sp incidents of denia INCLUDE the cost – repair and replacen labor, hardware, so EXCLUDE costs ass
	the dollar value of y information taken 20012	Mil.	Thou.	Dol.	with the prevention incidents.
ESTIMATES e. What other due to thes INCLUDE the labor, hardw	are acceptable. <sup>32</sup> monetary losses and c e incidents? ESTIMATE: e cost of diagnosis, repair are, software, etc. If poss vntime, lost productivity,	costs were S are accept r and replace	otable. cement suc	ch as	h. What other mone due to these incid INCLUDE the estim downtime, lost proo from lost sales, lab legal or investigativ
income from for legal or i EXCLUDE co	l lost sales, labor or fees nvestigative work, etc. osts associated solely vention of future	Mil. \$	Thou.	Dol.	i. How many of the or other monetar reported above?

#### 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? 324
- **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?

	on $\Box$ Yes $\rightarrow$ In how many incidents?	32	7	Number
	02 🗌 No			
	₀₃□Don't know			
€.	What was the total duration (in ho	urs) of th	e inciden	ts of
	denial of service indicated in 8a?			
	INCLUDE downtime needed for repairs	<b>S.</b> 32	8	Hours
•	How many of these incidents of de	nial of a	orvioo roc	ultod
••	in the company taking some action		ervice res	builleu
	to restore the level of service?	32	9	Number
J.	How much was spent in 2001 to re	cover fro	om these	h la
	incidents of denial of service? EST INCLUDE the cost – both internal and e			
	repair and replacement such as		or anagrio	0.07
	labor, hardware, software, etc. EXCLUDE costs associated solely	Mil.	Thou.	Dol.
	with the prevention of future	¢		
	incidents. 330	\$		
	What other monetary losses and co		inourrod	in 2001
••	due to these incidents? ESTIMATES			111 200 1
	INCLUDE the estimated value of	Mil.	Thou.	Dol.
	downtime, lost productivity, income from lost sales, labor or fees for		THOU.	
	legal or investigative work, etc. <sup>331</sup>	\$		
_		_		
i.	How many of the incidents in 8a re or other monetary losses and cost		recover	y costs
i.	How many of the incidents in 8a re		recover	y costs

332

Number

### **III. TYPES OF COMPUTER SECURITY INCIDENTS – Continued**

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.	<ul> <li>b. 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.</li> </ul>			
	INCLUDE incidents of destructive viruses, worms, Trojan horses, etc.		INCLUDE the estimated value of downtime, lost productivity, income from lost sales, labor or fees for		
	EXCLUDE incidents of alteration which resulted in fraud. Report these in 6, page 3.		legal or investigative work, etc. <sup>344</sup>		
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?	1.	How many of the incidents in 9a         resulted in recovery costs or other         monetary losses and costs reported         above?         345		
	333 334 Number				
	o1 Yes $\rightarrow$ How many incidents were detected? Number 02 No - (If "No," skip to 10.)	10.	COMPUTER VIRUS		
b.	How many of these incidents of vandalism or		A computer virus is a hidden fragment of computer code which propagates by inserting itself into or modifying other programs.		
	sabotage were caused by a destructive virus, worm or Trojan horse? 335 Number		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		EXCLUDE incidents in which viruses caused excessive amounts of incoming data, resulting in denial of service. Report these in 8, page 4.		
	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. 336 Number		EXCLUDE incidents of destructive viruses, worms, Trojan horses, etc. Report these in 9.		
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	a.	In 2001, did this company intercept any computer viruses before they could infect any part of its computer systems? <sup>346</sup> <sup>01</sup> Yes <sup>02</sup> No <sup>03</sup> Don't know $- (Continue with 10b.)$		
	02 No 03 Don't know	b	<ul> <li>Did this company detect any viruses which infected any part of its computer systems in 2001?</li> <li>EXCLUDE viruses already reported in this survey.</li> </ul>		
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.		347 01 Yes → How many incidents of virus infections were detected? Count EACH DISTINCT INFECTION as a separate incident, even if caused by the same virus. 348 Number		
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.	C.	<ul> <li>No – (If "No," skip to 11, page 6.)</li> <li>How many of these incidents were reported to law enforcement, FedCIRC, ISAC or CERT? INCLUDE incidents reported to last activate and states are forcement the Federal law.</li> </ul>		
	1) Downtime of company websites/ web servers		reported to local, State or Federal law enforcement, the Federal Computer Incident Response Center, the Information Sharing and Analysis Center or the		
	2) Downtime of servers, routers or switches EXCLUDE downtime of websites/ web servers. 341 Hours		CERT® Coordination Center. 349 Number		
	3) Downtime of individual PCs/workstations EXCLUDE network-wide downtime reported above	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.		
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.		350 01 Yes → In how many incidents? 351 Number 02 No 03 Don't know		

## **III. TYPES OF COMPUTER SECURITY INCIDENTS – Continued**

10. COMPUTER VIRUS – Continued	11. OTHER COMPUTER SECURITY INC
e. What was the total number of infections for each of the following due to the computer virus incidents in 10b?	<b>b.</b> Please briefly describe these compute
1) Number of server, router or switch infections 352 Number	
2) Number of individual PC/workstation infections INCLUDE infections resulting from server, router and switch infections AND infections from e-mail attachments, disks, Internet	
downloads, etc.       353       Number         f. What was the total downtime (in hours) for each of the following due to these virus infections?       INCLUDE downtime needed for repairs.	c. How many of these incidents were enforcement, FedCIRC, ISAC or CEF reported to local, State or Federal law e Computer Incident Response Center, th and Analysis Center or the CERT® Coordination Center.
1) Downtime of servers, routers or switches 354 Hours	d. For the incidents in 11a, were any o
<ul> <li>2) Downtime of individual PCs/workstations         EXCLUDE network-wide downtime reported above.         355         Hours     </li> <li>B. How much was spent in 2001 to recover from these account of the second secon</li></ul>	offenders employed by this compar incident? 363 01 ☐ Yes → In how many incidents? 02 ☐ No 03 ☐ Don't know
<ul> <li>computer viruses? ESTIMATES are acceptable.</li> <li>INCLUDE the cost – both internal and external – of diagnosis, repair and replacement such as labor, hardware, software, etc.</li> <li>EXCLUDE costs associated solely with the prevention of future incidents.</li> <li>Mil. Thou. Dol.</li> <li>\$</li> <li>\$</li> </ul>	<ul> <li>e. How many of the other computer services in the downtime of this conswitches, individual PCs/workstatic or websites? INCLUDE downtime need for repairs.</li> <li>f. What was the total downtime (in hor following due to these other computer INCLUDE downtime needed for repairs)</li> </ul>
<b>2001 due to these incidents?</b> 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.         357	<ol> <li>Downtime of company websites/ web servers</li> <li>Downtime of servers, routers or s EXCLUDE downtime of websites/ web servers.</li> <li>Downtime of individual PCs/work</li> </ol>
i. How many of the incidents in 10b resulted in recovery costs or other monetary losses and costs reported above? 358 Number	EXCLUDE network-wide downtime reported above.      G. How much was spent in 2001 to rec computer security incidents? ESTIM. INCLUDE the cost – both internal and ex
<b>11. OTHER COMPUTER SECURITY INCIDENTS</b> 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	repair and replacement such as labor, hardware, software, etc. EXCLUDE costs associated solely with the prevention of future incidents.
a result. EXCLUDE incidents already reported in this survey. a. Did this company detect any other computer security incidents in 2001? <sup>359</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>360</sup> <sup>3</sup>	<ul> <li>h. What other monetary losses and cost due to these incidents? ESTIMATES a INCLUDE actual losses such as the value INCLUDE the estimated value of downtime, lost productivity, income from lost sales, labor or fees for legal or investigative work, etc. 370</li> <li>i. How many of the incidents in 11a re or other monetary losses and costs reported above?</li> </ul>

	361			
C.	How many of these incidents were enforcement, FedCIRC, ISAC or CE reported to local, State or Federal law Computer Incident Response Center, th and Analysis Center or the	RT? INCL	UDE incident, the F	ederal
	CERT® Coordination Center.	362		_ Numbe
d	For the incidents in 11a, were any offenders employed by this compa incident?			the
	$_{01}$ Yes $\rightarrow$ In how many incidents?	364		Numbe
	03 Don't know			
	How many of the other computer s resulted in the downtime of this co switches, individual PCs/workstati or websites? INCLUDE downtime need	ompany's ons eded		
	for repairs. What was the total downtime (in h	365 ours) of e	ach of t	_
f	for repairs. What was the total downtime (in he following due to these other comp INCLUDE downtime needed for repair 1) Downtime of company websites,	ours) of e uter secu 's.		he
f	<ul> <li>What was the total downtime (in he following due to these other comp INCLUDE downtime needed for repair</li> <li>1) Downtime of company websites, web servers</li> </ul>	ours) of e uter secu rs. / 	irity inci	he
f	What was the total downtime (in he following due to these other comp INCLUDE downtime needed for repair 1) Downtime of company websites,	ours) of e uter secu rs. / 	irity inci	he dents?
f	<ul> <li>What was the total downtime (in he following due to these other comp INCLUDE downtime needed for repair</li> <li>1) Downtime of company websites, web servers</li> <li>2) Downtime of servers, routers or EXCLUDE downtime of websites/</li> </ul>	ours) of e uter secu 's. <u>366</u> switches	rity inci	he dents?
f	<ul> <li>What was the total downtime (in he following due to these other comp INCLUDE downtime needed for repair</li> <li>1) Downtime of company websites, web servers</li> <li>2) Downtime of servers, routers or EXCLUDE downtime of websites/ web servers.</li> <li>3) Downtime of individual PCs/wor EXCLUDE network-wide downtime</li> </ul>	ours) of e uter secu 's. <u>366</u> switches	rity inci	he dents?
	<ul> <li>What was the total downtime (in he following due to these other comp INCLUDE downtime needed for repair</li> <li>1) Downtime of company websites, web servers</li> <li>2) Downtime of servers, routers or EXCLUDE downtime of websites/ web servers.</li> <li>3) Downtime of individual PCs/wor EXCLUDE network-wide downtime reported above.</li> </ul>	ours) of e uter secu 's. / switches 	irity inci	he dents? Hours Hours Hours
	<ul> <li>What was the total downtime (in he following due to these other comp INCLUDE downtime needed for repair</li> <li>1) Downtime of company websites, web servers</li> <li>2) Downtime of servers, routers or EXCLUDE downtime of websites/ web servers.</li> <li>3) Downtime of individual PCs/wor EXCLUDE network-wide downtime reported above.</li> <li>How much was spent in 2001 to react computer security incidents? ESTIM INCLUDE the cost – both internal and e repair and replacement such as</li> </ul>	ours) of e uter secu 's. / switches 367 kstations 368 cover from IATES are	m these acceptab	he dents? Hours Hours Hours other
	<ul> <li>What was the total downtime (in he following due to these other comp INCLUDE downtime needed for repair</li> <li>1) Downtime of company websites, web servers</li> <li>2) Downtime of servers, routers or EXCLUDE downtime of websites/ web servers.</li> <li>3) Downtime of individual PCs/wor EXCLUDE network-wide downtime reported above.</li> <li>How much was spent in 2001 to recomputer security incidents? ESTIM INCLUDE the cost – both internal and e</li> </ul>	ours) of e uter secu 's. / switches 367 kstations 368 cover from IATES are	m these acceptab	he dents? Hours Hours Hours other
	<ul> <li>What was the total downtime (in he following due to these other comp INCLUDE downtime needed for repair</li> <li>1) Downtime of company websites, web servers</li> <li>2) Downtime of servers, routers or EXCLUDE downtime of websites/ web servers.</li> <li>3) Downtime of individual PCs/wor EXCLUDE network-wide downtime reported above.</li> <li>How much was spent in 2001 to recomputer security incidents? ESTIM INCLUDE the cost – both internal and e repair and replacement such as labor, hardware, software, etc. EXCLUDE costs associated solely with the prevention of future</li> </ul>	ours) of e uter secu 's. / switches 366 switches 367 kstations 368 cover from IATES are xternal – c Mil.	m these acceptab	he dents? Hours Hours Hours other ble. sis,
g	<ul> <li>What was the total downtime (in he following due to these other complexity includes a server of the serve</li></ul>	ours) of e uter secu s. / 	m these acceptak of diagnos Thou.	he dents? Hours Hours Hours other ble. sis, Dol.
g	<ul> <li>What was the total downtime (in he following due to these other comp INCLUDE downtime needed for repair</li> <li>1) Downtime of company websites, web servers</li> <li>2) Downtime of servers, routers or EXCLUDE downtime of websites/ web servers.</li> <li>3) Downtime of individual PCs/wor EXCLUDE network-wide downtime reported above.</li> <li>How much was spent in 2001 to reac computer security incidents? ESTIM INCLUDE the cost – both internal and e repair and replacement such as labor, hardware, software, etc. EXCLUDE costs associated solely with the prevention of future incidents.</li> <li>What other monetary losses and co due to these incidents? ESTIMATES INCLUDE actual losses such as the valu INCLUDE the estimated value of downtime, lost productivity, income</li> </ul>	ours) of e uter secu s. / 	m these acceptak of diagnos Thou.	he dents? Hours Hours Hours other ble. sis, Dol.
g	<ul> <li>What was the total downtime (in he following due to these other comp INCLUDE downtime needed for repair</li> <li>1) Downtime of company websites, web servers</li> <li>2) Downtime of servers, routers or EXCLUDE downtime of websites/ web servers.</li> <li>3) Downtime of individual PCs/wor EXCLUDE network-wide downtime reported above.</li> <li>How much was spent in 2001 to recomputer security incidents? ESTIM INCLUDE the cost – both internal and e repair and replacement such as labor, hardware, software, etc. EXCLUDE costs associated solely with the prevention of future incidents.</li> <li>What other monetary losses and codue to these incidents? ESTIMATES INCLUDE actual losses such as the value INCLUDE the estimated value of</li> </ul>	ours) of e uter secu s. <u>366</u> switches <u>367</u> kstations <u>368</u> cover from ATES are xternal – c Mil. <u>\$</u> sts were are accept ie of lost in Mil.	m these acceptab of diagnos Thou. incurred table. nformatic	he dents? Hours Hours Hours other ble. sis, Dol. I in 200 on.

	IV. SPECIFIC INCIDENT INFORMATION								
	For Questions 12–15, please report for the single most signif computer security incident for this company in 2001. If there multiple similar incidents, choose ONE representative incide	were	<b>13f. 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, in what	t month	or fees for legal or Mil. Thou. Dol.						
	did this company's single most significant computer security incident occur? 401	Month	investigative work, etc. 410 \$						
	<ul> <li>13a. Which of this company's computer networks we in this particular incident? Mark (X) all that apply.</li> <li>402</li> <li>01 Local area network (LAN)</li> <li>10 Extranet</li> </ul>	re affected	<b>g. Which of the following types describes this</b> <b>particular incident?</b> <i>Mark (X) only one.</i> 411 o1 Embezzlement 06 Computer virus						
	02       Wide area network (WAN)       11       Individual w         03       Process control network (PCN)       (on LAN)         04       Virtual private network (VPN)       12       Stand-alone         05       Electronic Data       13       Other - Spe	e PC N)	02       Fraud       07       Other computer security         03       Theft of proprietary information       07       Other computer security         04       Denial of service (to Internet connection or e-mail service)       04       07						
	Interchange (EDI) of Wireless network (e.g., 802.11) or E-mail system		05 Vandalism or sabotage 08 Not applicable (electronic)						
	08 □ Internet   14 □ Don't know     09 □ Intranet   15 □ Not applical	ble	<b>14a. To which of the following organizations was this</b> <b>incident reported?</b> <i>Mark (X) all that apply.</i>						
	<ul> <li>b. Which of the following were used to access this networks in this particular incident? Mark (X) all that apply.</li> <li>403</li> <li>01 Hard-wired communications lines</li> </ul>	company's	412 01 Local law enforcement 02 State law enforcement 03 FBI (Federal Bureau of Investigation) 04 FedCIRC (Federal Computer Incident Response Center)						
	02 Remote dial-in access		05 Other government agency – <i>Specify</i>						
	03 Access to networks through Internet		06 ISAC (Information Sharing and Analysis Center)						
	o₄		07 CERT® Coordination Center						
	$_{06}$ Wireless access to the networks	s							
	o7 Publicly accessible website WITHOUT e-commerce		b. If this incident was not reported to any of the organizations listed in 14a, what were the reasons?						
	08 🗌 Publicly accessible website WITH e-commerce cap	•	Mark (X) all that apply.						
	09 🗌 Other – Specify		413						
	$10 \square$ None of the above		01 Negative publicity						
	11 🗌 Don't know		02 Lower customer/client/investor confidence						
	12 Not applicable		<ul> <li>03 Competitor advantage</li> <li>04 Incident outside jurisdiction of law enforcement</li> </ul>						
	c. If this particular incident resulted in any downtin was the total duration (in hours) of each of the for INCLUDE downtime needed for repairs.	<ul> <li>04 ☐ Incluent outside junsuiction of law enforcement</li> <li>05 ☐ Reported elsewhere – Specify</li> <li>06 ☐ 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						
	2) Downtime of company websites/	Hours	08 Did not think to report						
	web servers 405	Hours	<sup>09</sup> Nothing to be gained/nothing worth pursuing 10 Other – Specify $\mathbf{z}$						
	3) Downtime of servers, routers or switches EXCLUDE downtime of websites/ web servers. 406	Hours	10 Other - Specify Z						
	4) Downtime of individual PCs/workstations		<b>15.</b> What was the relationship between the suspected						
	EXCLUDE network-wide downtime reported above 407	Hours	offender and this company at the time of this particular incident? Mark (X) only one.						
	d. How much was spent in 2001 to recover from th particular incident? ESTIMATES are acceptable. INCLUDE the cost – both internal and external – of dia repair and replacement such as labor, hardware, softw	ignosis,	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.						
	EXCLUDE costs associated solely Mil. Thou.	. Dol.	03 Domestic competitor						
	of future incidents. 408 \$		$_{04}$ Foreign competitor – <i>Specify country</i>						
			$_{05}$ Foreign hacker – Specify country						
e. In this particular incident, what was the dollar value of money or other things taken or lost (by embezzlement,			$_{06}$ Hacker (no known association with this company)						
	fraud, theft, vandalism, Mil Thou								
	sabotage, etc.)? ESTIMATES		07 Other – <i>Specify</i> 08 Don't know						
	are acceptable. 409 \$								

FORM CS-1 (7-31-2002)

	V. OTHER TRENDS IN COMPUTER SECURITY			VI. COMPANY INFORMATION – Continued					
16.	In 2001, was the overall number of computer security incidents detected by this company more, less or about		20. What were the tota receipts and opera						
	the same compared to the numb	per detected in 20	000?	revenue for this co in 2001? ESTIMATE	mpany	Bil.	Mil.	Thou.	Dol.
	Mark (X) only one.			are acceptable.		\$			
	01 More								
	02 Less			21. What was the total	number	of emp	loyees	on this	
	03 About the same/did not chang	ge		company's payroll March 12, 2001? E	stimates a	are acce	ptable.	n includes	;
				Count EACH part-tim EXCLUDE contractor		ee as ol	ne.		
17.	In 2001, did this company have a policy or rider to cover losses de computer security breaches?	a separate insura ue specifically to	ince	leased and temporar employees.					_ Numbe
	502 01 <b>Yes</b>			22. Does the information	ion repor	ted in 1	his surv	/ev	
				cover the calendar	year 200	01?		- 1	
	03 Don't know			605 01 <b>Yes</b>					
100	In 2001, which of the following	turnes of digital m	voduoto	02 No – Specify pe	riod cove	red:			
Iod	did this company develop for res	sale? Mark (X) all a	that apply.	Month	Year		Month	Year	
	503			FROM	loui	то	month	/	
	o1 Software			606 /		607		/	
	02 Music 03 Motion pictures						• • •		
	$_{04}$ Other – <i>Specify</i>			23. What was this com end of 2001? Mark			onal stat	us at the	
	os None; company did not produc	ce digital products	for resale	608					
	in 2001 – (If "None," skip to 19a	a.)		01 In operation					
b	. In 2001, did this company exper	ience any unlice	nsed	02 Under construct		•		oration	
	use or copying (piracy) of digital developed for resale?	I products which	it	03 Temporary or s		inactive	Month	Year	
	504			04 Ceased operation		<b>609</b>		1	
	01 Yes				operator	J		/	
	02 No – (Skip to 19a.)			Cueseser compon	v (if cold)				
	03 Don't know – ( <i>Skip to 19a.</i> )			Successor compan Company Name	y (11 Solu)	•			
С	What was the estimated	Mil. Thou.	Dol.						
	revenue lost in 2001 due to this unlicensed use or			Street address					
	copying? 505	\$							
				City		:	State	Zip code	
	VI. COMPANY INFO	RMATION							
10-	. In 2001, which of the following	Internet corvices	ifany						
154	did this company provide? Mark	(X) all that apply.	, ii uiiy,	СО	NTACT I	NFORM	IATION		
				Person to contact	regardir	ng this	report:		
	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
b	. In 2001, which of the following	Internet services	. if anv.	( )					
	was the PRIMARY business activ	vity for this com	pany?	Fax number				I	
	Mark (X) only one.			( )					
	01 Internet Service Provider (ISP	')		E-mail address					
	02 Web Search Portal								
	03 Internet Publishing								
	04 ☐ Internet Broadcasting 05 ☐ None of the above			Please make a copy	of this	form f	or vou	r records.	
							-		
				Use a separate shee may be essential in					