I. COMPUTER SECURITY CONCERNS

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

   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 ____________________________
II. COMPUTER INFRASTRUCTURE AND SECURITY

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

- Local area network (LAN)
- Wide area network (WAN)
- Process control network (PCN)
- Virtual private network (VPN)
- Electronic Data Interchange (EDI)
- Wireless network (e.g., 802.11)
- Internet
- Intranet
- Extranet
- Stand-alone PCs (not on LAN)
- Company has no computers – (Skip to 20, page 8.)
- Don’t know

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

Number

2b. 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.

- Remote dial-in access
- Access to networks through Internet
- Wireless access to e-mail
- Wireless access to Internet
- Wireless access to this company’s other networks
- Publicly accessible website WITHOUT e-commerce capabilities
- Publicly accessible website WITH e-commerce capabilities
- Other – Specify
- None of the above
- Don’t know

d. In 2001, what computer security services did this company contract out to a third party? Mark (X) all that apply.

- Evaluation of vulnerability
- Intrusion/penetration testing of computer security
- Installation of computer security
- System administration of computer security
- Other – Specify
- None; all computer security was done in-house
- Don’t know

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

- Anti-virus software
- Biometrics
- Digital certificates
- E-mail logs/filters
- System administrative logs
- Encryption
- Firewall
- Intrusion detection system
- One-time password generators (smartcards, tokens, keys)
- Passwords (changed every 30 or 60 days, etc.)
- Other – Specify
- None; no computer security
- Don’t know

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

- Anti-virus software
- Biometrics
- Digital certificates
- E-mail logs/filters
- System administrative logs
- Encryption
- Firewall
- Intrusion detection system
- One-time password generators (smartcards, tokens, keys)
- Passwords (changed every 30 or 60 days, etc.)
- Other – Specify
- None; no computer security
- Don’t know

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

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

ESTIMATES are acceptable. EXCLUDE personnel costs.

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

Round to nearest whole percent.

3d. In 2001, was the amount this company spent on the types of computer system security technology identified in 3a, more, less or about the same compared to the amount spent in 2000? Mark (X) only one.

- More
- Less
- About the same/did not change
- Don’t know

3e. In 2001, was the amount this company spent on the types of computer system security technology identified in 3a, more, less or about the same compared to the amount spent in 2000? Mark (X) only one.

- More
- Less
- About the same/did not change
- Don’t know

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

- Business continuity program for computer systems
- Disaster recovery program for computer systems
- Corporate policy on computer security
- Regular review of system administrative logs
- Periodic computer security audits
- Formal computer security audit standards
- Training employees in computer security practices
- Other – Specify
- None of the above
- Don’t know

4b. 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.

- Tested
- Used in emergency situation
- Updated
- None of the above
- Don’t know
- Not applicable
III. TYPES OF COMPUTER SECURITY INCIDENTS

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

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

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

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

ESTIMATES are acceptable.

5. EMBEZZLEMENT

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

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

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

☐ Yes  → How many incidents were detected? ______________________ Number
☐ No  → (If "No," skip to 6.)

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

☐ Yes  → How many incidents were detected? ______________________ Number
☐ No  → (If "No," skip to 7, page 4.)

6. FRAUD

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

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

EXCLUDE incidents of embezzlement. Report these in 5.

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

☐ Yes  → How many incidents were detected? ______________________ Number
☐ No  → (If "No," skip to 7, page 4.)

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

☐ Yes  → How many incidents were detected? ______________________ Number
☐ No  → (If "No," skip to 7, page 4.)

ESTIMATES are acceptable.

5. EMBEZZLEMENT

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

☐ Yes  → How many incidents were detected? ______________________ Number
☐ No  → (If "No," skip to 6.)

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

☐ Yes  → How many incidents were detected? ______________________ Number
☐ No  → (If "No," skip to 7, page 4.)

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

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

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

$ ___________ Mil. Thou. Dol.

5. EMBEZZLEMENT

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

☐ Yes  → How many incidents were detected? ______________________ Number
☐ No  → (If "No," skip to 6.)

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

☐ Yes  → How many incidents were detected? ______________________ Number
☐ No  → (If "No," skip to 7, page 4.)

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

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

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

$ ___________ Mil. Thou. Dol.
III. TYPES OF COMPUTER SECURITY INCIDENTS – Continued

6. FRAUD – Continued

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

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

7. THEFT OF PROPRIETARY INFORMATION

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

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

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

d. Did this company detect any incidents in which someone inside or outside this company used a computer in order to obtain proprietary information from this company in 2001?

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
<th>Don’t know</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Number

How many incidents were detected?

8. DENIAL OF SERVICE

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

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?

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
<th>Don’t know</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Number

How many of these incidents of denial of service were caused by a virus, worm or Trojan horse?

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

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
<th>Don’t know</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Number

How many 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.

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

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
<th>Don’t know</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Number

How many incidents were detected?

How much was spent in 2001 to recover from these incidents? INCLUDE downtime needed for repairs.

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

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
<th>Don’t know</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Number

How many incidents in 8a were detected?

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

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
<th>Don’t know</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Number

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

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

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

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

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

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

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
<th>Don’t know</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Number

How many incidents in 8a resulted in recovery costs or other monetary losses and costs reported above?
III. TYPES OF COMPUTER SECURITY INCIDENTS – Continued

9. VANDALISM OR SABOTAGE (ELECTRONIC)

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

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

EXCLUDE incidents of alteration which resulted in fraud. Report these in 6, page 3.

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

   333 □ Yes → How many incidents were detected? □ Number
   01 □ No – (If “No,” skip to 10.)

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

   335 □ Number

EXCLUDE viruses already reported in this survey.

EXCLUDE incidents of alteration which resulted in fraud. Report these in 6, page 3.

EXCLUDE incidents in which an employee inadvertently executed a virus.

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.

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

   338 □ Number

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.

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.

   339 □ Number

EXCLUDE downtime of websites/web servers.

EXCLUDE costs associated solely with the prevention of future incidents.

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

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

EXCLUDE network-wide downtime.

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.

   343 □ Mil. □ Thou. □ Dol. $
### III. TYPES OF COMPUTER SECURITY INCIDENTS – Continued

#### 10. COMPUTER VIRUS – Continued

e. What was the total number of infections for each of the following due to the computer virus incidents in 10b?

<table>
<thead>
<tr>
<th>1) Number of server, router or switch infections</th>
<th>352 Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>2) Number of individual PC/workstation infections</td>
<td>353 Number</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>1) Downtime of servers, routers or switches</th>
<th>354 Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>2) Downtime of individual PCs/workstations</td>
<td>355 Hours</td>
</tr>
</tbody>
</table>


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

b. Please briefly describe these computer security incidents.

<table>
<thead>
<tr>
<th>361</th>
</tr>
</thead>
</table>


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

<table>
<thead>
<tr>
<th>362 Number</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>01 Yes</th>
<th>In how many incidents?</th>
</tr>
</thead>
<tbody>
<tr>
<td>02 No</td>
<td></td>
</tr>
<tr>
<td>03 Don’t know</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>363 Number</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>01 Yes</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>02 No</td>
<td></td>
</tr>
<tr>
<td>03 Don’t know</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>364 Number</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>1) Downtime of company websites/web servers</th>
<th>366 Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>2) Downtime of servers, routers or switches</td>
<td>367 Hours</td>
</tr>
<tr>
<td>3) Downtime of individual PCs/workstations</td>
<td>368 Hours</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>369 Hours</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>1) Downtime of company websites/web servers</th>
<th>366 Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>2) Downtime of servers, routers or switches</td>
<td>367 Hours</td>
</tr>
<tr>
<td>3) Downtime of individual PCs/workstations</td>
<td>368 Hours</td>
</tr>
</tbody>
</table>


#### 11. OTHER COMPUTER SECURITY INCIDENTS

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.

<table>
<thead>
<tr>
<th>359</th>
</tr>
</thead>
</table>

a. Did this company detect any other computer security incidents in 2001?

<table>
<thead>
<tr>
<th>360 Number</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>01 Yes</th>
<th>How many incidents were detected?</th>
</tr>
</thead>
<tbody>
<tr>
<td>02 No</td>
<td>(If “No,” skip to 12, page 7.)</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>369 $</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Mil.</th>
<th>Thou.</th>
<th>Dol.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>1) Downtime of company websites/web servers</th>
<th>366 Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>2) Downtime of servers, routers or switches</td>
<td>367 Hours</td>
</tr>
<tr>
<td>3) Downtime of individual PCs/workstations</td>
<td>368 Hours</td>
</tr>
</tbody>
</table>

i. How many of the incidents in 11a resulted in recovery costs or other monetary losses and costs reported above?

<table>
<thead>
<tr>
<th>371 Number</th>
</tr>
</thead>
</table>
IV. SPECIFIC INCIDENT INFORMATION

For Questions 12–15, please report for the single most significant computer security incident for this company in 2001. If there were multiple similar incidents, choose ONE representative incident.

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

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

- Local area network (LAN)
- Wide area network (WAN)
- Process control network (PCN)
- Virtual private network (VPN)
- Electronic Data Interchange (EDI)
- Wireless network (e.g., 802.11)
- E-mail system
- Internet
- Intranet

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

- Hard-wired communications lines
- Remote dial-in access
- Access to networks through Internet
- Wireless access to e-mail
- Wireless access to Internet
- Wireless access to this company’s other networks
- Publicly accessible website WITHOUT e-commerce capabilities
- Publicly accessible website WITH e-commerce capabilities
- Other – Specify

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

- Denial of service (to Internet connection or e-mail services)
- Downtime of company websites/web servers
- Downtime of servers, routers or switches
- Downtime of individual PCs/workstations

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

- Include the estimated value of downtime, lost productivity, income from lost sales, labor or fees for legal or investigative work, etc.

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

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

- Local law enforcement
- State law enforcement
- FBI (Federal Bureau of Investigation)
- FedCIRC (Federal Computer Incident Response Center)
- Other government agency – Specify
- ISAC (Information Sharing and Analysis Center)
- CERT® Coordination Center
- None of the above

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

- Negative publicity
- Lower customer/client/investor confidence
- Competitor advantage
- Incident outside jurisdiction of law enforcement
- Reported elsewhere – Specify
- Did not want data/hardware seized as evidence
- Did not know who to contact
- Did not think to report
- Nothing to be gained/nothing worth pursuing
- Other – Specify

15. What was the relationship between the suspected offender and this company at the time of this particular incident? Mark (X) only one.

- Current employee, contractor, temporary worker, etc.
- Former employee, contractor, temporary worker, etc.
- Domestic competitor
- Foreign competitor – Specify country
- Foreign hacker – Specify country
- Hacker (no known association with this company)
- Other – Specify
- Don’t know
V. OTHER TRENDS IN COMPUTER SECURITY

16. In 2001, was the overall number of computer security incidents detected by this company more, less or about the same compared to the number detected in 2000?  
Mark (X) only one.  
01 More  
02 Less  
03 About the same/did not change  
04 Don’t know

17. In 2001, did this company have a separate insurance policy or rider to cover losses due specifically to computer security breaches?  
Mark (X) only one.  
01 Yes  
02 No  
03 Don’t know

18a. In 2001, which of the following types of digital products did this company develop for resale?  Mark (X) all that apply.  
Mark (X) only one.  
01 Software  
02 Music  
03 Motion pictures  
04 Other – Specify  
05 None; company did not produce digital products for resale in 2001 – If “None,” skip to 19a.

b. In 2001, did this company experience any unlicensed use or copying (piracy) of digital products which it developed for resale?  
Mark (X) only one.  
01 Yes  
02 No – (Skip to 19a.)  
03 Don’t know – (Skip to 19a.)

c. What was the estimated revenue lost in 2001 due to this unlicensed use or copying?  
Mark (X) only one.  
505

VI. COMPANY INFORMATION

19a. In 2001, which of the following Internet services, if any, did this company provide?  Mark (X) all that apply.  
Mark (X) only one.  
01 Internet Service Provider (ISP)  
02 Web Search Portal  
03 Internet Publishing  
04 Internet Broadcasting  
05 None of the above – (Skip to 20.)

b. In 2001, which of the following Internet services, if any, was the PRIMARY business activity for this company?  Mark (X) only one.  
Mark (X) only one.  
01 Internet Service Provider (ISP)  
02 Web Search Portal  
03 Internet Publishing  
04 Internet Broadcasting  
05 None of the above – (Skip to 20.)