U.S. Department of Justice
Office of Justice Programs

Revised 10/27/08

Bureau of Justice Statistics
Special Report

September 2008, NCJ 221943

Cybercrime against Businesses, 2005

By Ramona R. Rantala
BJS Statistician

Among 7,818 businesses that responded to the National Computer Security Survey, 67% detected at least one cybercrime in 2005 (table 1). Nearly 60% detected one or more types of cyber attack, 11% detected cyber theft, and 24% of the businesses detected other computer security incidents. Respondents, representing 36 economic industries, said they detected more than 22 million incidents of cybercrime in 2005. The vast majority of cybercrimes (20 million incidents) were other computer security incidents, primarily spyware, adware, phishing, and spoofing. There were nearly 1.5 million computer virus infections and 126,000 cyber fraud incidents.

The effects of these crimes were measured in terms of monetary loss and system downtime. Ninety-one percent of the businesses providing information sustained one or both types of loss. The monetary loss for these businesses totaled $867 million in 2005. Cyber theft accounted for more than half of the loss ($450 million). Cyber attacks cost businesses $314 million. System downtime caused by cyber attacks and other computer security incidents totaled 323,900 hours. Computer viruses accounted for 193,000 hours and other computer security incidents resulted in more than 100,000 hours of system downtime.

Of the businesses responding to the survey, telecommunications businesses (82% of these businesses), computer system design businesses (79%), and manufacturers of durable goods (75%) had the highest prevalence of cybercrime in 2005. Utilities, computer system design businesses, manufacturers of durable goods, and internet service providers detected the highest number of incidents, with a total of more than 10.5 million incidents. Administrative support, finance, and food service businesses incurred the highest monetary loss with a combined total of $325 million, more than a third of the total for all businesses.

Forestry, fishing, and hunting (44% of businesses) and agriculture (51%) had the lowest prevalence of cybercrime in 2005. Agriculture, rental services, and business and technical schools incurred the least monetary loss ($3 million).

Table 1. Prevalence of computer security incidents, types of offenders, and reporting to law enforcement, 2005

Characteristic	Percent of businesses by type of incident: All incidents	Cyber attack	Cyber theft	Other
All businesses responding	67%	58%	11%	24%
Number of employees				
2-24	50%	44%	8%	15%
25-99	59	51	7	17
100-999	70	60	9	24
1,000 or more	82	72	20	36
Industries with the highest prevalence of cybercrime[a]				
Telecommunications	82%	74%	17%	32%
Computer system design	79	72	15	25
Manufacturing, durable goods	75	68	15	32
Suspected offender was an—[b]				
Insider	40%	27%	74%	30%
Outsider	71	74	32	72
Incidents were reported—[c]				
Within the business	80%	81%	46%	69%
To another organization	15	14	9	7
To law enforcement authorities	15	6	56	12

Note: A total of 7,818 businesses responded to the National Computer Security Survey. Detail may sum to more than 100% because businesses could detect multiple types of incidents.

[a]See appendix table 3 for all industries.

[b]Percentages are based on businesses that detected an incident and provided information on suspected offenders.

[c]Percentages are based on businesses that detected an incident and provided information on reporting incidents to authorities.

Detailed information is available in appendix tables in the online version of this report on the BJS Website at <http://www.ojp.usdoj.gov/bjs/pub/pdf/cb05.pdf>.

Insiders (i.e., employees, contractors, or vendors working for the business) were responsible for the cyber thefts against nearly 75% of businesses victimized by cyber theft. Conversely, more than 70% of businesses victimized by cyber attacks or other computer security incidents said the suspected offenders were outsiders (i.e., hackers, competitors, and other non-employees).

Overall, few businesses that detected an incident (15%) reported cybercrimes to official law enforcement agencies. More than 50% of victimized businesses reported cyber thefts to police, while cyber attacks and other computer security incidents were reported to authorities by 6% and 12% of victimized businesses, respectively.

The National Computer Security Survey provides the nation's first large-scale measure of cybercrime

The President's National Strategy to Secure Cyberspace directs the Department of Justice to develop better data about the nature and prevalence of cybercrime and electronic intrusions.[1] Other data collections address cybercrime, but no large-scale (or nationally representative) survey collects sufficient information to accurately measure cybercrime and its consequences or to develop risk factors.

The National Computer Security Survey (NCSS) was developed by the U.S. Department of Justice (DOJ), Office of Justice Programs, Bureau of Justice Statistics in partnership with the U.S. Department of Homeland Security, National Cyber Security Division. The DOJ Computer Crime and Intellectual Property Section, the Computer Intrusion Section of the Federal Bureau of Investigation Cyber Division, and the U.S. Secret Service also collaborated on the project. The survey was also supported by a wide variety of trade associations and industry groups. (A complete list is available online at <http://www.ojp.usdoj.gov/bjs/survey/ncss/ncss.htm>.)

The NCSS documents the nature, prevalence, and impact of cyber intrusions against businesses in the United States. This report examines three general types of cybercrime:

- *Cyber attacks* are crimes in which the computer system is the target. Cyber attacks consist of computer viruses (including worms and Trojan horses), denial of service attacks, and electronic vandalism or sabotage.

- *Cyber theft* comprises crimes in which a computer is used to steal money or other things of value. Cyber theft includes embezzlement, fraud, theft of intellectual property, and theft of personal or financial data.

- *Other computer security incidents* encompass spyware, adware, hacking, phishing, spoofing, pinging, port scanning, and theft of other information, regardless of whether the breach was successful or damage or losses were sustained as a result.

[1]The National Strategy to Secure Cyberspace, February 2003; Recommendation A/R 2-1.

More than 8,000 businesses participated in the survey

The National Computer Security Survey sample was a stratified, random sample of businesses designed to produce national and industry-level estimates. The sample was stratified by industry, risk level, and size of business. Thirty-six industries, as defined by the North American Industrial Classification System (NAICS), were within the scope of the survey. (See appendix table 1 for a full list and definitions of industries, *Methodology* for details of the sample design, and page 11 for a glossary.)

To produce national and industry-level estimates a sample of nearly 36,000 businesses was selected (table 2). Responses were received from more than 8,000 businesses, giving an overall response rate of 23%. Response rates varied by business size, with larger businesses responding at a higher rate. Response rates also varied by industry. Response rates were highest for utility businesses (37%). Telecommunications (16%) had one of the lowest response rates. (See appendix table 2 for response rates for all industries). Though response rates were not sufficient to support national or industry-level estimates, they were the highest of any survey of this kind.

Table 2. Universe, sample, and response, by business size and selected industries, 2005

Characteristics	Number of businesses			Response rate
	Universe	Sample	Response	
All businesses	7,278,109	35,596	8,079	23%
Number of employees				
2 - 24	6,771,026	11,479	2,056	18%
25 - 99	396,355	5,601	1,236	22
100 - 999	98,585	11,472	2,894	25
1,000 or more	12,143	7,044	1,893	27
Risk level[a]				
Critical Infrastructure	1,680,606	11,694	2,719	23%
High	2,074,041	7,564	1,737	23
Moderate	774,494	5,294	1,184	22
Low	2,748,969	11,044	2,439	22
Industries with highest response rate[b]				
Utilities	11,850	906	336	37%
Social services	180,376	967	317	33
Health care	577,499	1,444	423	29
Manufacturing, durable goods	275,319	1,859	503	27
Industries with lowest response rate[b]				
Internet service providers	23,874	776	135	17%
Telecommunications	26,547	821	134	16
Accommodations	60,944	1,006	143	14
Motion picture and sound recording	31,902	642	88	14

[a]Risk level is based on Department of Homeland Security classifications and industry's risk of incidents, monetary loss, or downtime.

[b]See appendix table 2 for all industries.

Computer virus infections were the most prevalent cybercrime among businesses in 2005

Of the 8,000 respondent businesses representing 36 economic industries, more than 7,800 used some type of computer system. Two-thirds of the businesses that used computers detected at least one computer security incident (5,081 businesses) in 2005 (table 3). Nearly three-fifths detected one or more types of cyber attack. A tenth detected a cyber theft. A quarter of the businesses detected other computer security incidents, such as spyware or phishing.

Computer virus infection was the most prevalent type of cyber attack, detected by 52% of responding businesses. Nearly 90% of respondents reported that they were able to stop a virus before it caused an infection (not shown in a table). Of those businesses able to intercept viruses, 40% said they were successful in preventing all virus infections.

Cyber fraud was the most common type of cyber theft, having been detected by 5% of the businesses responding to the survey (table 3).

Of the businesses detecting theft of intellectual property, 70% indicated at least one incident involving the theft of trade secrets (table 4). For victims of theft of personal or financial data, names and dates of birth were taken from 60% of businesses. More than 75% of the businesses detecting other computer security incidents indicated that some type of malware (primarily adware) was installed, and 58% of victims discovered spyware or keystroke logging applications. Slightly more than 50% of the businesses detecting other computer security incidents were victims of corporate identity theft in the form of phishing or spoofing.

Prevalence of cybercrime varied by industry and risk level. In 2005, telecommunications businesses (82% of these businesses), computer system design businesses (79%), and manufacturers of durable goods (75%) had the highest prevalence of cybercrime (appendix table 3.) These three industries also showed the highest prevalence of cyber attacks. Finance (33% of businesses) and Internet service providers (21%) had the highest proportion of businesses detecting cyber theft. About a third of responding telecommunications businesses, manufacturers of durable goods, and architecture and engineering businesses detected other computer security incidents.

Forestry, fishing, and hunting (44% of businesses) and agriculture (51%) had the lowest prevalence of cybercrime in 2005. Forestry, fishing, and hunting also had the lowest proportion of businesses detecting cyber theft (3%), followed by warehousing (4%) and social services (5%).

Table 3. Prevalence of computer security incidents among businesses, by type of incident, 2005

Type of incident	All businesses*	Businesses detecting incidents	
		Number	Percent
All incidents	7,636	5,081	67%
Cyber attack	7,626	4,398	58%
Computer virus	7,538	3,937	52
Denial of service	7,517	1,215	16
Vandalism or sabotage	7,500	350	5
Cyber theft	7,561	839	11%
Embezzlement	7,492	251	3
Fraud	7,488	364	5
Theft of intellectual property	7,492	227	3
Theft of personal or financial data	7,476	249	3
Other computer security incidents	7,492	1,792	24%

Note: Number of businesses and detail may sum to more than total because respondents could answer questions about more than one type of incident. See appendix table 3 for prevalence, by industry.

*Based on businesses that indicated whether they detected an incident.

Table 4. Detailed characteristics of selected types of computer security incidents, by type, 2005

Incident characteristic	Percent of businesses
Intellectual property	
Trade secrets	70%
Copyrighted material	47
Patented material	14
Trademarks	8
Number of businesses*	**198**
Personal or financial information	
Names or dates of birth	60%
Social security numbers	49
Credit card numbers	34
Account or PIN numbers	27
Debit or ATM card numbers	14
Other	21
Number of businesses*	**235**
Other computer security incidents	
Adware or other malware	77%
Spyware, keystroke logging	58
Phishing or spoofing	53
Scanning, pinging or sniffing	33
Hacking	16
Theft of other information	3
Other	8
Number of businesses*	**1,762**

Note: Detail may sum to more than 100% because respondents could provide more than one type.

*Based on businesses that detected an incident and provided detailed characteristics.

86% of victimized businesses detected multiple incidents

The majority of victimized businesses (86%) detected multiple incidents, with half of these (43%) detecting 10 or more incidents during the year (table 5). However, the percentage of businesses detecting multiple incidents varied by type of incident. For victims of computer viruses, denial of service attacks, fraud, and other computer security incidents, the majority of victims detected multiple incidents. Conversely, fewer than half of the victims of vandalism or sabotage, embezzlement, theft of intellectual property, or theft of personal or financial data detected multiple incidents.

91% of businesses detecting cybercrime incurred losses

The effects of cybercrime were measured in terms of monetary loss and system downtime. During testing of the survey instrument, many businesses indicated that they had no reliable way to estimate the costs associated with system downtime. The businesses cited various reasons for difficulty in estimating the cost: employees were able to work offline, customers could return after systems were restored, and there was no method for measuring lost sales. For these reasons, the NCSS asked only for duration of downtime rather than a dollar loss equivalent.

Ninety-one percent of the businesses that detected incidents and answered questions on loss sustained one or both types of loss. Forty-one percent of businesses sustained both monetary loss and system downtime.

Type of loss	Percent of businesses*
No loss	9%
Any loss	91%
Monetary loss only	38
Downtime only	12
Both	41

*Based on 4,083 businesses answering at least one question on monetary loss or downtime.

Of the 3,591 businesses that detected incidents and responded to monetary loss questions, 3,247 (90%) incurred monetary loss from the computer security incidents (table 6). The amount of monetary loss depended on the type of incident. Approximately 68% of the victims of cyber theft sustained monetary loss of $10,000 or more. By comparison, 34% of the businesses detecting cyber attacks and 31% of businesses detecting other computer security incidents lost more than $10,000. The other computer security incidents category had the highest proportion of businesses experiencing some form of cybercrime but incurring no monetary loss (20%).

Table 5. Number of computer security incidents, by type of incident, 2005

Type of incident	Number of businesses	Percent of businesses that detected incidents			
		Total	1 incident	2 - 9 incidents	10 or more incidents
All incidents	4,439	100%	14	43	43
Cyber attack	3,841	100%	17	53	30
Computer virus	3,404	100%	18	54	28
Denial of service	1,024	100%	26	52	23
Vandalism or sabotage	264	100%	57	34	8
Cyber theft	681	100%	47	33	20
Embezzlement	185	100%	64	24	12
Fraud	289	100%	39	29	32
Theft of intellectual property	183	100%	62	34	4
Theft of personal or financial data	193	100%	51	32	17
Other computer security incidents	1,400	100%	10	24	66

Note: Number of businesses may sum to more than total because respondents could detect more than one type of incident. Detail may not sum to 100% due to rounding. See appendix table 4 for number of incidents, by industry.

Table 6. Monetary loss incurred from computer security incidents, by type of incident, 2005

Type of incident	Number of businesses	Percent of businesses with monetary loss				
		Total	No loss	$1,000-$9,000	$10,000-$99,000	$100,000 or more
All incidents	3,591	100%	10	51	27	13
Cyber attack	3,072	100%	9	57	25	9
Computer virus	2,779	100%	7	60	24	9
Denial of service	697	100%	19	52	23	6
Vandalism or sabotage	220	100%	11	59	21	9
Cyber theft	542	100%	6	26	38	30
Embezzlement	160	100%	4	19	44	33
Fraud	237	100%	7	32	36	24
Theft of intellectual property	133	100%	9	17	36	38
Theft of personal or financial data	141	100%	11	31	29	29
Other computer security incidents	1,165	100%	20	49	25	7

Note: Number of businesses may sum to more than total because respondents could detect more than one type of incident. Detail may not sum to 100% due to rounding. See appendix table 5 for monetary loss, by industry.

There was no downtime for a tenth of the businesses detecting cyber attacks or other computer security incidents (table 7). System downtime lasted between 1 and 24 hours for half of the businesses and more than 24 hours for a third of businesses detecting these types of incidents.

The duration of system downtime varied by type of incident. Denial of service attacks noticeably affected the computer systems of 92% of victims. By comparison, incidents of vandalism or sabotage shut systems down for 73% of businesses, and other computer security incidents caused system downtime for 68% of victimized businesses.

Cybercrime resulted in monetary loss of $867 million among businesses responding to the survey

Nearly 4,500 businesses provided information on 22 million cybercrime incidents in 2005 (table 8). The 3,247 businesses that incurred monetary loss from cybercrime lost a total of $867 million. About 2,000 businesses said their business networks, PCs, or web sites (or combinations of the three) were down for a total of 324,000 hours.

Cyber attacks accounted for nearly 1.6 million incidents, more than $300 million in loss, and 220,000 hours of system downtime. Computer viruses accounted for about 90% each of: cyber attack incidents (1.5 million incidents), monetary loss ($281 million), and system downtime (193,000 hours).

Cyber theft accounted for less than 1% of all incidents but more than 50% of the total monetary loss ($450 million). Theft of intellectual property had the fewest number of incidents (607), and the greatest amount of monetary loss of all types of cyber theft (nearly $160 million). Embezzlement also cost businesses nearly $160 million. System downtime data were not collected for cyber theft.

Although 24% of businesses detected other computer security incidents, these other incidents accounted for 92% of the total number of incidents, or 20 million incidents. Other computer security incidents accounted for 12% of all monetary loss ($103 million) and 32% of system downtime (104,000 hours).

Two-thirds of computer security incidents were targeted against critical infrastructure businesses

The number of incidents varied by risk level and industry. Ninety-five percent of victimized scientific research and development businesses detected multiple incidents (appendix table 4). By comparison, fewer than 80% of victimized businesses operating in management of companies; forestry, fishing, and hunting; or other services detected more than one incident.

Table 7. System downtime caused by computer security incidents, by type of incident, 2005

Type of incident	Number of businesses	Percent of businesses with system downtime				
		Total	None	1 - 4 hours	5 - 24 hours	25 hours or longer
All incidents	2,412	100%	11	20	33	36
Cyber attack	2,150	100%	8	24	36	32
Computer virus	1,952	100%	9	24	37	30
Denial of service	505	100%	8	36	37	19
Vandalism or sabotage	160	100%	27	24	27	22
Other computer security incidents	817	100%	32	11	25	32

Note: Number of businesses may sum to more than total because respondents could detect more than one type of incident. See appendix table 6 for system downtime by industry.

Table 8. Number of computer security incidents and amount of monetary loss and system downtime, by type of incident, 2005

Type of incident	Number of incidents		Monetary loss (in thousands)		Downtime	
	Total	Median	Total	Median	Total	Median
All incidents	22,138,250	6	$866,600	$6	323,900 hrs	16 hrs
Cyber attack	1,582,913	4	$313,900	$5	219,600 hrs	12 hrs
Computer virus	1,460,242	3	280,700	5	193,000	12
Denial of service	121,652	3	21,100	5	19,200	7
Vandalism or sabotage	1,019	1	12,200	5	7,300	10
Cyber theft	130,970	2	$450,000	$29		
Embezzlement	1,565	1	158,700	50		
Fraud	125,510	3	103,100	20		
Theft of intellectual property	607	1	159,400	43		
Theft of personal or financial data	3,288	1	28,800	20		
Other computer security incidents	20,424,367	20	$102,700	$5	104,300 hrs	23 hrs
Number of businesses	4,433		3,247		2,157	

Note: Downtime information was not collected for incidents of cyber theft. For specific types of incidents, data were suppressed to ensure confidentiality and accuracy. For number of incidents, six responses were excluded; for monetary loss, six responses were excluded; and for system downtime, three responses were excluded.

Critical infrastructure businesses detected 13 million incidents (nearly two-thirds of the total). High risk industries detected more than 4 million incidents (a fifth of the total).

Risk level	Number of incidents
All businesses	22,138,250
Critical infrastructure	13,039,900
High risk	4,133,800
Moderate risk	1,979,400
Low risk	2,985,100

Utilities, computer system design businesses, durable goods manufacturers, and internet service providers detected the most incidents. Businesses in these four industries detected more than 10.5 million incidents in 2005 (not shown in a table). Forestry, fishing, and hunting; food service; and rental service businesses detected the lowest number of incidents. Combined, these 3 industries detected fewer than 10,000 incidents.

Computer system design businesses (98%) incurred monetary loss more frequently than any other industry (appendix table 5). In 2005 computer security incidents resulted in losses of $10,000 or greater for more than half of the finance businesses, manufacturers of durable goods, insurance businesses, and mining businesses.

Critical infrastructure ($288 million) and low-risk businesses ($298 million) sustained the greatest monetary loss from cybercrime in 2005.

Risk level	Monetary loss (in thousands)
All businesses	$866,600
Critical infrastructure	$287,600
High risk	205,100
Moderate risk	76,100
Low risk	297,800

Specifically, administrative support, finance, and food service businesses incurred the greatest monetary loss with a combined total of $325 million, more than a third of the total for all businesses (not shown in a table). Agriculture businesses, rental services, and business and technical schools incurred the least monetary loss with a combined loss of $3 million.

More than half of the manufacturers of durable goods (56%) sustained system downtime of 25 hours or longer (appendix table 6). By comparison, more than a third of legal services and accounting businesses had a total of 1 to 4 hours of system downtime. Critical infrastructure industries suffered 152,200 hours of system downtime (nearly half of the total). Health care businesses reported the greatest duration of system downtime (34,800 hours). Accounting; forestry, fishing, and hunting; and warehousing had the least downtime—a total of 2,500 hours, with fewer than 1,000 hours each.

Insiders were involved in cyber theft for 74% of businesses in 2005

A third of the victimized businesses indicated that they were unable to determine what affiliation any computer security offenders had with the business (table 9). The type of incident for which businesses had the least information about the offender was denial of service (50% of businesses). Conversely, some offender information was known by the majority of victims of theft of intellectual property, (94% of businesses) and embezzlement (93%).

Table 9. Businesses with no information about computer security offenders, by type of incident, 2005

Type of incident	Businesses	
	Number	Percent*
All incidents	4,875	35%
Cyber attack	4,204	41%
Computer virus	3,778	43
Denial of service	1,104	50
Vandalism or sabotage	314	23
Cyber theft	800	10%
Embezzlement	228	7
Fraud	349	15
Theft of intellectual property	216	6
Theft of personal or financial data	236	20
Other computer security incidents	1,709	40%

*Represents businesses detecting the given type of incident and providing "don't know" as the only response to the offender question.

Table 10. Suspected computer security offenders' affiliation with business, by type of incident, 2005

Type of incident	Number of businesses	Percent of businesses for which the suspected offender was an—		
		Insider	Outsider	Other
All incidents	3,182	40%	71%	11%
Cyber attack	2,480	27%	74%	10%
Computer virus	2,151	25	75	6
Denial of service	547	19	67	18
Vandalism or sabotage	243	42	56	6
Cyber theft	720	74%	32%	8%
Embezzlement	212	93	7	#
Fraud	298	52	50	9
Theft of intellectual property	202	84	20	5
Theft of personal or financial data	188	68	32	7
Other computer security incidents	1,030	30%	72%	8%

Note: Number of businesses may sum to more than total because respondents could detect more than 1 type of incident. Detail may sum to more than 100% because respondents could provide multiple suspected offender classifications. See appendix table 7 for suspected offenders, by industry.

Percentage was suppressed to avoid disclosing information about individual businesses.

In 2005 someone from outside the business, such as a hacker or competitor, was responsible for at least one computer security incident against 71% of the businesses that were able to make a determination about the suspected offender (table 10). For cyber attacks and other computer security incidents, nearly 75% of businesses said the suspected offender was an outsider. By comparison, the majority of businesses detecting cyber theft reported that the suspected offender was an insider (employee, contractor, or vendor working for the business). For embezzelment, more than 90% of businesses said the suspected offender was an insider, which is to be expected due to the nature of the crime. For thefts of intellectual property, nearly 85% of businesses said an insider was involved.

Motion picture and sound recording businesses (87% of victimized businesses) had the highest percentage of outside offenders (see apppendix table 7). By comparison, arts and entertainment businesses had the lowest (55%). Retail (54%), finance (50%), and utility businesses (50%) showed the highest percentage of inside offenders. Petroleum businesses (24%), architecture and engineering businesses (25), and business and technical schools (26%) had the lowest. Computer system design businesses had the second highest prevalence of outside offenders (84% of victimized businesses) and one of the lowest prevalence rates of inside offenders (29%).

Most businesses did not report cyber attacks to law enforcement authorities

When a computer security incident was detected, businesses responded in a variety of ways. The majority of businesses (87%) reported the incident to some person or organization (table 11). Eighty percent of responding businesses reported incidents to someone within their business. Fifteen percent of respondents reported incidents to another organization, such as their computer security contractor or internet service provider. Fifteen percent of victimized businesses reported incidents to law enforcement. Law enforcement includes federal, state and local law enforcement agencies, and official organizations affiliated with law enforcement such as InfraGard (an organization that works with the Federal Bureau of Investigation), the United States Secret Service (USSS) sponsored Electronic Crimes Task Forces, USSS Cyber Investigative Section (CIS), and CERT CC (an organization that works with the Department of Homeland Security).

Reporting of incidents to law enforcement authorities varied by the type of incident. The majority of businesses reported embezzlement (72%), fraud (63%), and theft of personal or financial data (60%). Few businesses reported theft of intellectual property (27%), any type of cyber attack (6%), or other computer security incidents (12%) to law enforcement officials.

Among businesses not reporting incidents to law enforcement authorities, the majority (86%) indicated that incidents were reported elsewhere (within the business or to an organization such as their security contractor) rather than to law enforcement (table 12). Half of the businesses responded that they thought there was nothing to be gained by reporting an incident to law enforcement. Other businesses said they did not think to report the incident (22%), did not know who to contact (11%), or thought the incident was outside the jurisdiction of law enforcement authorities (7%).

Table 11. Organizations to which computer security incidents were reported, by type of incident, 2005

Type of incident	Number of businesses	Percent of businesses reporting incidents— Total	Within business	To another organization	To law enforcement
All incidents	2,714	87%	80%	15%	15%
Cyber attack	2,353	86%	81%	14%	6%
Computer virus	2,150	87	83	13	5
Denial of service	579	70	57	18	6
Vandalism or sabotage	177	76	60	11	14
Cyber theft	424	92%	46%	9%	56%
Embezzlement	136	96	27	5	72
Fraud	176	91	38	13	63
Theft of intellectual property	109	88	67	4	27
Theft of personal or financial data	127	85	33	9	60
Other computer security incidents	952	78%	69%	7%	12%

Note: Number of businesses may sum to more than total because respondents could detect more than one type of incident. Detail may sum to more than 100% because businesses could report to more than one place.

Table 12. Reasons businesses did not report incidents to law enforcement authorities, by type of incident, 2005

Reason for not reporting	Type of incident All	Cyber attack	Cyber theft	Other
Reported elsewhere	86%	87%	78%	77%
Within business	83	84	72	75
To another organization	16	15	14	8
Nothing to be gained	50	47	28	55
Did not think to report	22	22	4	17
Did not know who to contact	11	11	3	9
Outside jurisdiction of law enforcement	7	6	10	7
Negative publicity or decreased confidence	3	2	8	1
Other reason	11	9	18	9
Number of businesses	2,606	2,285	272	874

Note: Number of businesses may sum to more than total because respondents could detect more than one type of incident. Detail may sum to more than 100% because respondents could provide more than one reason.

Few businesses (3%) indicated that their decision not to report an incident to law enforcement was based on the possibility of negative publicity or decreased confidence in the business.

Three-fifths of the businesses detecting cyber attacks reported that the Internet was involved

One critical aspect of computer security is determining which networks were accessed in an incident. (*Accessed networks* include networks that were breached, used to get into another part of the computer system, or affected by the incident—for instance, networks vandalized or on which malware was surreptitiously installed.) NCSS data identify which systems tended to be targeted. Nearly 1,600 businesses that detected incidents also provided information on the systems the business used and which ones were accessed during an incident.

A majority of the businesses detected at least one incident involving the Internet and/or a local area network (LAN) (table 13). The Internet was the most prevalent vehicle or target of cyber attacks (64% of businesses), while cyber thieves tended to access a business's LAN (57% of businesses). For victims of other computer security incidents, half of the businesses reported the Internet, half reported their LAN, and more than a quarter said their wide area network (WAN) was accessed.

Other networks were accessed to a lesser extent. Intranet or Extranet connections were accessed during computer breaches for 17% of respondents, stand-alone workstations (15%), other networks such as virtual private networks (12%) and wireless connections (8%) were also accessed (not shown in a table).

Another critical aspect of computer security is determining whether laptops not owned by the business posed more of a security threat than business-owned laptops. Nearly a third of the businesses said a business-owned laptop was involved in at least one computer security incident. Business-owned laptops were cited less frequently as having been used in cyber attacks (10% of businesses) or cyber thefts (20%) than in other computer security incidents (38%). In comparison, 8% of the businesses reported non-business laptops were used in a cyber attack, 7% in a cyber theft, and 16% in an other computer security incident (not shown in a table).

Of the 4,000 businesses detecting a virus infection, 51% provided information on how viruses were introduced into their computer systems. E-mail attachments were the most commonly cited vehicle (77% of businesses) for introducing computer virus infections (table 14).

Small businesses (83%) were somewhat more vulnerable to virus-laden e-mails than large businesses (72%). Conversely, large businesses (37%) were more vulnerable to portable media such as CDs or thumb drives as a source of virus infections, compared to small businesses (14%). This difference might be explained by a greater tendency of larger businesses to use portable media.

Internet downloads were the second most prevalent source of computer virus infections. Sixty-one percent of businesses detected virus infections from Internet downloads. This percent did not vary by business size.

Table 13. Networks most frequently accessed in computer security incidents, by type of incident, 2005

	Percent of businesses for which accessed system or network was—				
Type of incident	Total	Internet	Local area network	Wide area network	Business laptop
All incidents	100%	56%	55%	31%	30%
Cyber attack[a]	42	64	46	33	10
Cyber theft	24	39	57	26	20
Other	57	50	53	28	38
Number of businesses[b]	1,586	1,509	1,545	1,191	1,424

Note: Detail may sum to more than 100% because incidents could involve multiple networks.

[a]Includes incidents of denial of service and vandalism or sabotage only.

[b]Based on businesses that detected an incident and used the given system.

Table 14. Sources of computer viruses, by business size, 2005

		Percent of businesses for which source of virus was—			
Number of employees	Number of businesses	E-mail attachment	Internet download	Portable media	Other
All businesses	1,995	77%	61%	27%	18%
25 - 99	301	83	61	14	13
100 - 999	1,012	80	62	24	15
1,000 or more	682	72	60	37	25

Note: Detail may sum to more than 100% because respondents could provide more than one virus source. Businesses with fewer than 25 employees were not asked about virus sources.

Insufficient anti-virus software was the most prevalent vulnerability

Overall, 62% of the businesses using anti-virus software said the software was inadequate in preventing incidents (table 15). Nearly half of the businesses using anti-spyware or anti-adware said the software did not prevent an incident. Internal controls (31% of businesses), e-mail logs and filters (27%), and firewalls (26%) were also commonly cited as insufficient.

Security insufficiencies differed depending on the type of incident. The most prevalent security deficiencies were anti-virus software for cyber attacks (66% of businesses), misuse of authorized access for cyber theft (46%), and anti-spyware and anti-adware for other computer security incidents (62%).

Other security measures appeared to be more successful in preventing incidents. Biometrics (5% of businesses), digital certificates (5%), password generators (6%), and encryption (7%) were least frequently cited as the mechanisms that were inadequate to prevent incidents (not shown in a table).

Businesses that outsourced all or part of their computer security had a greater prevalence of incidents

Businesses that outsourced all or part of their computer security had a higher prevalence of cybercrime compared to businesses that performed all security in-house.

Sixty-four percent of businesses that outsourced at least one security measure detected one or more cyber attacks in 2005 (table 16). By comparison, 55% of businesses that kept all security functions in-house detected a cyber attack that same year.

The security measure that showed the greatest difference in prevalence of attacks between outsourcing and in-house was physical security. Businesses that outsourced physical security had the highest prevalence of cyber attacks (73%), compared to businesses that managed their own physical security (60%). Several security measures showed little or no difference between the businesses that outsourced computer security and those that kept it in-house. These include business continuity plans and formal audit standards. Two security measures showed a slightly lower prevalence of cyber attacks when outsourced: network watch centers and configuration management.

Table 15. Most frequent computer security vulnerabilities, by type of incident, 2005

Inadequate security measure	Type of incident: All incidents	Cyber attack	Cyber theft	Other
Anti-virus software	62%	66%	10%	38%
Anti-spyware/anti-adware	47	36	10	62
Internal controls	31	28	29	24
E-mail logs and filters	27	24	10	27
Firewall	26	25	9	22
Personnel policy	24	19	34	22
Misuse of authorized access	18	11	46	15
Number of businesses*	4,525	3,899	718	1,544

Note: Number of businesses may sum to more than total because businesses could detect more than one type of incident. Detail may sum to more than 100% because respondents could provide multiple vulnerabilities.
*Represents the number of businesses that detected incidents and provided information on security inadequacies.

Table 16. Detection of cyber attacks, by whether security was in-house or outsourced, 2005

Type of security practice	In-house security: Number of businesses	In-house security: Percent detecting cyber attack	Outsourced security[a]: Number of businesses	Outsourced security[a]: Percent detecting cyber attack
Total	3,194	55%	3,416	64%
Physical security	1,482	60	331	73
Equipment decommissioning	876	63	397	70
Other[b]	141	34	232	69
Personnel policy	1,305	60	337	68
Network watch center	369	71	654	68
Periodic audits	961	62	834	67
Vulnerability/risk assessment	733	62	962	67
Intrusion testing	552	63	1,249	66
Identification of critical assets	1,109	62	195	65
Formal audit standards	316	64	310	65
Disaster recovery plan	1,971	59	894	64
Corporate security policy	1,733	61	189	63
Regular review of systems/logs	1,190	59	497	62
Configuration management	843	64	606	62
Employee training	1,056	59	298	62
Business continuity plan	1,200	60	458	60

Note: Number of businesses may sum to more than total and detail may sum to more than 100% because respondents could provide more than one type of security practice.
[a] Security practices may have been partially or completely outsourced.
[b] Includes limiting system access, practices designed to comply with the Sarbanes-Oxley Act of 2002, and automatic patch management.

Methodology

Sample design

The National Computer Security Survey sample was a stratified, random sample of businesses designed to produce national and industry-level estimates. The sample was stratified by industry, risk level, and size of business. Thirty-six industries, as determined by the North American Industrial Classification System (NAICS), were within the scope of the survey. (See appendix table 1 for a complete list and definition of industries.) Risk level comprised four groups: critical infrastructure, high risk, moderate risk, and low risk. Critical infrastructure consisted of businesses operating in the industries with which the Department of Homeland Security formed Information Sharing and Analysis Centers (ISACs). Each of the remaining businesses was designated as high, moderate, or low risk depending on its industry of operation's risk of incidents, loss, and downtime. Business size was determined by the number of employees and was divided into nine size categories. The sampling frame, Dunn and Bradstreet, contained records for nearly 7.3 million in-scope businesses. Businesses without employees on their payroll—such as family owned and operated businesses—were out of scope.

Sampling was done at the enterprise level, except in cases of businesses with large subsidiaries operating in different economic sectors. To preserve the ability to provide industry-level findings, these businesses were sampled at the highest level of subsidiary with distinct lines of business.

A sample of 35,596 businesses was drawn to produce national and industry-level estimates and to track changes of more than 2.5% over time. (See appendix table 2 for a summary of the sample by risk level and industry.) Businesses with more than 5,000 employees and Fortune 500 businesses were drawn with certainty to ensure the representation of all industries. Because some industries typically do not have large businesses, the largest 50 businesses were also included with certainty. Due to the particular importance of the nation's critical infrastructure, businesses in these strata were over-sampled. High risk industries such as manufacturing, retail, and wholesale were also over-sampled.

Tables

Denominators reflect the number of businesses that responded to the questions relevant to a given table. For example, in table 5 the denominator represents the number of businesses that responded to questions on networks used by the business, whether computer security incidents were detected, and networks that were affected in those incidents (if any). Unless otherwise noted, missing items or responses of “don’t know” have been omitted. Totals and medians are based on positive responses and exclude zeroes.

Incident percentages are based on 7,636 businesses that had a computer and responded to at least 1 incident question; 7,626 businesses responded to at least 1 question on cyber attacks, 7,561 to at least 1 question on cyber theft, and 7,492 to at least 1 question on other computer security incidents.

For theft of intellectual property, 29% of 198 businesses provided multiple types; for personal or financial data, 60% of 235 businesses specified more than 1 type; and for other computer security incidents, 59% of 1,762 businesses identified multiple types.

Missing and excluded data

Of the 8,079 businesses providing information on whether or not they had computer systems, 14 businesses reported contradictory information. Because the responses from these 14 businesses could not be reconciled, they were excluded from all analyses.

Each table underwent a detailed disclosure analysis to ensure the confidentiality of responses given by individual businesses. As a result, some responses were excluded from totals and medians. Table 8 and appendix table 6 were affected. Six responses were excluded from the number of computer security incidents; six responses were excluded from monetary loss; and three responses were excluded from system downtime. The disclosure analysis also resulted in the suppression of values for some cells in table 10, appendix table 6, and appendix table 7.

Definitions of computer security incidents

Computer virus—a hidden fragment of computer code which propagates by inserting itself into or modifying other programs. Includes viruses, worms, and Trojan horses. Excludes spyware, adware, and other malware.

Denial of service—the disruption, degradation, or exhaustion 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, or excessive amounts of incoming data.

Electronic vandalism or sabotage—the deliberate or malicious damage, defacement, destruction or other alteration of electronic files, data, web pages, or programs.

Embezzlement—the unlawful misappropriation of money or other things of value, by the person to whom the property was entrusted (typically an employee), for his or her own purpose. Includes 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, or various services by the person to whom they were entrusted.

Fraud—the intentional misrepresentation of information or identity to deceive others, the unlawful use of a credit or 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 business. Includes instances in which a computer was used to defraud the business of money, property, financial documents, insurance policies, deeds, use of rental cars, or various services by forgery, misrepresented identity, credit card or wire fraud. Excludes incidents of embezzlement.

Theft of intellectual property—the illegal obtaining of copyrighted or patented material, trade secrets, or trademarks (including designs, plans, blueprints, codes, computer programs, software, formulas, recipes, graphics) usually by electronic copying. Excludes theft of personal or financial data such as credit card or social security numbers, names and dates of birth, financial account information, or any other type of information.

Theft of personal or financial data—the illegal obtaining of information that potentially allows someone to use or create accounts under another name (individual, business, or some other entity). Personal information includes names, dates of birth, social security numbers, or other personal information. Financial information includes credit, debit, or ATM card account or PIN numbers. Excludes theft of intellectual property such as copyrights, patents, trade secrets, and trademarks. Excludes theft of any other type of information.

Other computer security incidents—Incidents that do not fit within the definitions of the specific types of cyber attacks and cyber theft. Encompasses spyware, adware, hacking, phishing, spoofing, pinging, port scanning, sniffing, and theft of other information, regardless of whether damage or losses were sustained as a result.

Definitions of other terms

Business—a company, service or membership organization consisting of one or more establishments under common ownership or control. For this survey, major subsidiaries were treated as separate businesses.

CERT C.C.—an organization that works with the U.S. Computer Emergency Readiness Team (CERT) and the private sector. CERT C.C. studies computer and network security in order to provide incident response services to victims of attacks, publish alerts concerning vulnerabilities and threats, and offer information to help improve computer and network security.

DHS National Cyber Security Division (NCSD)—works cooperatively with public, private, and international entities to secure cyberspace and America's cyber assets. Its strategic objectives are to build and maintain an effective national cyberspace response system and to implement a cyber-risk management program for protection of critical infrastructure.

DOJ Computer Crime and Intellectual Property Section (CCIPS)—is responsible for implementing the Department's national strategies in combating computer and intellectual property crimes worldwide. The Computer Crime Initiative is a comprehensive program designed to combat electronic penetrations, data thefts, and cyber attacks on critical information systems.

FBI Cyber Division, Computer Intrusion Section—addresses computer intrusions, which often have international facets and national economic implications. The Cyber Division as a whole simultaneously supports FBI priorities across program lines, assisting counterterrorism, counterintelligence and other criminal investigations when aggressive technological investigative assistance is required.

Information Sharing and Analysis Centers (ISACs)—organizations that work with the U.S. Government, law enforcement agencies, technology providers, and security associations such as U.S. CERT. ISACs maintain secure databases, analytic tools and information gathering and distribution facilities designed to allow authorized individuals to submit reports about information security threats, vulnerabilities, incidents and solutions.

InfraGard—an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a partnership between the Federal Bureau of Investigation and the private sector.

Subsidiary—a company in which another business has more than 50% ownership or the power to direct or cause the direction of management and policies.

U.S. CERT—The United States Computer Emergency Readiness Team is a partnership between the Department of Homeland Security and the public and private sectors. Established in 2003 to protect the nation's Internet infrastructure, U.S. CERT coordinates defense against and responses to cyber attacks across the nation.

United States Secret Service (USSS)—Originally founded to suppress the counterfeiting of U.S. currency, the USSS now investigates many financial crimes. The USSS has established working partnerships in both the law enforcement and business communities to address such cybercrime issues as protecting the critical infrastructure, Internet intrusions, and associated fraud. These partnerships include the *Electronic Crimes Task Forces* and the *Cyber Investigative Section.*

U.S. Department of Justice
Office of Justice Programs
Bureau of Justice Statistics

Washington, DC 20531

Official Business
Penalty for Private Use $300

NCJ 221943

PRESORTED STANDARD
POSTAGE & FEES PAID
DOJ/BJS
Permit No. G-91

Revised 10/27/08

The Bureau of Justice Statistics is the statistical agency of the U.S. Department of Justice. Michael D. Sinclair is acting director.

This Special Report was written by Ramona R. Rantala, BJS Statistician. Mark Motivans verified the statistical information. Elizabeth Billheimer and Bethany Allen assisted with verification.

Ramona R. Rantala was project manager for the National Computer Security Survey. RAND Corporation staff, under a cooperative agreement and in collaboration with BJS, designed the sample, updated the questionnaire, and collected the data: Lois M. Davis, Principal Investigator; Daniela Golinelli, Statistician; Robin Beckman, Research Programmer; Sarah Cotton, Survey Director; Robert Anderson, Co-Principal Investigator; Anil Bamezai, Policy Researcher; Christopher Corey, Survey Technical Support Manager; Megan Zander-Cotugno, Survey Coordinator; and John Adams, Senior Statistician. Joseph Garrett, Senior Vice President, and Julie Young, Research Director of Market Research, Inc., designed and monitored the web-based data collection instrument.

Catherine Bird and Tina L. Dorsey edited and produced the report. Jayne E. Robinson prepared the report for final printing.

September 2008, NCJ 221943

This report in portable document format and in ASCII and its related statistical data and tables are available at the BJS World Wide Web Internet site: <http://www.ojp.usdoj.gov/bjs/abstract/cb05.htm>

Office of Justice Programs

Innovation • Partnerships • Safer Neighborhoods
http://www.ojp.usdoj.gov

Appendix table 1. North American Industrial Classification System (NAICS) codes used in sample design, 2005

Risk level and industry	NAICS code* Sector	Sub-sector or Industry group	Description
Critical Infrastructure			
Agriculture	11	111	Crop production (farms, orchards, groves, nurseries)
		112	Animal production (ranches, farms, feedlots)
Chemical and drug manufacturing	32	325	Basic chemicals, resins and plastics, agricultural chemicals, pharmaceuticals and medicines, paint and adhesives, cleaning compounds, explosives, other chemicals
Computer system design	54	5415	Computer system design, custom programming, facilities management, and other related computer services
Finance	52	521	Central banks
		522	Commercial banks, savings and credit institutions, credit cards, loan brokers
		523	Securities, commodity contracts, other financial investments, and related activities
Health Care	62	621	Ambulatory health care services (physicians, dentists, other health care, outpatient care, substance abuse, diagnostic laboratories, and home health care)
		622	Hospitals (medical, surgical, psychiatric, substance abuse, other specialty treatment hospitals)
		623	Residential nursing, mental health, substance abuse, elderly, and retirement care facilities
Internet service providers	51	518	Internet service providers, web search portals, data processing and related services
Petroleum mining and manufacturing	21	211	Oil and gas extraction
	32	32411	Petroleum refineries
Publications and broadcasting	51	511	Publishing (except Internet)
		515	Broadcasting (except Internet)
		516	Internet publishing and broadcasting
		519	Other information services including news syndicates, libraries and archives
Real estate	53	531	Lessors, agents and brokers, and related activities
Telecommunications	51	517	Wired and wireless carriers and resellers, satellite telecommunications, cable and other program distributors, other telecommunications
Transportation/pipelines	48		Air, rail, water, trucking, transit and ground passenger transportation, pipelines, sight-seeing, support activities
	49	492	Couriers and messengers
Utilities	22		Electric power generation, transmission, and distribution; natural gas distribution; water, sewage, and other systems
High			
Manufacturing, durable goods	32	321	Wood products (lumber, plywood, mill work)
		327	Non-metallic mineral products (clay, glass, cement)
	33	331	Primary metals (foundries, smelting, refining, rolling, drawing, extruding, and alloying)
		332	Fabricated metal products
		333	Machinery
		334	Computers and electronics
		335	Electrical equipment, appliances, and components
		336	Transportation equipment (motor vehicles, aircraft, railroad rolling stock, ships and boats)
		337	Furniture, cabinets, and fixtures
		338	Miscellaneous products such as medical equipment, jewelry, sporting goods, and toys
Manufacturing, non-durable goods	31		Food products, beverage and tobacco products, textiles, apparel, leather and leather products
	32	322	Paper
		323	Printing and support activities
		32412	Asphalt
		32419	Other non-fuel petroleum products and coal products
		326	Plastics and rubber products
Motion picture and sound recording	51	512	Motion picture, video, and sound recording production, distribution, and related activities

Appendix table 1. North American Industrial Classification System (NAICS) codes used in sample design, 2005 (continued)

Risk level and industry	NAICS code* Sector	Sub-sector or Industry group	Description
High (continued)			
Retail	44		Motor vehicles and parts, furniture and home furnishings, electronics and appliances, building materials, garden equipment and supplies, food and beverages, health and personal care, gasoline stations, clothing and accessories
	45		Sporting goods, hobby, books and music; general merchandise; miscellaneous stores, such as florists and office supplies; non-store retailers including online retailers, mail-order, vending machines, and direct selling establishments
Scientific research and development	54	5416	Management, scientific, and technical consulting services
		5417	Research and development in the physical, engineering, life, and social sciences
Wholesale	42		Merchant wholesalers, durable goods; merchant wholesalers, non-durable goods
Moderate			
Accounting	54	5412	Accounting, tax preparation, bookkeeping, and payroll services
Advertising	54	5418	Advertising, public relations, media representatives, display, direct mail, distribution
		5419	Other professional and scientific services such as market research
Architecture and engineering	54	5413	Architectural and engineering services
		5414	Specialized design services such as interior, industrial, and graphic design
Business and technical schools	61	6114	Business schools and computer and management training
		6115	Technical and trade schools
		6116	Other schools and instruction including fine arts, sports, language, and driving
		6117	Educational support services
Insurance	52	524	Insurance carriers and related activities
		525	Funds, trusts, and other financial vehicles
Legal services	54	5411	Lawyers, notaries, title abstract and settlement, other legal services
Low			
Accommodations	72	721	Traveler accommodation, recreational parks, campgrounds, and vacation camps, rooming and boarding houses
Administrative support	56		Administrative and support services, waste management and remediation services
Arts and entertainment	71		Performing arts, spectator sports, and related industries; museums, historical sites, and similar institutions; amusement, gambling, and recreation industries
Construction	23		Construction of buildings, heavy and civil engineering construction, specialty trade contractors
Food services	72	722	Full-services restaurants, cafeterias, caterers, and drinking establishments
Forestry, fishing, and hunting	11	113	Forestry and logging
		114	Fishing, hunting and trapping
		115	Support activities for agriculture, forestry, fishing, and hunting
Management of businesses	55		Banks and other holding companies and corporate, subsidiary, and regional managing offices
Mining	21	212	Coal, metal ore, and non-metallic mineral mining
		213	Support activities for mining
Other services	81	811	Repair and maintenance services
		812	Personal and laundry services
		813	Religious, grantmaking, civic, professional, and similar organizations
Rental services	53	532	Rental and leasing of goods such as automobiles, appliances, videos, industrial machinery
		533	Lessors of non-financial intangible assets, except copyrighted works
Social services	62	624	Social assistance such as family, temporary shelter, vocational rehabilitation, and child day care services
Warehousing and storage	49	493	General, refrigerated, farm product, and other storage and warehousing

* Some sectors were divided for sampling purposes. The sub-sector and industry group codes provided above show these divisions.

Appendix table 2. National Computer Security Survey universe, sample, and response, by risk level and industry, 2005

Risk level and industry	Number of businesses			Response rate
	Universe	Sample	Response	
All businesses	7,278,109	35,596	8,079	23%
Critical Infrastructure	1,680,606	11,694	2,719	23%
Agriculture	179,442	740	175	24
Chemical and drug manufacturing	15,998	1,052	201	19
Computer system design	80,289	932	170	18
Finance	187,044	1,275	323	25
Health care	577,499	1,444	423	29
Internet service providers	23,874	776	135	17
Petroleum mining and manufacturing	5,247	567	126	22
Publications and broadcasting	63,758	1,086	218	20
Real estate	352,625	949	175	18
Telecommunications	26,547	821	134	16
Transportation/pipelines	156,433	1,146	303	26
Utilities	11,850	906	336	37
High	2,074,041	7,564	1,737	23%
Manufacturing, durable goods	275,319	1,859	503	27
Manufacturing, non-durable goods	127,248	1,371	327	24
Motion picture and sound recording	31,902	642	88	14
Retail	1,005,175	1,418	316	22
Scientific research and development	185,571	1,053	219	21
Wholesale	448,825	1,221	284	23
Moderate	774,494	5,294	1,184	22%
Accounting	96,023	675	176	26
Advertising	121,116	876	154	18
Architecture and engineering	131,291	897	214	24
Business and technical schools	51,275	756	190	25
Insurance	174,108	1,243	269	22
Legal services	200,680	847	181	21
Low	2,748,969	11,044	2,439	22%
Accommodations	60,944	1,006	143	14
Administrative support	355,532	1,297	255	20
Arts and entertainment	145,913	957	198	21
Construction	692,084	1,103	241	22
Food services	277,281	1,129	212	19
Forestry, fishing, and hunting	29,132	632	152	24
Management of companies	12,960	722	168	23
Mining	15,082	795	190	24
Other services	897,994	1,039	272	26
Rental services	62,970	793	159	20
Social services	180,376	967	317	33
Warehousing	18,701	604	132	22

Appendix table 3. Use of computers and prevalence of computer security incidents, by risk level and industry, 2005

Risk level and industry	Respondents		All incidents		Cyber attack		Cyber theft		Other	
	Number of businesses	Percent with computers	Number of businesses	Percent detecting incident	Number of businesses	Percent detecting incident	Number of businesses	Percent detecting incident	Number of businesses	Percent detecting incident
All businesses	8,079	97%	7,636	67%	7,626	58%	7,561	11%	7,492	24%
Critical Infrastructure	2,719	98%	2,610	67%	2,605	58%	2,580	14%	2,557	25%
Agriculture	175	82	142	51	141	40	142	6	142	17
Chemical and drug manufacturing	201	98	192	73	192	66	190	12	188	27
Computer system design	170	100	167	79	167	72	165	15	165	25
Finance	323	100	317	67	317	49	316	33	311	25
Health care	423	100	410	67	409	59	404	11	400	24
Internet service providers	135	100	132	66	132	60	132	21	131	24
Petroleum mining and manufacturing	126	98	124	56	122	52	123	7	123	26
Publications and broadcasting	218	100	212	71	212	65	206	14	205	25
Real estate	175	97	167	65	167	56	164	9	163	25
Telecommunications	134	100	130	82	130	74	127	17	126	32
Transportation/pipelines	303	98	294	64	294	54	291	10	287	22
Utilities	336	98	323	64	322	53	320	8	316	26
High	1,737	97%	1,656	71%	1,655	62%	1,639	12%	1,622	28%
Manufacturing, durable goods	503	97	479	75	479	68	473	15	469	32
Manufacturing, non-durable goods	327	99	319	72	319	61	317	9	314	28
Motion picture and sound recording	88	99	84	67	84	63	84	13	81	19
Retail	316	94	293	67	293	58	289	12	288	24
Scientific research and development	219	99	210	70	210	61	206	8	204	26
Wholesale	284	98	271	67	270	59	270	13	266	27
Moderate	1,184	99%	1,140	67%	1,140	57%	1,127	9%	1,116	24%
Accounting	176	100	173	55	173	47	170	6	168	18
Advertising	154	99	149	67	149	56	148	10	148	26
Architecture and engineering	214	97	204	70	204	60	201	7	200	31
Business and technical schools	190	95	177	72	177	64	173	8	171	18
Insurance	269	100	263	69	263	57	262	15	258	25
Legal services	181	99	174	69	174	55	173	6	171	27
Low	2,439	94%	2,230	63%	2,226	55%	2,215	8%	2,197	20%
Accommodations	143	96	134	60	134	56	133	14	133	16
Administrative support	255	98	239	65	239	55	238	11	234	25
Arts and entertainment	198	96	181	62	181	54	179	9	176	18
Construction	241	97	223	70	223	61	223	7	222	23
Food services	212	88	186	54	185	48	184	9	183	15
Forestry, fishing, and hunting	152	88	131	44	131	40	129	3	128	16
Management of companies	190	93	150	59	150	51	150	12	150	19
Mining	272	94	170	65	169	58	168	7	167	20
Other services	159	97	249	68	249	59	248	8	245	22
Rental services	317	96	151	64	150	59	150	7	148	18
Social services	132	92	299	66	298	57	296	5	294	24
Warehousing	168	90	117	60	117	53	117	4	117	16

Note: Incident detail may sum to more than 100% because businesses could detect multiple types of incidents. Incident percentages are based on businesses with computers responding to questions on incidents.

Appendix table 4. Number of computer security incidents, by risk level and industry, 2005

Risk level and industry	Number of businesses		Percent of businesses that detected incidents			
	Detecting incidents	Providing number of incidents	Total	1 incident	2 - 9 incidents	10 or more incidents
All businesses	5,081	4,439	100%	14	43	43
Critical Infrastructure	1,747	1,518	100%	14	40	46
Agriculture	72	61	100%	18	41	41
Chemical and drug manufacturing	140	122	100%	12	52	36
Computer system design	132	122	100%	9	48	43
Finance	211	176	100%	15	36	48
Health care	274	247	100%	15	40	45
Internet service providers	87	76	100%	16	38	46
Petroleum mining and manufacturing	70	63	100%	17	38	44
Publications and broadcasting	151	135	100%	10	37	53
Real estate	108	94	100%	15	35	50
Telecommunications	107	93	100%	11	44	45
Transportation/pipelines	187	163	100%	14	39	47
Utilities	208	166	100%	15	40	45
High	1,172	1,031	100%	10	43	47
Manufacturing, durable goods	360	313	100%	9	41	50
Manufacturing, non-durable goods	230	197	100%	15	45	41
Motion picture and sound recording	56	52	100%	15	38	46
Retail	197	177	100%	12	43	45
Scientific research and development	147	131	100%	5	47	47
Wholesale	182	161	100%	7	44	48
Moderate	768	671	100%	15	46	39
Accounting	95	80	100%	15	44	41
Advertising	100	88	100%	14	48	39
Architecture and engineering	143	127	100%	8	48	44
Business and technical schools	128	114	100%	18	49	33
Insurance	182	151	100%	19	43	38
Legal services	120	111	100%	15	43	41
Low	1,394	1,219	100%	15	45	40
Accommodations	81	73	100%	16	42	41
Administrative support	156	130	100%	15	37	48
Arts and entertainment	112	96	100%	17	44	40
Construction	155	132	100%	15	49	36
Food services	101	92	100%	14	55	30
Forestry, fishing, and hunting	58	48	100%	21	48	31
Management of companies	110	93	100%	22	43	35
Mining	169	149	100%	17	44	38
Other services	96	87	100%	21	48	31
Rental services	197	174	100%	8	44	48
Social services	70	64	100%	14	50	36
Warehousing	89	81	100%	10	42	48

Note: Detail may not sum to 100% due to rounding.

Appendix table 5. Monetary loss incurred from computer security incidents, by risk level and industry, 2005

Risk level and industry	Number of businesses	Percent of businesses with monetary loss				
		Total	No loss	$1,000-$9,000	$10,000-$99,000	$100,000 or more
All businesses	3,591	100%	10%	51	27	13
Critical Infrastructure	1,248	100%	8%	49	29	14
Agriculture	48	100	10%	71	15	4
Chemical and drug manufacturing	83	100	10%	46	27	18
Computer system design	99	100	2%	51	34	13
Finance	153	100	7%	35	29	29
Health care	199	100	9%	49	28	14
Internet service providers	72	100	8%	44	28	19
Petroleum mining and manufacturing	52	100	12%	50	27	12
Publications and broadcasting	104	100	9%	51	27	13
Real estate	81	100	6%	57	31	6
Telecommunications	82	100	9%	41	38	12
Transportation/pipelines	142	100	9%	52	27	11
Utilities	133	100	11%	56	27	7
High	855	100%	9%	46	29	16
Manufacturing, durable goods	274	100	9%	36	34	21
Manufacturing, non-durable goods	159	100	11%	50	28	11
Motion picture and sound recording	42	100	12%	55	21	12
Retail	141	100	6%	51	25	18
Scientific research and development	101	100	7%	55	26	12
Wholesale	138	100	8%	49	27	17
Moderate	521	100%	9%	55	25	12
Accounting	62	100	10%	58	19	13
Advertising	66	100	12%	50	26	12
Architecture and engineering	104	100	10%	52	28	11
Business and technical schools	82	100	12%	67	16	5
Insurance	122	100	4%	44	32	20
Legal services	85	100	9%	61	22	7
Low	967	100%	12%	56	23	8
Accommodations	54	100	7%	48	33	11
Administrative support	106	100	12%	48	26	13
Arts and entertainment	70	100	19%	60	11	10
Construction	106	100	8%	59	25	8
Food services	71	100	13%	59	17	11
Forestry, fishing, and hunting	38	100	13%	68	11	8
Management of companies	66	100	18%	41	33	8
Mining	72	100	15%	33	40	11
Other services	114	100	14%	60	19	7
Rental services	71	100	10%	61	27	3
Social services	151	100	12%	64	21	3
Warehousing	48	100	4%	75	15	6

Note: Detail may not sum to 100% due to rounding.

Appendix table 6. System downtime caused by computer security incidents, by risk level and industry, 2005

Risk level and industry	Number of businesses	Downtime (in hours)*		Percent of businesses with downtime			
		Total	Median	Total	1 - 4 hours	5 - 24 hours	25 hours or longer
All businesses	2,158	323,900 hrs	16 hrs	100%	23	37	40
Critical Infrastructure	708	152,200 hrs	15 hrs	100%	23	37	40
Agriculture	26	1,200	11	100%	31	23	46
Chemical and drug manufacturing	48	2,600	17	100%	25	42	33
Computer system design	61	8,500	16	100%	21	38	41
Finance	76	11,900	12	100%	24	38	38
Health care	137	34,800	15	100%	18	43	39
Internet service providers	33	#	14	100%	27	36	36
Petroleum mining and manufacturing	23	1,300	10	100%	26	43	30
Publications and broadcasting	53	5,600	20	100%	26	26	47
Real estate	46	#	20	100%	22	39	39
Telecommunications	47	4,600	20	100%	19	34	47
Transportation/pipelines	82	#	14	100%	24	35	40
Utilities	76	#	12	100%	26	37	37
High	511	75,000hrs	22hrs	100%	19	35	46
Manufacturing, durable goods	162	26,900	32	100%	14	31	56
Manufacturing, non-durable goods	95	15,400	12	100%	26	37	37
Motion picture and sound recording	24	1,600	21	100%	21	38	42
Retail	83	8,700	22	100%	24	34	42
Scientific research and development	70	5,000	20	100%	23	34	43
Wholesale	77	17,600	20	100%	13	43	44
Moderate	312	39,500hrs	12hrs	100%	27	36	38
Accounting	35	700	9	100%	34	37	29
Advertising	39	1,200	10	100%	18	56	26
Architecture and engineering	60	10,300	11	100%	18	42	40
Business and technical schools	55	3,200	24	100%	29	25	45
Insurance	75	20,100	13	100%	27	32	41
Legal services	48	3,900	11	100%	38	27	35
Low	627	57,200hrs	15hrs	100%	23	40	37
Accommodations	39	3,700	24	100%	18	36	46
Administrative support	69	#	16	100%	22	41	38
Arts and entertainment	49	2,600	16	100%	22	41	37
Construction	59	3,400	12	100%	31	29	41
Food services	48	2,400	11	100%	29	38	33
Forestry, fishing, and hunting	16	900	21	100%	19	31	50
Management of companies	40	1,800	14	100%	20	45	35
Mining	49	#	11	100%	22	45	33
Other services	91	15,700	10	100%	26	44	30
Rental services	43	1,600	12	100%	21	49	30
Social services	99	8,100	20	100%	20	33	46
Warehousing	25	900	16	100%	16	48	36

Note: 254 businesses sustained no downtime. These were excluded to avoid disclosing information about individual businesses. The percentage of businesses sustaining no downtime varied by industry and ranged from 4% to 18%. Downtime information was not collected for incidents of cyber theft. Detail may not sum to 100% due to rounding.

*Total and median downtime hours exclude three outliers and the values of some cells are suppressed (#) to avoid disclosing information about individual businesses.

Appendix table 7. Suspected offenders' affiliation with business, by risk level and industry, 2005

Risk level and industry	Number of businesses	Percent of businesses for which the suspected offender was an— Insider	Outsider	Other
All businesses	3,182	40%	71%	11%
Critical Infrastructure	1,144	42%	70%	11%
Agriculture	41	17	78	7
Chemical and drug manufacturing	90	44	72	11
Computer system design	91	29	84	7
Finance	152	50	72	15
Health care	179	49	63	14
Internet service providers	64	44	80	8
Petroleum mining and manufacturing	42	24	81	17
Publications and broadcasting	91	36	81	10
Real estate	70	44	59	11
Telecommunications	73	37	68	12
Transportation/pipelines	111	41	68	11
Utilities	140	50	61	9
High	738	43%	74%	9%
Manufacturing, durable goods	233	48	75	9
Manufacturing, non-durable goods	151	36	75	9
Motion picture and sound recording	30	40	87	13
Retail	113	54	66	11
Scientific research and development	97	31	72	14
Wholesale	114	44	78	4
Moderate	477	32%	74%	15%
Accounting	53	32	75	8
Advertising	57	30	75	9
Architecture and engineering	99	25	80	12
Business and technical schools	66	26	70	21
Insurance	132	41	73	22
Legal services	70	31	71	13
Low	823	38%	69%	10%
Accommodations	50	46	70	#
Administrative support	94	43	62	11
Arts and entertainment	58	43	55	17
Construction	95	37	78	3
Food services	56	45	64	9
Forestry, fishing, and hunting	26	27	65	23
Management of companies	68	43	65	9
Mining	105	30	75	8
Other services	59	37	68	15
Rental services	117	37	74	9
Social services	40	30	65	10
Warehousing	55	29	73	18

Note: Detail may sum to more than 100% because respondents could provide multiple offender classifications. Of the 4,875 businesses responding to questions on offenders for at least one type of incident, 35% were unable to provide any offender classifications. Total percentages are based on the businesses that provided at least 1 offender classification.

Cell value suppressed to avoid disclosing information about individual businesses.