U.S. Department of Justice
Office of Justice Programs

Bureau of Justice Statistics
Technical Report

March 2004, NCJ 200639

Pilot test results, 2001 Computer Security Survey

Cybercrime against Businesses

Ramona R. Rantala
BJS Statistician

Among 198 businesses responding to a 2001 pilot survey, 74% reported being a victim of cybercrime. Other findings on the 198 businesses included the following: nearly two-thirds had been victimized by a computer virus at least once; a quarter had experienced denial of service attacks, such as the degradation of Internet connections due to excessive amounts of incoming information; about a fifth reported that their computer systems had been vandalized or sabotaged.

These are some of the findings from the Computer Security Survey (CSS) 2001 pilot, which covered a group of 500 businesses nationwide. These findings are not nationally representative but illustrate the feasibility and utility of a data collection program to be initiated in 2004 among some 36,000 businesses.

The Bureau of Justice Statistics (BJS), collaborating with the U.S. Census Bureau, conducted the CSS pilot. Results of this test demonstrated a need for an increased response rate to produce valid national estimates and a need to refine survey questions.

Various estimates exist on cybercrime against businesses, but when implemented, CSS will provide the first official national statistics on the extent and consequences of cybercrime against the Nation's 5.3 million businesses.[1]

[1]This figure excludes farms and businesses owned and operated by only one person.

Highlights

CSS pilot test data for 2001 showed that —

- Of the 500 sampled companies, 42% responded.
- 95% of responding companies used computers.
- 99% of companies with computers reported whether they detected incidents of cybercrime.
- Nearly 75% of companies with computers detected at least one incident.
- Of all companies detecting incidents, 91% had 100 or more employees.
- 68% of companies detecting incidents reported losses totaling $61 million.
- 83% of companies detecting computer attacks or other computer security incidents reported having 1 or more hours of downtime.
- Fewer than 5% of companies detecting computer attacks said the offender was a company employee.
- Of companies detecting computer attacks, 12% or fewer reported incidents to law enforcement authorities.
- 94% percent or more companies answered each core question on computer infrastructure and security practices.
- More than 97% of checks on returned questionnaires passed completeness and consistency edits.

Response time varied by company size —

- Companies with fewer than 100 employees typically spent less than 1 hour to complete the survey.
- Those with 1,000 or more employees took 2¾ hours on average to complete the survey.
- The overall average completion time was 1¾ hours.

Pilot test development included —

- external consultations with Federal entities such as the National Security Council, businesses, trade associations, and academia
- pre-testing questionnaire on 69 companies representing 14 industries
- pilot sample of 500 companies, covering 11% of employment and 16% of payroll nationwide.

118 companies provided reasons for not participating —

- 82% reported that their company did not participate in voluntary surveys of any kind.
- 17% were concerned about confidentiality of reported data.
- 14% said data were not available.

Note: Respondents could provide more than one reason.

Data collection and unit response

The CSS pilot sample was 500 companies, drawn from 5.3 million. Nearly half of the 500 were selected from the largest companies in each industry; the remainder were randomly selected to represent businesses of all sizes and types (table 1). The sample covered 11% of employment nationwide.

The CSS pilot began as a mail survey. Questionnaire packages contained a cover letter, the survey form, answers to frequently asked questions, and instructions. (The questionnaire is available on the BJS website <http://www.ojp.usdoj.gov/bjs/quest.htm>.) After all follow-ups, the response rate was slightly below 42%.

Response rates varied by industry. For example, 100% of sampled social service companies but fewer than 20% of accounting firms completed the survey.

Response rates also varied by size of company. Response for companies with 1,000 or more employees was 29% compared to 58% for companies with fewer than 1,000 employees.

	Unit response	
Number of employees	Companies in sample	Percent responding*
All companies	500	41.8%
0 to 19	42	66.7
20 to 99	21	52.4
100 to 999	162	56.2
1,000 or more	273	28.6

*Excludes 2 out-of-scope companies.

Table 1. CSS pilot sample and response, by risk level and industry, 2001 pilot survey

	Universe			Sample of companies				Responding companies			
						Percent of industry			Percent	Percent of industry	
Industry and risk level	Companies	Employment	Payroll	Certainty	Non-certainty	Employment	Payroll	Number	of sample	Employment	Payroll
Total	5,321,815	125,009,254	$3,894,185,805	236	264	11%	16%	208	41.8%	2.4%	3.0%
Infrastructure	861,624	27,599,389	$1,246,635,003	114	110	20%	25%	95	42.4%	4.1%	5.0%
Computer systems design	96,380	2,026,164	139,000,366	9	10	22	22	9	47.4	5.0	3.9
Data processing	7,680	283,402	13,493,844	5	10	41	48	9	60.0	40.6	44.0
Finance	96,874	4,054,484	259,867,914	16	10	24	26	10	38.5	6.8	8.2
Health care	436,117	11,864,053	385,770,874	8	11	5	5	8	42.1	0.7	0.7
Internet service providers[a]	9,511	235,040	22,793,314	8	9	8	17	5	29.4	2.7	2.8
Chemical/drug manufacturing	7,468	729,285	40,418,563	6	10	30	36	8	50.0	5.1	5.1
Petroleum mining/manufacturing	7,244	323,150	19,896,637	6	10	54	57	7	43.8	5.1	5.1
Publications/broadcasting	25,041	1,605,955	85,575,608	12	10	29	32	10	45.5	9.4	9.9
Telecommunications	17,908	1,783,094	94,804,904	10	10	57	60	6	30.0	1.2	1.5
Transportation/pipelines	150,517	3,921,743	136,965,714	17	10	35	39	10	37.0	7.9	8.5
Utilities	6,878	747,278	46,103,807	11	10	22	25	10	47.6	3.7	3.8
Internet publishers[b]	6	25,741	1,943,458	6	0	100	100	3	50.0	19.4	16.6
High risk	1,493,966	53,282,923	$1,445,978,585	46	40	10%	14%	34	40.0%	2.7%	2.5%
Manufacturing —											
Durable goods	157,913	10,595,209	496,812,912	16	8	17	23	9	37.5	0.8	1.0
Non-durable goods	129,878	7,517,600	278,832,838	11	8	8	12	5	26.3	1.5	1.7
Retail	724,146	27,969,852	339,997,859	9	8	9	14	11	64.7	4.3	7.2
Scientific research/development	135,524	1,379,367	86,881,998	5	8	8	10	4	30.8	0.2	0.2
Wholesale[c]	346,505	5,820,895	243,452,978	5	8	2	2	5	41.7	0.9	1.0
Medium risk	485,563	5,708,733	$229,840,589	25	34	11%	12%	24	40.7%	2.3%	2.8%
Advertising	36,143	475,670	23,918,750	5	7	20	23	3	25.0	1.0	0.8
Architecture/engineering	112,472	1,297,403	67,737,370	5	7	9	11	4	33.3	1.8	3.4
Education	40,647	516,263	14,518,581	5	7	23	34	6	50.0	10.6	17.2
Insurance	127,911	2,332,706	111,473,623	5	7	12	13	5	41.7	1.9	2.4
Legal services	168,390	1,086,691	62,192,265	5	6	1	2	6	54.5	0.5	0.8
News syndication libraries[a]	0	0	0								
Low risk	2,480,662	38,418,209	$921,731,628	51	80	7%	7%	55	42.3%	1.1%	1.5%
Accommodations	48,938	1,900,602	39,567,184	5	6	20	26	6	54.5	6.4	8.5
Accounting[c]	93,397	1,696,001	43,277,194	5	6	37	33	<3	<20.0	<1.0	<1.0
Administrative support	229,806	8,377,834	193,989,040	5	6	7	7	3	27.0	0.7	1.6
Agricultural services	356	38,479	986,465	0	5	23	19	3	60.0	0.3	0.5
Arts and entertainment	96,078	1,689,091	42,028,973	3	6	4	3	<3	<30.0	<1.0	<1.0
Construction	699,322	6,546,276	237,796,683	5	6	1	2	7	63.6	0.4	0.6
Food services	361,876	8,328,685	99,553,143	5	6	7	9	4	36.4	<0.1	<0.1
Management of companies	6,643	155,299	8,058,153	0	5	4	3	<3	<45.0	<1.0	<1.0
Mining	11,954	437,516	19,734,792	5	6	26	28	5	45.5	6.6	5.4
Motion pictures	18,204	291,094	10,406,741	5	5	13	27	<3	<30.0	<1.0	<3.0
Other services	464,636	3,487,808	81,386,138	5	5	3	3	4	40.0	1.5	1.4
Real estate/rental services	241,201	1,910,247	59,248,186	5	6	5	7	5	45.5	1.8	2.3
Social services	94,077	1,990,068	32,628,376	1	6	1	1	7	100.0	1.0	0.8
Warehousing	4,183	147,572	4,552,374	2	6	15	18	4	50.0	3.8	4.2
Unclassified (out of scope)	109,991	1,421,637	48,518,186	0	0						

Note: Exact frequencies or percentages are not used in some cells (<>) to avoid disclosing information about individual companies.
[a]Includes news syndicates in 2001. Distinct North American Industrial Classification System (NAICS) codes to occur with 2002 Economic Census.
[b]Can identify only industry leaders in 2001. NAICS codes to be assigned in 2002 Economic Census.
[c]One company was found to be out of scope and is excluded from response rates.

Cybercrime incidents

Nearly three-fourths (147 companies) of businesses detected at least 1 computer security incident in 2001 (table 2). Computer viruses were most common (64%), followed by denial of service attacks (25%) and vandalism or sabotage (19%).

Larger companies detected incidents most often. Of the 147 companies detecting incidents, 91% had 100 or more employees (table 3). At least 7 in 10 companies detecting incidents of cybertheft had 1,000 or more employees.

At least 92% of companies detecting incidents reported the number of incidents detected (table 4). More than half of the victims of computer virus, denial of service, and fraud detected multiple incidents in 2001.

"Other" computer security incidents

Description	Companies reporting other computer security incidents: Number	Percent
All other incidents	26	100%
Hacking	8	31
Spam	5	19
Spoofing, sniffing, or port scanning	5	19
Other	4	15
Unspecified	6	23

Note: Respondents could provide descriptions of more than one type.

Most companies detecting "other" computer security incidents described what took place. Hacking, or gaining unauthorized access to computers, was the most common response supplied by respondents (31%). Spam — frequent, unwanted e-mail advertisements — was the second most common (19%). Spoofing (gaining unauthorized access through a message using an IP address apparently from a trusted host), sniffing (monitoring data traveling over a network), and port scanning (looking for open "doors" into a computer) together constituted 19% of incidents.

Table 2. Detection of cybercrime incidents, by type of incident, 2001 pilot survey

Type of incident	Companies that had computers: Number	Percent, that — Total	Detected incidents	Did not detect incidents	Missing*
Total	198	100%	74.2%	24.2%	1.5%
Theft					
Embezzlement	198	100%	4.0%	92.4%	3.5%
Fraud	198	100	8.6	86.4	5.1
Theft of proprietary	198	100	6.1	88.9	5.1
Computer attack					
Denial of service	198	100%	25.3%	71.2%	3.5%
Vandalism or sabotage	198	100	18.7	74.2	7.1
Computer virus	198	100	64.1	29.3	6.6
Other	198	100%	13.1%	81.3%	5.6%

Note: Detail may not add to total because of rounding. Ten companies that did not have computer systems were omitted.
*The total represents those companies that did not respond to any of the questions on detection of cybercrime.

Table 3. Detection of cybercrime incidents, by type of incident and company size, 2001 pilot survey

Type of incident	Companies that detected an incident: Number	Percent, by number of employees: Total	0 to 99	100 to 999	1,000 or more
Total	147	100%	8.8%	44.2%	46.9%
Theft					
Embezzlement	8	100%	--	--	75.0%
Fraud	17	100	0	29.4	70.6
Theft of proprietary information	12	100	0	< 30.0	> 70.0
Computer attack					
Denial of service	50	100%	12.0%	36.0%	52.0%
Vandalism or sabotage	37	100	8.1	45.9	45.9
Computer virus	127	100	7.1	43.3	49.6
Other	26	100%	11.5%	23.1%	65.4%

Note: Exact percentages are not used in some cells (<>) and are withheld from other cells (--) to avoid disclosing information about individual companies. Detail may not add to total because of rounding.

Table 4. Frequency of cybercrime incidents, by type of incident, 2001 pilot survey

Type of incident	Companies that detected an incident: Number	Percent, with — Total	One incident	More than one incident	Missing
Total	147	100%	8.2%	89.1%	2.7%
Theft					
Embezzlement	8	100%	75.0%	--	--
Fraud	17	100	41.2	52.9	5.9
Theft of proprietary information	12	100	50.0	41.7	8.3
Computer attack					
Denial of service	50	100%	34.0%	64.0%	2.0%
Vandalism or sabotage	37	100	51.4	48.6	0
Computer virus	127	100	7.9	86.6	5.5
Other	26	100%	34.6%	57.7%	7.7%

Note: Percentages are withheld from some cells (--) to avoid disclosing information about individual companies.

Table 5. Whether the suspected offender was an employee, by type of incident, 2001 pilot survey

Type of incident	Companies that detected an incident				
		Percent, with the offender as —			
	Number	Total	Employee	Non-employee	Missing or unknown
Total	147	100%	14.3%	56.5%	29.3%
Theft					
Embezzlement	8	100	87.5	--	--
Fraud	17	100	52.9	29.4	17.6
Theft of proprietary information	12	100	66.7	--	--
Computer attack					
Denial of service	50	100	6.0	82.0	12.0
Vandalism or sabotage	37	100	0	83.8	16.2
Computer virus	127	100	1.6	72.4	26.0
Other	26	100	26.9	53.8	19.2

Note: Percentages are withheld from some cells (--) to avoid disclosing information about individual companies. Detail may not add to total because of rounding.

Table 6. Losses from cybercrime, by type of incident, 2001 pilot survey

Type of incident and loss	Companies that detected an incident					
		Percent, by monetary loss				Total losses in 2001 (in $ millions)
	Number	Total	$1,000 or more	No loss	Missing	
Total	147	100%	68.0%	11.6%	20.4%	$61.0
Theft						
Embezzlement						
Value of things taken	8	100	87.5%	--	--	$2.0
Other monetary losses	8	100	50.0	--	--	0.1
Fraud						
Value of things taken	17	100	64.7	--	--	18.1
Other monetary losses	17	100	23.5	41.2	35.3	--
Theft of proprietary information						
Value of things taken	12	100	--	--	58.3	0.5
Other monetary losses	12	100	--	--	66.7	--
Computer attack						
Denial of service						
Recovery cost	50	100	70.0%	8.0%	22.0%	$7.4
Other monetary losses	50	100	38.0	30.0	32.0	7.0
Vandalism or sabotage						
Recovery cost	37	100	59.5	13.5	27.0	1.1
Other monetary losses	37	100	32.4	24.3	43.2	1.1
Computer virus						
Recovery cost	127	100	60.6	6.3	33.1	9.8
Other monetary losses	127	100	29.9	22.8	47.2	12.0
Other						
Recovery cost	26	100	46.2%	15.4%	38.5%	$0.6
Other monetary losses	26	100	30.8	23.1	46.2	0.3

Note: Some companies that initially refused to participate agreed to complete a shortened CSS form. Computer security expenditures questions were not included on this form. These 17 companies are tabulated as missing. Percentages or dollar values are withheld from some cells (--) to avoid disclosing information about individual companies. Detail may not add to total because of rounding.

Reporting to law enforcement

Type of incident	Percent of companies reporting incidents to law enforcement		
	Reported	Did not report	Missing
Theft			
Embezzlement	87.5%	--	--
Fraud	47.1	29.4%	23.5%
Theft of proprietary information	16.7	58.3	25.0
Computer attack			
Denial of service	12.0	72.0	16.0
Vandalism or sabotage	10.8	62.2	27.0
Computer virus	5.5	66.9	27.6
Other	23.1	50.0	26.9

Note: Percentages are withheld from some cells (--) to avoid disclosing information about individual companies.

Reporting incidents to law enforcement varied by type of incident. Seven in eight companies detecting embezzlement reported it to authorities, and about 5 in 10 reported fraud. More than half of companies detecting computer attacks or thefts of proprietary information indicated they did not contact law enforcement.

Employee offenders

For at least one type of incident, 7 out of 10 companies indicated whether or not suspected offenders were employees (table 5). Suspected offenders were employees for more than 50% of companies detecting cybertheft, but fewer than 6% of computer attack victims said employees were responsible.

Monetary losses

Reporting of monetary losses varied by type of incident. Nearly 90% of companies detecting embezzlement reported the amount of loss (table 6). Of those detecting denial of service, 7 in 10 companies estimated recovery costs. Among the responding companies, there was a reported total of $61 million in losses and recovery costs for 2001. Computer viruses accounted for losses of nearly $22 million, fraud more than $18 million, and denial of service $14 million.

Computer downtime

Response to questions on downtime varied by both type of computer attack and type of downtime. Of companies detecting denial of service, 90% reported that incidents lasted 1 hour or longer (table 7). For computer viruses, two-thirds of victims reported their PC's were down for at least an hour. Of those detecting vandalism or sabotage, 57% reported website downtime of 1 hour or more.

Table 7. Type and length of downtime by offense for companies detecting computer attacks or "other" computer security incidents, 2001 pilot survey

	Companies that detected an incident other than cybertheft				
		Percent, by length of downtime			
Type of downtime	Number	Total	1 hour or longer	No downtime	Missing
Total	145	100%	82.8%	2.1%	15.2%
Computer attack					
Denial of service	50	100	90.0	0	10.0
Vandalism or sabotage					
Downtime of websites	37	100	56.8	21.6	21.6
Downtime of servers	37	100	45.9	32.4	21.6
Downtime of PC's	37	100	45.9	32.4	21.6
Computer virus					
Downtime of servers	127	100	44.9	25.2	29.9
Downtime of PC's	127	100	67.7	10.2	22.0
Other					
Downtime of websites	26	100	19.2	38.5	42.3
Downtime of servers	26	100	26.9	30.8	42.3
Downtime of PC's	26	100	19.2	30.8	50.0

Note: Some companies that initially refused to participate agreed to complete a shortened CSS form. Downtime questions were not included on this form. These 17 companies are tabulated as missing. Two companies detected cybertheft but had no other incident. Detail may not add to total because of rounding.

Most significant incident

Of the 147 companies detecting incidents, nearly 86% identified 1 incident as most significant. Computer viruses were reported as most significant by 62% of companies.

Most significant incident	Companies identifying most significant incident	
	Number	Percent
Total companies detecting incidents	147	100.0%
Embezzlement or fraud	3	2.0
Denial of service	18	12.2
Vandalism or sabotage	7	4.8
Computer virus	91	61.9
Other	7	4.8
Missing or none	21	14.3

Eighty-eight percent of companies detecting incidents reported having one (35%) or more (53%) affected networks (table 8). Local area networks, individual workstations connected to the LAN, and e-mail were most commonly affected. Seven in ten companies identified how company networks were accessed: By Internet was the most common.

Fourteen percent of companies that detected incidents reported their most significant incident to one or more law enforcement agencies. For those that did not report to authorities, more than half said the incident was not worth pursuing, and 3 in 10 "did not think to report" it (not shown in a table).

More than half of companies could not identify the offender in general terms for their most significant incident. Three in ten classified the offender as a hacker.

Offender	Companies identifying offender in most significant incident	
	Number	Percent
Total	147	100 %
Employee	7	4.8
Hacker	45	30.6
Other	18	12.2
Missing/don't know	77	52.4

Table 8. Characteristics of most significant cybercrime incident, 2001 pilot survey

	Companies that detected an incident						
		Percent with —					
Characteristic	Number	Total	One type	More than one type	None	Not applicable	Missing or don't know
Affected network	147	100%	35.4%	53.1%	0	4.1%	7.5%
Mode of access	147	100	51.7	19.7	6.1	7.5	15.0
Reported to law enforcement	147	100	10.9	2.7	65.3	0	21.1

Note: Some companies that initially refused to participate agreed to complete a shortened CSS form. Questions on reporting to law enforcement were not included on this form. These 17 companies are tabulated as missing. Detail may not add to total because of rounding.

Table 9. Comparing the number of cybercrime incidents in 2000 and 2001, by company size, 2001 pilot survey

	Companies that had computers				
		Percent, by difference in number of incidents, 2000 and 2001			
Number of employees	Number	Total	More incidents in 2001	No change	Missing or don't know
Total	184	100%	45.7%	25.0%	29.3%
0 to 19	18	100	22.2	22.2	55.6
20 to 99	11	100	27.3	45.5	27.3
100 to 999	82	100	43.9	25.6	30.5
1,000 or more	73	100	56.2	21.9	21.9

Note: The 14 companies that indicated fewer incidents in 2001 than in 2000 were omitted to avoid disclosing information on individual companies. Detail may not add to total because of rounding.

Computer security in 2000 and 2001

When asked about the difference in the number of computer security incidents detected in 2001 from the previous year, 56% of companies with 1,000 or more employees said they detected more incidents in 2001 (table 9).

When asked about insurance, 10% of all companies said they had separate policies or riders to cover losses due

Table 10. Computer infrastructure and security characteristics, 2001 pilot survey

Characteristic	Companies participating in the CSS: Number	Percent with — Total	One type	More than one type	None	Missing or don't know
Networks[a]	208	100%	11.1%	79.8%	4.8%	4.3%
Network access	198	100	14.1	72.2	9.1	4.5
Servers, routers, switches	198	100	13.1	79.8	2.5	4.5
Individual PC's/workstations	198	100	3.5	93.9	0	2.5
Computer security technology	198	100	9.1	86.9	<2.0	>2.0
Third party contracting[b]	198	100	15.7	25.8	42.4	16.2
Computer security practices	198	100	13.1	70.2	11.1	5.6
Testing, using, or updating business continuity or disaster recovery programs[c]	135	100	44.4	32.6	19.3	3.7

Note: Exact percentages are not used in some cells (<>) to avoid disclosing information about individual companies.
Detail may not add to total because of rounding.
[a]Of the 208 responding companies, 10 had no computers and are included in response analysis of networks only.
[b]Some companies that initially refused to participate agreed to complete a shortened CSS form. Third party contracting questions were not included on this form. These 17 companies are tabulated as missing.
[c]Some companies had neither a business continuity program nor a disaster recovery plan. These 63 companies are excluded.

Table 11. Expenditures for computer security technology, by company size, 2001 pilot survey

Number of employees	Companies participating in the CSS: Number	Percent spending on computer security — Total	$1,000 or more	No expenditures	Missing
Total	198	100%	73.2%	6.6%	20.2%
0 to 19	19	100	52.6	26.3	21.1
20 to 99	11	100	63.6	18.2	18.2
100 to 999	90	100	73.3	<6.7	>20.0
1,000 or more	78	100	79.5	<7.8	>12.7

Note: Some companies that initially refused to participate agreed to complete a shortened CSS form. Computer security technology expenditures questions were not included on this form. These 17 companies are tabulated as missing. Exact percentages are not used in some cells (<>) to avoid disclosing information about individual companies.

specifically to computer security breaches.

Company has separate insurance policy	Total companies: Number	Percent
Total	198	100 %
Yes	20	10.1
No	92	46.5
Missing/don't know	86	43.4

Response to piracy questions was sparse. Of the 25 companies that developed digital products for resale, 4 reported incidents of piracy, and 1 estimated consequent lost revenue (not shown in a table).

Computer infrastructure and security

Questions on computer infrastructure and security had high response rates. Ninety-one percent of all respondents reported having one (11%) or more than one (80%) type of network (table 10). Nearly 5% indicated they used no computers. Of the 198 companies that used computers, 96% reported using one or more types of computer security technology. Anti-virus software was the most common.

Eighty-three percent of companies using computers reported one (13%) or more (70%) types of computer security practices, such as periodic audits and reviews of system administrative logs. Companies that had business continuity or disaster recovery programs were asked what actions they took in 2001 with those programs — testing, using, or updating. Forty-four percent of 135 companies indicated that they took only one action. Thirty-three percent took two or more actions.

Seventy-three percent of companies reported spending $1,000 or more in 2001 on computer security technology (table 11). Nearly 80% of companies

Table 12. CSS data quality checks, by passing rate, 2001 pilot survey

Edit description	Total checks	Percent of checks passed
Completeness		
Full-year data	198	97.5%
Consistency in reporting		
Networks and access	2,145	98.3%
Cost of computer security technology and reported technology	517	98.1
Contracting of computer security services	172	99.4
Computer security practices	137	100
Number of incidents	936	97.9
Most significant incident	712	99.3
Duplicate reporting		
Cybertheft incidents	55	100 %
Computer attack incidents	537	87.8
Data out of tolerance		
Percent of IT budget spent on computer security <1% or > 50%	157	84.1%
Multiple incidents		
Most significant incident data may represent multiple occurrences	1,055	79.3%

Note: Total checks are derived by multiplying number of questions pertaining to edit by number of companies responding.

with 1,000 or more employees spent at least $1,000.

Pilot test data quality

Preliminary data edits from the pilot test were drafted to evaluate data quality. Tolerance parameters were estimated. Pilot test results will be used to refine data edit parameters for the full-scale survey.

More than 97% of checks on returned questionnaires passed completeness and consistency edits (table 12). These edits indicate full-year data and consistent reporting on comparable items, respectively. For example, a company would fail one consistency edit if it reported that its local area network (LAN) was affected by the most significant incident, but did not report having a LAN in the questionnaire section on computer infrastructure.

Fewer cases (88%) passed edits on duplicate reporting for computer attacks. This duplication illustrates overlap in denial of service, vandalism or sabotage, and computer virus.[2] Because the former two can be caused by viruses, some respondents reported these incidents under all applicable categories.

Recommendations

The working groups that developed the questionnaire and conducted the pilot test were comprised of staff from both BJS and the Census Bureau. These groups reviewed the process and results of the pilot. Listed below are recommendations from these groups for the full-scale survey:

Response and follow-up

Several strategies could be employed to increase company response. Each addresses a different aspect of nonresponse:

- The primary reason given for not completing CSS was that the survey was voluntary. Mandatory reporting for this survey would help to increase unit response.
- Launch a more aggressive marketing strategy, including high-level endorsements and trade association support for reliable national statistics.
- Offer shortened questionnaires to more companies or reduce the entire survey to core questions.
- Expand telephone follow-up to contact all delinquent companies until a response or refusal is received.

Content

Responding to new surveys involves learning processes. Companies that have responded in the past better understand questions, definitions, and instructions. By year two or three, problems identified should be minimized.

Recommendations for survey questions that appear difficult or burdensome to report include the following:

- Drop questions on amount spent on computer security technology.
- Modify or drop questions on other monetary losses and costs.
- Further develop and test downtime questions and instructions.
- Further develop and test computer attack questions in order to resolve duplication between denial of service, vandalism or sabotage, and computer virus data.
- For computer viruses, decide if an average duration of downtime by type of machine is wanted (servers and PC's). If so, keep questions on number of servers and number of PC's as stated on CS-1.
- Either define computer virus incident as distinct infection or further develop and test a definition.
- Based on descriptions of "other" computer security incidents, provide a pick-list: hacking, spoofing, spam, sniffing, port scanning, and other (specify).
- Modify or drop Section IV. Some questions are repetitive to respondents who have only one incident. These same questions appear to be confusing to those with multiple incidents of the most significant type. If dropping Section IV, consider incorporating into Section III the questions on affected networks, mode of access, details of reporting incident to authorities or reasons for not reporting, and relationship between offender and company.

Questionnaire design and layout

The CSS pilot questionnaire design, layout, and question sequence received favorable remarks throughout questionnaire development and pilot testing. However, in Section III, types of incidents with questions beginning mid-page had lower response than those beginning at the top of a column. Dropping or modifying several questions will create enough space to begin questions for each type of computer security incident at the top of a column.

Edits

Preliminary tests showed clear patterns of duplicate incident data under two or more types (denial of service, vandalism or sabotage, and computer virus). The tests also showed that some companies reported multiple occurrences of a type instead of the single most significant incident. To flag these duplications or erroneous multiple reporting, the edit identified companies that failed one or more criteria (number of incidents, monetary loss, and downtime). Revise edits so that failure occurs only for companies reporting identical data for all criteria of two given types.

Reporting unit

Future surveys should be designed for company-level data collection, and allow companies to report by subsidiary or division on request. Forms for reporting below company level should differ visibly from the main form: for example, be a different color. These forms should be aggregated to the company level prior to data entry.

[2]Respondents are instructed to report incidents under the first applicable category. CSS questions about denial of service and vandalism or sabotage ask for the number of incidents caused by viruses.

Methodology

Preliminary research

Research was conducted to determine what types of cybercrime data would interest organizations such as government agencies, businesses, and trade associations and what types were currently being collected.

Current collections include the Computer Security Institute (CSI) reports on Computer Crime and Security Survey[3] and the FBI National Incident-Based Reporting System (NIBRS) data.[4] These data were also analyzed to determine what types of cybercrime businesses experienced most often and what types resulted in greatest dollar loss. Six types of incidents were identified: fraud, embezzlement, theft of proprietary information, denial of service, vandalism or sabotage, and computer virus. Current literature and news articles were also used to determine what types of data were important and what gaps needed to be filled.

External consultations for survey development

The Computer Security Survey Workshop was held April 24, 2002, in Alexandria, VA. Participants, including Federal Government agencies, trade associations, businesses, academia, and lobbyists, met to share ideas about what questions should be in the pilot. Presentations and discussions addressed the nature and prevalence of cybercrime, preventive and responsive security practices, need for reliable data, questionnaire content, and data collection strategies.

[3]The FBI's San Francisco office provided input in the development of CSI's survey, but they do not sponsor the survey. CSI does not use random sampling. It depends on "self-selected" sampling such as CSI members. CSI results are illustrative only and cannot be used to generate national estimates.

[4]NIBRS is a voluntary reporting program in which law enforcement agencies provide data. NIBRS includes details on offenses, victims, and losses. It records whether offenders used computers to commit the crime.

Cybercrime definitions for types of computer security incidents

Embezzlement: 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.

Fraud: 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, to obtain money or other things of value. Fraud may be committed by someone inside or outside the company.

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

Denial of service: 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 events such as ping attacks, port scanning probes, and excessive amounts of incoming data.

Vandalism or sabotage: the deliberate or malicious, damage, defacement, destruction or other alteration of electronic files, data, web pages, and programs.

Computer virus: a hidden fragment of computer code which propagates by inserting itself into or modifying other programs.

Other: includes all other intrusions, breaches and compromises of the respondent's computer networks (such as hacking or sniffing) regardless of whether damage or loss were sustained as a result.

Glossary of business terms

Company

Company: Business entity owning more than 50% interest in or overseeing operations and/or business establishments
Establishment: Generally each physical location of a business
Single-unit: Company with exactly one establishment
Multi-unit: Company with two or more establishments
Subsidiary: Company wholly controlled by another
Parent: Business entity owning more than 50% interest in or overseeing all operations, subsidiaries and/or establishments of a multi-unit company
Business Register: Census Bureau Business Register 2001 lists more than 7.5 million active establishments with a payroll in calendar year 2001

Industry

Industry: Line of business operated by company
NAICS: North American Industrial Classification System, which replaced Standard Industrial Classification in 1997
Principal: Line of business with greatest aggregate payroll

Complexity

Single-industry: Single or multi-unit company operating a single line of business
Complex: Company operating two to six lines of business
Very complex: Company operating seven or more lines of business

Size indicators

Employee: Person hired and paid by company
Employment: Aggregate number of employees
Payroll: Dollar amount paid to employees

Risk

Risk level: Based on principal industry, indicates company's potential level of vulnerability and/or damage due to cybercrime
Infrastructure: Principal industry is part of national infrastructure
High: Principal industry appears high risk cybercrime target
Medium: Principal industry appears medium risk cybercrime target
Low: Principal industry appears low risk cybercrime target

Reporting

Segmental: Company reports data for each industry or subsidiary on separate forms
Company-level: Company reports aggregate data for all industries or subsidiaries on one form

The CSS working group presented the project status paper *Computer Security Survey: Status on Questionnaire Development Efforts to Measure the Nature of Computer-Related Crime* to the Census Bureau's Advisory Committee of Professional Associations. Committee members supported CSS goals and commended the survey design, layout, and question sequence.

The National Security Council, President's Critical Infrastructure Protection Board, FBI National Infrastructure Protection Center, Carnegie Mellon Software Engineering Institute, Manufacturers Alliance, and Business Software Alliance were also consulted.

These consultations resulted in addressing major issues identified as important to the survey, including data sensitivity and confidentiality, data availability, collection authority (mandatory or voluntary), response burden, and company reluctance to contact law enforcement. The recommendations resulted in reworded survey questions on cybertheft and software piracy and added questions about suspected offenders and reporting incidents to law enforcement for each type of incident detected.

Cognitive testing

Drafts of CSS questionnaires were refined through three rounds of pre-testing, also called cognitive testing. During cognitive testing, employees from businesses read and answered the survey questions out loud. They explained what they were thinking, how they interpreted questions or terminology, what they included in their answers, and whether data were available.

Cognitive testing was conducted over 6 months and required between 1 and 2 hours per company. Sixty-nine companies participated, representing finance, manufacturing, and 12 other industries in 7 States and Washington, DC (table 13).

Cognitive testing revealed two concepts that needed clarification. Economic loss was difficult to define in a manner that would be interpreted consistently by all companies. For the pilot, definitions for monetary losses included lists of examples.

The concept of computer virus incidents was also difficult to define. Many respondents equated virus incidents with distinct infections; others, with different viruses. To understand how to capture computer virus incident data, an alternate series of virus questions was developed. The main form CS-1 retained the distinct infections definition. The alternate form CS-1A, sent to a fifth of the pilot sample, used different viruses. (See box on page 11 for details).

Census Bureau business surveys are usually sent to contacts designated by the company and kept on file in the Business Register. Because CSS questions are more technical, however, the computer or technical staff would seem to be a more appropriate recipient of the questionnaire. Cognitive testing showed that chief information officers, information technology directors, or security officers were the most likely to complete the survey.

Table 13. Company characteristics of cognitive testing participants, 2001 pilot survey

Company characteristic	Number
Total	69
Location	
Maryland	13
Virginia	13
Ohio	10
Washington	10
New York	9
California	7
Texas	4
District of Columbia	3
Complexity	
Single-industry	28
Multi-industry	41
Primary North American Industrial Classification System (NAICS) category	
Manufacturing	16
Finance and insurance	13
Information services	10
Professional, scientific, and technical services	7
Retail trade	5
Transportation	5
Administrative and support, and waste management and remediation services	3
Health care and social assistance	3
Wholesale	2
Arts, entertainment, and recreation	1
Construction	1
Educational services	1
Utilities	1
Miscellaneous services	1

Consequently, pilot questionnaires were mailed to Business Register contacts, requesting that they be forwarded appropriately. For companies without Business Register contacts, forms were addressed to "Information Technology Director."

Cybercrime and financial data are sensitive. During cognitive testing, many companies expressed concern regarding how (and by whom) their data would be used. To alleviate some of this concern, Title 13 confidentiality laws were placed on the front page of the CSS pilot and repeated in the section on types of computer security incidents.

These reminders reassured many subsequent respondents. Sending questionnaires to Business Register contacts also eased some concern because of their past experience with Title 13 confidentiality laws.

Business data can be collected at various levels: subsidiary, division, or company. (See box on page 8 for definitions.) Many companies, particularly large ones, operate in multiple industries. Reporting by division or subsidiary would allow better attribution of information to each line of business, and reduce burden for companies that keep records at that level.

Cognitive testing revealed that many complex companies had one information technology division for the entire company. For these companies, reporting by subsidiary would increase the burden. Other companies found multiple forms confusing. As a result, CSS pilot data were collected at the company level.

As a result of all research, external contacts, and cognitive testing, the CSS pilot questionnaire was divided into five sections, each focusing on a different aspect of computer security. Section II focused on computer infrastructure and security practices and Section III on prevalence of incidents and their cost to companies (table 14).

Sample design

Sampling frame construction relied on Census Bureau's 2001 Business Register. Aggregated to the company level, the Business Register contains principal industry, complexity, and employment data for approximately 5.3 million companies with 1 or more paid employees, excluding about 16 million firms that had no payroll and 2 million that engaged in farming.

A risk factor code, indicating the company's potential level of vulnerability and/or damage due to cybercrime, was assigned to each company based on primary industry.

Sampling was stratified and made without replacement. Strata were defined by principal industry, complexity, employment, and risk factor.

Due to their nationwide economic importance, 236 companies were selected from the largest companies from each industry. These are referred to as "certainty" companies, and will be included in the sample each time the survey is conducted.

The remainder of the sample was selected at random from each stratum. It comprised 29 very complex and 35 complex companies, one for each principal industry represented. Two hundred single-industry companies completed the sample.

Follow-up procedures

After all mail-back deadlines had passed, 26.2% of sampled companies had returned completed forms. Two rounds of telephone follow-up were conducted to increase response.

Table 14. Contents of Computer Security Survey questionnaire, by section, 2001 pilot survey

Computer security concerns
- Top three computer security concerns

Computer infrastructure and security
- Types of and access to computer networks
- Number of servers and PC's
- Types and cost of computer security technology
- Types of computer security practices

Types of computer security incidents
- Prevalence of computer security incidents
- Incidents reported to law enforcement
- Incidents committed by employees
- Downtime
- Monetary losses and recovery costs

Specific incident information
- Most significant computer security incident
- Types of networks affected
- Mode of access
- Downtime
- Monetary losses and recovery costs
- Reporting to law enforcement
- Relationship of offender to company

Other trends in computer security
- Trends in computer security incidents
- Insurance covering computer security breaches
- Piracy

Data collection activity	Cumulative percent of sample responding
Initial mailing	12.8%
Second mailing (follow-up)	21.4
Third mailing (follow-up)	26.2
First telephone follow-up	32.6
Second telephone follow-up	41.8

In the first round of telephone follow-up, companies which had neither returned questionnaire nor refused to respond were contacted. Operational status, new information, requests for forms, expected return dates, reasons for refusal (as applicable), and duration of phone calls were tracked for each company. Response rose by 6.4%.

A second telephone follow-up was conducted, limited to companies that said they would not participate. Protocols included explaining the importance of computer security information, emphasizing current lack of reliable data, ascertaining reasons for nonresponse, and offering a short form. The short form had core questions about types of networks, access, computer security technology, and practices; number of servers and PC's; detection and number of incidents by type; and, for most significant incident, type of incident, affected networks, means of access, and relationship between suspected offender and company. This last follow-up increased response by 9.2%.

Of companies not completing the pilot survey, 118 provided reasons for not participating. Eighty-two percent said they did not participate in voluntary surveys, but that they would if CSS were mandatory.

	Companies declining to complete CSS	
Reason	Number	Percent
Total	118	100%
Voluntary survey	97	82
Don't have time	49	42
Confidentiality/ sensitivity/ legal concerns	20	17
Data not available	16	14
Company policy	10	8
Other	4	3

Note: Respondents could provide more than one reason for refusal.

Response burden

Time spent completing CSS varied by company size. Companies with fewer than 100 employees spent less than an hour, on average. Companies with 1,000 or more employees took an average of about 2¾ hours to complete the CSS pilot.

Number of employees	Average time to complete CSS (minutes)
All	107
0 to 19	47
20 to 99	53
100 to 999	89
1,000 or more	166

Differences between questions and responses for the questionnaire CS-1 and its alternate CS-1A

Although many respondents classify virus incidents as distinct infections, cognitive testing revealed that some think in terms of different viruses.

To understand better how to collect information on virus incidents, alternate questions were drafted. Four-fifths of sample companies received the primary form, CS-1, containing questions modified through cognitive testing. A fifth received the alternate, CS-1A, containing untested questions about computer viruses. Tables in this report use aggregated responses from both questionnaires.

Differences between the two sets of questions include the definition of a virus incident. CS-1 defines a virus incident as a distinct infection, though the same virus might be responsible; CS-1A, as a different virus.

Item response, by question and questionnaire version for companies with virus incidents

Question	CS-1 Number	CS-1 Percent	CS-1A Number	CS-1A Percent
Total companies	104	100%	23	100%
Number of virus incidents				
One or more	101	97.1	19	82.6
Missing	3	2.9	4	17.4
PC/ workstation downtime				
1 hour or more	74	71.1	12	52.2
0 hours	9	8.7	4	17.4
Missing	21	20.2	7	30.4

For companies detecting incidents, CS-1 showed higher response rates for incident details. For example, 97% of companies receiving CS-1 reported the number of incidents detected, compared to 83% for CS-1A (table above).

Detection of virus incidents, by questionnaire version

Question	CS-1 Number	CS-1 Percent	CS-1A Number	CS-1A Percent
Total companies	162	100%	36	100%
Detection of virus incidents				
Detected incidents	104	64.2	23	63.9
Did not detect incidents	49	30.2	9	25.0
Missing	9	5.6	4	11.1

Response rates for detection of virus incidents were slightly higher for CS-1 (94%), than for CS-1A (89%) (table to left).

Small sample size and low response for CS-1A yield high standard deviations, making it difficult to form reliable conclusions about item response to the alternate set of questions. However, counting only unique viruses underestimates the magnitude of virus incidents because companies can contract a virus more than once.

Moreover, post-survey evaluation shows that two-thirds of companies equate virus incidents with distinct infections.

Virus question content and sequence, by version of questionnaire

Primary questionnaire CS-1	Alternate questionnaire CS-1A
- Viruses intercepted before causing infection	- Prevalence of incidents (different viruses)
- Prevalence of incidents (distinct infections)	- Infected machines (servers, routers, switches, PCs or workstations)
- Incidents reported to law enforcement	- Incidents reported to law enforcement
- Incidents committed by employees	- Incidents committed by employees
- Infected servers, routers or switches	- Downtime of servers, routers, or switches
- Infected PC's or workstations	- Downtime of PC's or workstations
- Downtime of servers, routers, or switches	- Person-hours spent to recover from incidents
- Downtime of PC's or workstations	- Recovery cost
- Recovery cost	- Other monetary losses
- Other monetary losses	

Item response analysis

Item response analysis describes patterns in data as reported. Only one type of imputation was used: companies that did not check *Yes* to detecting an incident but supplied positive response elsewhere were imputed as having detected that type of incident. Response analysis excludes 10 companies that reported no computer use because questions were not applicable. Response values are given only in general categories because pilot testing was aimed at determining feasibility, not producing national estimates.

Respondents were asked to report losses, expenditures, and downtime in rounded amounts. In tables 6 and 11 zeros could include amounts under $500. In table 7 zeros for downtime could include less than 30 minutes.

All tabulations and analyses are based on unweighted data. Due to small sample size and a relatively small number of respondents, the weighted estimates for CSS tabulations have standard errors ranging from 7% to 102%. Weighted responses for some CS-1A questions had a much higher standard error because of the extremely small sample size coupled with the generally low response rate.

One company requested segmental reporting for its three divisions. Two divisions returned forms, which were keyed individually. Each segment was weighted as a third. If two segments reported differently, their response was rounded down to zero. Responses for this company were adjusted manually to correct for this rounding error.

Data edits were performed on all data elements to identify reporting problems and evaluate the quality of reported data. Data edit failure does not necessarily mean the information is incorrect. It simply means that it is out of tolerance and has the potential for being incorrect. With no established baseline, tolerance limits had to be estimated.

Companies that did not answer questions due to proper use of skip patterns are excluded from analysis of those items.

The Bureau of Justice Statistics is the statistical agency of the U.S. Department of Justice. Lawrence A. Greenfeld is director.

Ramona R. Rantala, BJS statistician, wrote this report. Patrick A. Langan and Erica L. Schmitt reviewed the report. Cathy T. Maston reviewed the statistics. Tom Hester edited the report.

Representatives of the U.S. Census Bureau, BJS, the U.S. Department of Commerce, and the University of Maryland served on the team to create the 2001 Computer Security Survey. Census Bureau participants were Peggy Allen, Amy Anderson, Michael Armah, Ruth Bramblett, Stephanie Brown, Roger Brown, Carol Caldwell, Ann Daniele, Charles Funk, John Gates, Brad Jensen, Nancy Kenly, Ron Lee, Denise Lewis, Thomas Mesenbourg, Jr., Marilyn Monahan, Richard Moore, Jr., Marleen Motonis, Rebecca Morrison, John Seabold, Kristin Stettler. BJS participants were Marshall DeBerry, Jr., Lawrence Greenfeld, Ramona Rantala, and Brian Tokar (student intern). The Department of Commerce participant was Pat Buckley. Martin David was the University of Maryland participant.

To conduct the pilot took the cooperation and work of staff in the following Census Bureau offices or divisions: Forms and Mail Management and the Publication Services Branches in the Administrative and Customer Service Division, DocuPrint Staff in the Technologies Management Office, Annual Survey Processing and the Mailout and Data Capture Branches in the Economic Planning and Coordination Division, National Processing Center, Client Support and the Manufacturing and Company Statistics Annuals Branches in the Economic Statistical Methods and Programming Division, Business Investment Branch in the Company Statistics Division, and Telephone Follow-up Staff in the Governments Division, Manufacturing and Construction Division, Services Sector Statistics Division, and Company Statistics Division.

Richard Moore, Jr., and Jason Chancellor provided the data tabulations. Pam Sadowski and Susan Carodiskey provided graphics and web page design work. Jane Karl, Dawn LeBeau, Edith Stakem, Vivian Waters, Amber Niner, Melody Jones, and Debbie Vaughn gave secretarial or administrative support. Two hundred seventy-seven companies cooperated by participating in cognitive testing or responding to the pilot-survey questionnaire.

March 2004, NCJ 200639 C