Interviews: 395 IT professionals
Margin of error: ±5.0
Interview dates: June 5-7, 2002

Ipsos Public Affairs
1101 Connecticut Avenue NW, Suite 200
Washington, DC 20036
(202) 463-7300

CYBER SECURITY SURVEY
Business Software Alliance
JUNE 5-7, 2002

NOTE: All results shown are percentages unless otherwise labeled.

1. What is the likelihood that the U.S. government will be subject to a major cyber attack in the next 12 months—please use a scale of 1-to-5 where a 5 means extremely likely and a 1 means not at all likely.

5, extremely likely	16
4	34
3	31
2	13
1, not at all likely	2
Don't know/refused	4
Total 4 + 5	**49**
Total 1 + 2	**15**

2. Do you think that the risk of a major cyber attack on the U.S. has strongly increased, somewhat increased, remained the same, somewhat decreased, or strongly decreased since 9/11?

Strongly increased	15
Somewhat increased	40
Remained the same	37
Somewhat decreased	6
Strongly decreased	1
Don't know/refused	1
Total Increased	**55**
Total Decreased	**7**

3. How prepared do you think the U.S. government is for a major cyber attack—please use a scale of 1-to-5 where a 5 means extremely prepared and a 1 means not at all prepared.

5, extremely prepared	1
4	18
3	39
2	29
1, not at all prepared	9
Don't know/refused	4
Total 4 + 5	**19**
Total 1 + 2	**38**

4. Has the U.S. government's ability to defend against a major cyber attack since 9/11 gotten much better, a little better, remained the same, gotten a little worse or much worse since 9/11?

Much better	4
A little better	54
Remained the same	34
A little worse	2
Much worse	-
Don't know/refused	6
Total Better	**57**
Total Worse	**3**

5. How important is it for the U.S. government to secure its sensitive information so hackers will not be able to access it even if they break into government computer systems? Please use a scale of 1-to-5 where a 5 means extremely important and a 1 means not at all important.

5, extremely important	88
4	9
3	2
2	-
1, not at all important	-
Don't know/refused	1
Total 4 + 5	**96**
Total 1 + 2	**0**

6. Do you think there is a gap between the threat of a major cyber attack in the U.S. and the government's ability to defend against a major cyber attack?

Yes	72
No	13
Don't know/refused	15

(ASKED ONLY OF RESPONDENTS WHO SAY, "YES, THERE IS A GAP" IN Q.6.)

7. Has the gap between the threat of a major cyber attack in the U.S. and the government's ability to defend against a major cyber attack increased a lot, increased a little, remained the same, decreased a little, or decreased a lot since 9/11?

Increased a lot	7
Increased a little	29
Remained the same	31
Decreased a little	28
Decreased a lot	2
Don't know/refused	3
Total Increased	**37**
Total Decreased	**30**

8. Do you think that the US government is devoting much more time and resources, a little more time and resources, the same amount of time and resources, a little less time and resources, or much less time and resources to defending against cyber attacks than they did to addressing Y2K issues?

Much more	10
A little more	37
The same amount	13
A little less	19
Much less	15
Don't know/refused	6
Total More	**47**
Total Less	**34**

9. Do you think that the US government SHOULD devote much more time and resources, a little more time and resources, the same amount of time and resources, a little less time and resources, or much less time and resources to defending against cyber attacks than they did to addressing Y2K issues?

Much more	53
A little more	33
The same amount	11
A little less	1
Much less	-
Don't know/refused	2
Total More	**86**
Total Less	**1**

10. The US Federal government is in the process of implementing its e-government services. E-government services include on-line registration forms, licenses, tax filing, a web portal that allows for easy access to information and direct communication between citizens and government agencies, and data sharing and communications among government agencies. How strongly do you believe that the U.S. government has built adequate security measures into its e-government program? To answer, please use a scale of 1-5, where a 5 means you strongly believe that the U.S. government has built adequate security measures into its e-government program and a 1 means that you do not at all believe that the U.S. government has built adequate security measures into its e-government program.

5, extremely adequate	1
4	22
3	36
2	22
1, not at all adequate	10
Don't know/refused	9
Total 4 + 5	**23**
Total 1 + 2	**32**

11. Rate the likelihood that each of the following will be the target of a major cyber-attack in the next year, using a 1-to-5 scale, where 5 means that the institution is certain to be the target of a cyber-attack and a 1 means that the institution is not at all likely to be the target of a cyber-attack.

THIS TABLE IS RANKED BY THE PERCENTAGE WHO GIVE A RATING OF 4 OR 5

	Certain 5	4	3	2	Not At All Likely 1	DK/ REF	**Total 4 + 5**	**Total 1 + 2**
National financial institutions, such as Wall Street or big national banks	33	41	18	5	-	3	**74**	**6**
Communication systems such as telephones and the Internet	28	39	23	5	2	3	**67**	**7**
Transportation infrastructure such as air traffic control computer systems	26	41	22	7	1	3	**67**	**8**
Utilities such as water stations, dams, or power plant computer systems	25	39	23	9	2	2	**64**	**10**
Energy industry computer systems such as those related to pipelines, wells, or tankers	20	39	26	10	2	3	**59**	**12**
Personal financial institutions' databases, at banks and credit card companies	24	33	25	12	3	3	**57**	**15**
Emergency response systems for the police, fire departments, or ambulances	14	28	31	20	4	3	**42**	**24**
Media outlets such as radio, TV, and newspapers	7	24	33	26	7	3	**32**	**32**
The health care system, including hospitals, clinics, or health insurance provider data bases	5	17	36	31	8	3	**22**	**39**

DEMOGRAPHICS

A. What is the size of the company you work for, less than thirty employees, thirty to one hundred employees, one hundred to five hundred employees, or more than five hundred employees?

Less than 30 employees	16
30 to 100 employees	11
100 to 500 employees	18
More than 500 employees	50
Don't know/refused	5

B. Which of the following categories best describes your business sector?

Manufacturing	7
Service	18
Technology	43
Sales	6
Other	24
Don't know/refused	2

C. What is your greatest level of involvement in purchasing or developing computer on-line security or cyber-security protection for your company?

Make final recommendations	8
Have significant input in these recommendations	20
Have informal input in these recommendations	34
Have no input at all in these recommendations	35
Don't know/refused	3

D1. How long have you been an IT professional?

1 year or less	5
2 to 3 years	14
4 to 5 years	14
6 to 10 years	24
11 to 15 years	14
More than 15 years	23
Don't know/refused	6

D2. How old are you?

18 to 24	3
25 to 29	11
30 to 34	16
35 to 39	14
40 to 44	19
45 to 49	14
50 or older	23
Don't know/refused	-