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

Interviews: 602 IT professionals
Margin of error: ±4.1
Interview dates: July 8-10, 2002

IPSOS/BSA/BUSINESS 2.0
CYBER-SECURITY SURVEY
IT PROFESSIONALS
JULY 8-10, 2002

NOTE: All results shown are percentages unless otherwise labeled.

1. What is the likelihood that U.S. businesses 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	15
4	31
3	31
2	15
1, not at all likely	4
Don't know/refused	4
Total 4 + 5	**47**
Total 1 + 2	**19**

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

Strongly increased	14
Somewhat increased	48
Remained the same	30
Somewhat decreased	5
Strongly decreased	2
Don't know/refused	1
Total Increased	**62**
Total Decreased	**7**

3. How prepared do you think U.S. businesses are to defend themselves against 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	17
3	35
2	37
1, not at all prepared	7
Don't know/refused	3
Total 4 + 5	**18**
Total 1 + 2	**45**

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

Much better	5
A little better	52
Remained the same	36
A little worse	3
Much worse	1
Don't know/refused	3
Total Better	**58**
Total Worse	**4**

5. Considering all the things U.S. businesses need to focus on—costs, price, innovation, employees, and so forth—how big a priority do you think U.S. businesses should place efforts to defend themselves against a major cyber attack. Use a 1-to-5 scale, where 5 means it should be among their top priorities and 1 means they should put it low on their list of priorities.

5, top priority	23
4	48
3	23
2	5
1, low priority	-
Don't know/refused	1
Total 4 + 5	**71**
Total 1 + 2	**5**

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

Yes	68
No	16
Don't know/refused	16

(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 U.S. businesses' ability to defend themselves 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	9
Increased a little	31
Remained the same	26
Decreased a little	30
Decreased a lot	2
Don't know/refused	2
Total Increased	**41**
Total Decreased	**32**

8. Do you think that businesses in the U.S. are 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	4
A little more	29
The same amount	18
A little less	22
Much less	25
Don't know/refused	2
Total More	**33**
Total Less	**47**

9. Do you think that businesses in the U.S. 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	32
A little more	39
The same amount	18
A little less	8
Much less	2
Don't know/refused	1
Total More	**71**
Total Less	**10**

10. Now I'd like to ask you some questions about cyber security at your own company. For each of the following, please tell me if this is an action that your company has already undertaken, will undertake in the near term, will undertake in the long term, or if it is not an action that your company is contemplating.

THIS TABLE IS RANKED BY THE PERCENTAGE WHO SAY COMPANY HAS ALREADY UNDERTAKEN

	Has Already Under-taken	Will Undertake In The Near Term	Will Undertake In The Long Term	Company Is Not Contem-plating	DK/ Ref
Every computer has anti-virus software installed	92	2	1	-	5
Every network uses a firewall to prevent unauthorized access to and use by hackers	86	6	1	1	6
Your organization uses backup software daily	78	5	2	3	12
Your organization's IT staff has basic security training	61	8	5	9	17
Computer passwords are changed every 90 days	60	9	5	17	9
Your organization has at least one employee or outside consultant responsible for your cyber security needs	57	6	3	13	21
Your IT administrator checks for security updates at least every 7 days for all programs on your organization's computers, including operating systems	57	10	4	7	22
Your organization explains to all employees on a regular basis the need to be cyber secure	57	9	8	16	10

Q.10 (cont.)	Has Already Under-taken	Will Undertake In The Near Term	Will Undertake In The Long Term	Company Is Not Contem-plating	DK/ Ref
Your organization uses virtual private networking to protect against data interception	55	7	4	10	24
Your organization's backup software is kept offsite	53	7	6	13	21
Your organization's annual budget includes a specific computer security component	51	7	3	10	29
Your organization securely authenticates the electronic communications of your customers, partners, and employees	48	9	7	11	25
Your organization uses end-to-end encryption to protect your sensitive customer and business information, such as credit card data, company business plans, and payroll information	47	8	7	11	27
Your organization has a central person to coordinate reporting of cyber attacks to local law enforcement agencies, or your organization's IT provider	44	5	5	11	35
Your organization has insurance against cyber crime	13	6	5	15	61

11. How important is it for your company to be able to conduct business on-line—is it very important, fairly important, not very important, or not at all important for your company to be able to conduct business on-line?

Very important	56
Fairly important	29
Not very important	10
Not at all important	3
Don't know/refused	2
Total Important	**84**
Total Not Important	**14**

12. Do you think it is very safe, fairly safe, not very safe, or not safe at all for your company to conduct business on-line?

Very safe	21
Fairly safe	71
Not very safe	6
Not safe at all	-
Don't know/refused	2
Total Safe	**91**
Total Not Safe	**7**

13. When it comes to doing business on the Internet, which **ONE** of the following three statements comes closest to your view?

I do not worry about the security of my business transactions on the Internet	19
I am concerned about security of business transactions, but the benefits and convenience of using the Internet outweigh these concerns	70
I am very concerned about security of my business transactions, and would be unwilling to handle any important business transactions over the Internet	11
Don't know/refused	-

14. How much confidence do you have in the technology industry to develop tools to give companies like yours more control over your on-line security—a great deal, a fair amount, not much, or no confidence?

A great deal of confidence	30
A fair amount of confidence	59
Not much confidence	7
No confidence at all	1
Don't know/refused	3
Total Great Deal/Fair Amount Of Confidence	**89**
Total Not Much/No Confidence	**8**

15. In terms of security, how important is it to be using a licensed and up-to-date version of software?

Very important	68
Fairly important	25
Not very important	5
Not at all important	1
Don't know/refused	1
Total Important	**93**
Total Not Important	**6**

DEMOGRAPHICS

A. What is the size of the company you work for?

Less than 50 employees	16
50 to 100 employees	9
100 to 500 employees	13
More than 500 employees	60
Don't know/refused	2

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

Manufacturing	8
Service	18
Technology	35
Sales	5
Government	11
Other	22
Don't know/refused	1

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	11
Have significant input in these recommendations	18
Have informal input in these recommendations	30
Have no input at all in these recommendations	39
Don't know/refused	2

D. What is your job title?

Executive/manager	24
Analyst	8
Administrator	6
Programmer/software designer	9
Engineer	7
Support/help desk/customer service	7
Consultant	6
Other	30
None	1
Don't know/refused	1

E. How long have you been an IT professional?

1 year or less	5
2 to 3 years	17
4 to 5 years	18
6 to 10 years	19
11 to 15 years	11
More than 15 years	26
Don't know/refused	4

F. How old are you?

18 to 24	5
25 to 29	14
30 to 34	14
35 to 39	15
40 to 44	14
45 to 49	15
50 or older	22
Don't know/refused	1