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

New York
Toronto
Minneapolis
Washington, D.C.
Vancouver
San Francisco
Montréal
Ottawa
Winnipeg
Calgary

Research for the Business Software Alliance

Business Software Alliance
www.bsa.org

Cyber Security Survey

June 25, 2002

Survey of 395 IT Professionals
Conducted June 5 to June 7, 2002

Executive Summary

IT pros say the U.S. is at risk of a *major* cyber attack, and the government is not adequately prepared to face that attack.

- Half of all IT pros **(49%)** say it is likely that the U.S. government will be subject to a **major** cyber attack in the next 12 months.
  - IT pros are 8 times more likely to say a **major** cyber attack is **extremely likely (16%)** than **not at all likely (2%).**
  - Among those IT pros most expert on security issues – those responsible for their company's computer and Internet security – **59%** feel a **major** cyber attack is likely within the next year.
- More than half of all IT pros **(55%)** feel that the risk of a **major** cyber attack on the U.S. has increased since 9/11, whereas only 7% feel the risk has decreased.
  - By a 15-to-1 margin IT pros are more likely to say the risk of a **major** cyber attack has **strongly increased (15%)** than **strongly decreased (1%).**
- By a 2-to-1 margin, IT pros are more likely to say that the government is not prepared for a **major** cyber attack **(38%)** than to say the government is prepared **(19%).**
  - By a 9-to-1 margin, IT pros are more likely to say the U.S. government is **not at all prepared (9%)** than **extremely prepared (1%)**.

Executive Summary (Continued)

IT pros say there is a gap between the threat of a *major* cyber attack and the government's ability to defend against it – and that gap has not decreased since 9/11.

- Almost 3-in-4 IT pros **(72%)** say 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.
  - Among those IT pros most expert on security issues – those responsible for their company's computer and Internet security, **84%** say there is a gap between the threat of a **major** cyber attack and the government's ability to defend against it.
- 2-in-3 IT pros **(68%)** say the gap between the threat of a **major** cyber attack and the government's ability to defend against it has has either **increased (37%)** or **remained the same (31%)** since 9/11.
  - Few IT pros **(30%)** say the gap between the threat of a **major** cyber attack and the government's ability to defend against it has **decreased** since 9/11.

Executive Summary (Continued)

Nearly all IT pros believe that the U.S. government should secure its sensitive information so hackers will not be able to access it even if they break into government's computer system.

- **96%** of IT pros say it is important that the U.S. government secure its sensitive information.
  - Nearly 9-in-10 IT pros **(88%)** say it is **extremely important**.

IT pros are generally divided regarding whether or not the U.S. government has built adequate security measures into its e-government program.

- About 1-in-4 IT pros **(23%)** say the U.S. government has built **adequate** security measures into its e-government program whereas 1-in-3 IT pros **(32%)** say the security measures are **not adequate**.
  - By a 10-to-1 margin, however, IT pros are more likely to say the U.S. government security measures are **not at all adequate (10%)** than **extremely adequate (1%).**

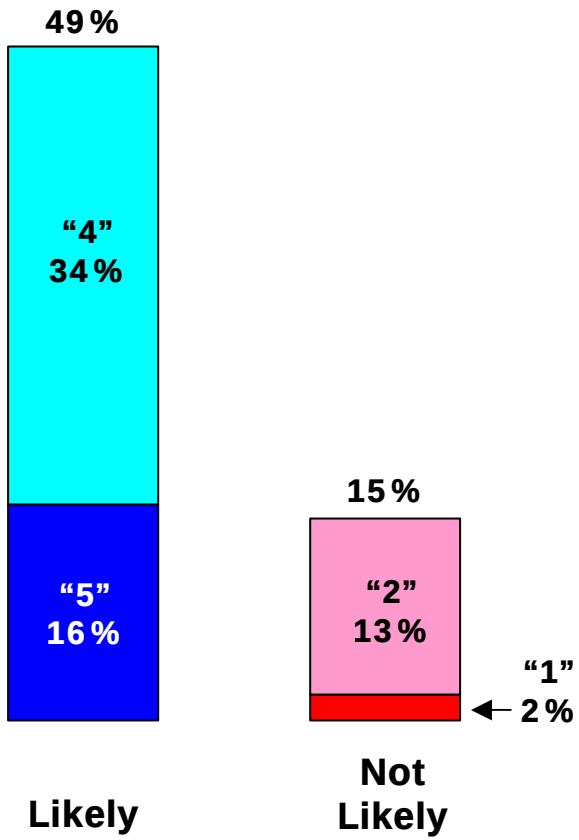
Executive Summary (Continued)

IT pros say the government's response to the threat of cyber attacks should be even more vigilant than its efforts on Y2K.

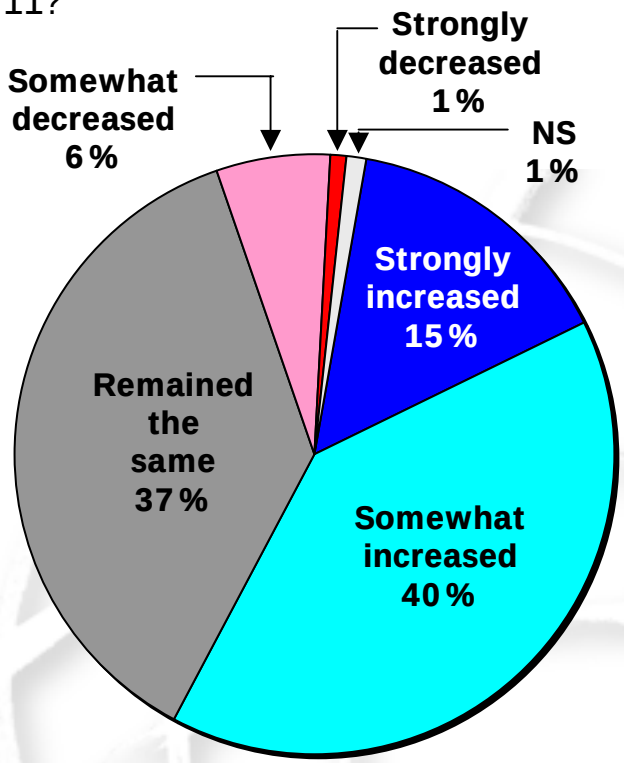
- Nearly all IT pros **(86%)** say the U.S. government **should** devote **more** time and resources to defending against cyber attacks than it did addressing Y2K issues.
  - Only **1%** of IT pros say the U.S. government **should** devote **less** time and resources.
- Fewer than half of all IT pros **(47%)** say the U.S. government **is** devoting **more** time and resources to defending against cyber attacks than it did addressing Y2K issues.
  - 1-in-3 IT pros **(34%)** say the U.S. government is devoting **less** time and resources.

Likelihood of Major Cyber Attack on U.S. Government

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.



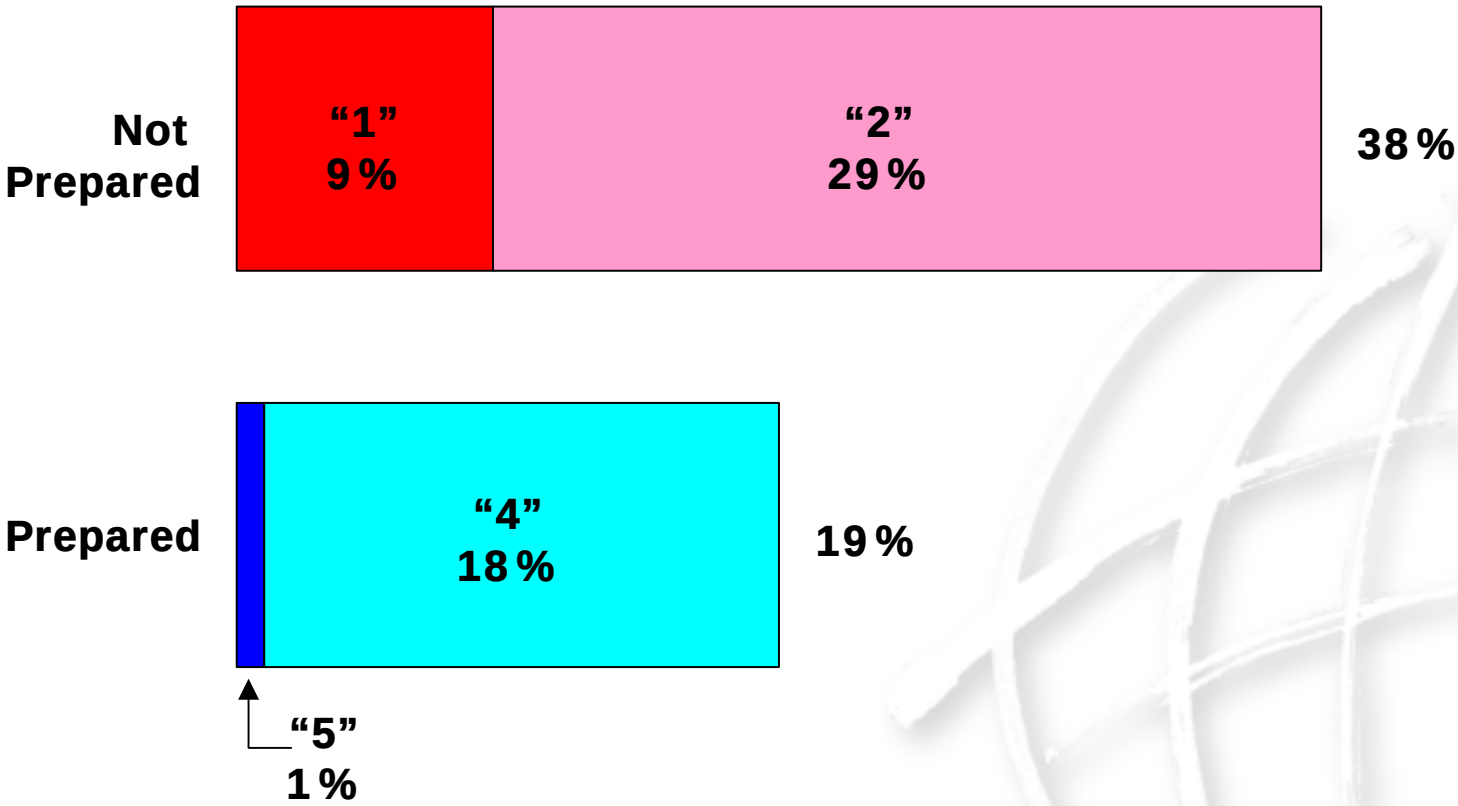
Do you think that the risk of a **major** cyber attack on the U.S. has strongly increased, somewhat increased, remained the same, somewhat decreased, or strongly decreased since 9/11?



Total increased = *55%*
Total decreased = *7%*

Preparedness of U.S. Government for Major Cyber Attack

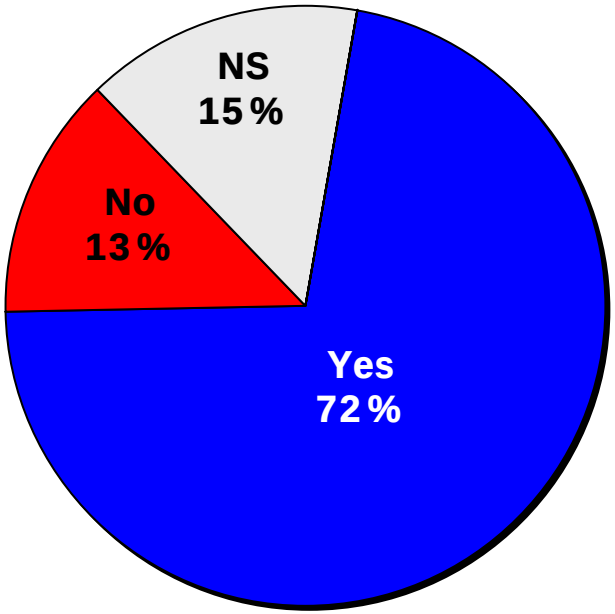
How prepared do you think the U.S. government is for a **major** cyber attack — please use a scale of 1-to-5 where a 5 means extremely prepared and a 1 means not at all prepared.



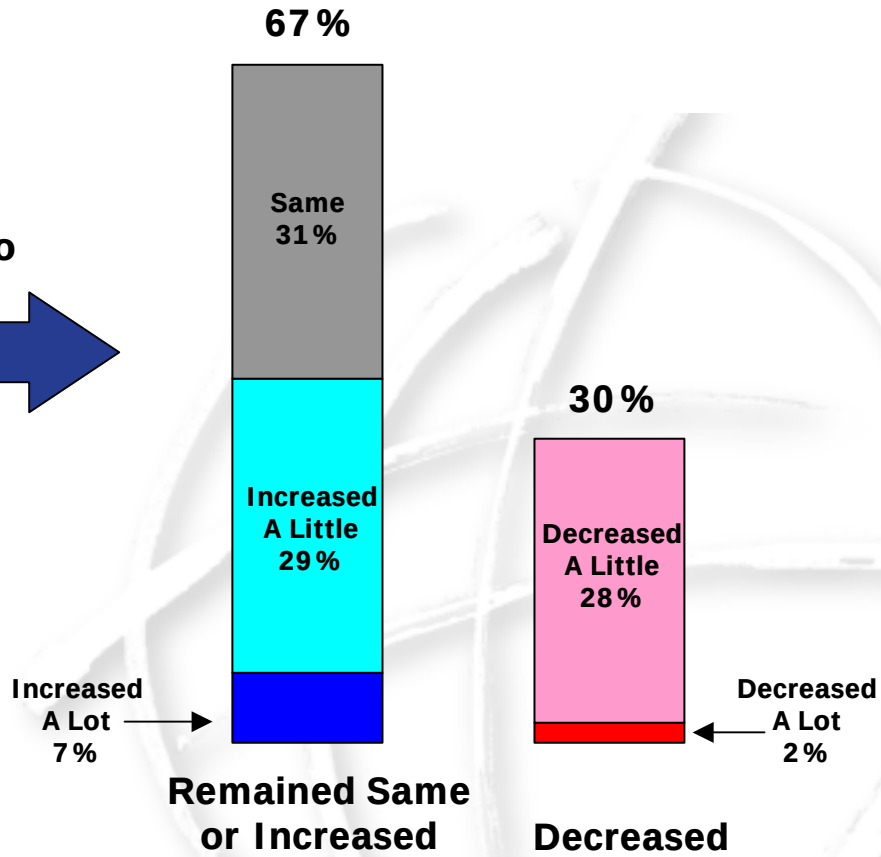
Gap Between Threat of Major Cyber Attack & Government's Ability to Defend

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?

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?

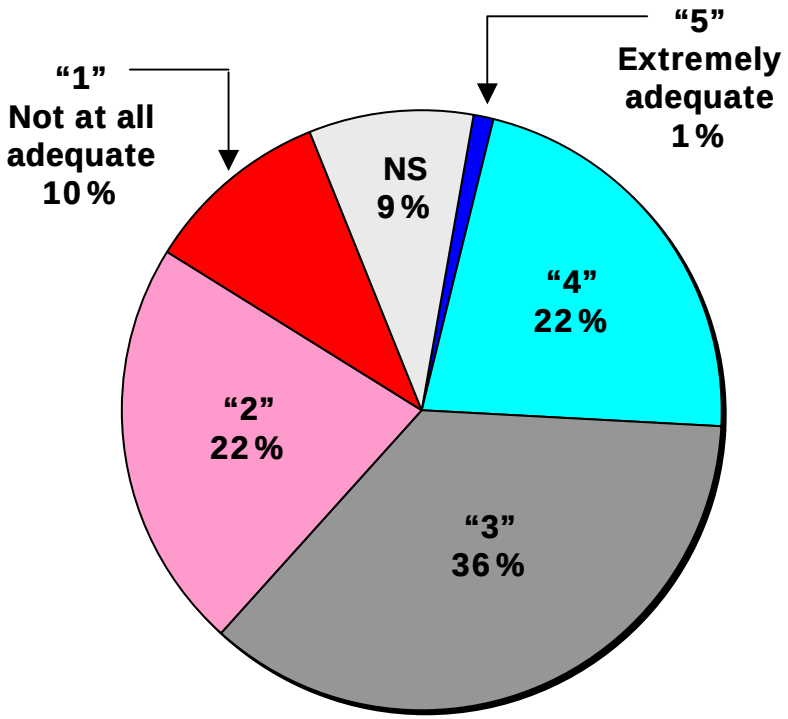


Those who say "Yes"



Adequacy of Security Measures for E-Gov't Program & Importance of Security

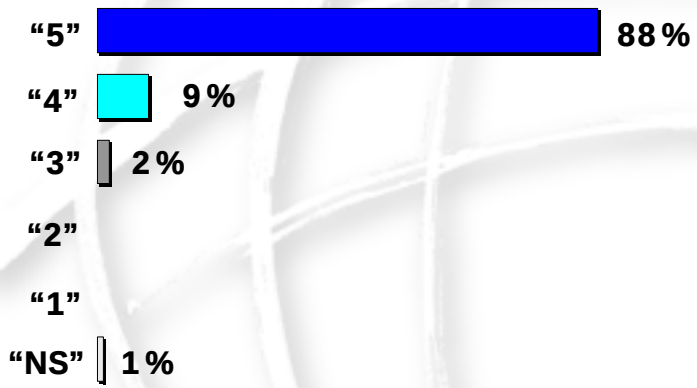
The U.S. federal government is in the process of implementing its e-government services... How strongly do you believe that the U.S. government has built adequate security measures into its e-government program? To answer, please use a scale of 1-5, where a 5 means you strongly believe that the U.S. 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.



Total 4 + 5 = *23%*
Total 1 + 2 = *32%*

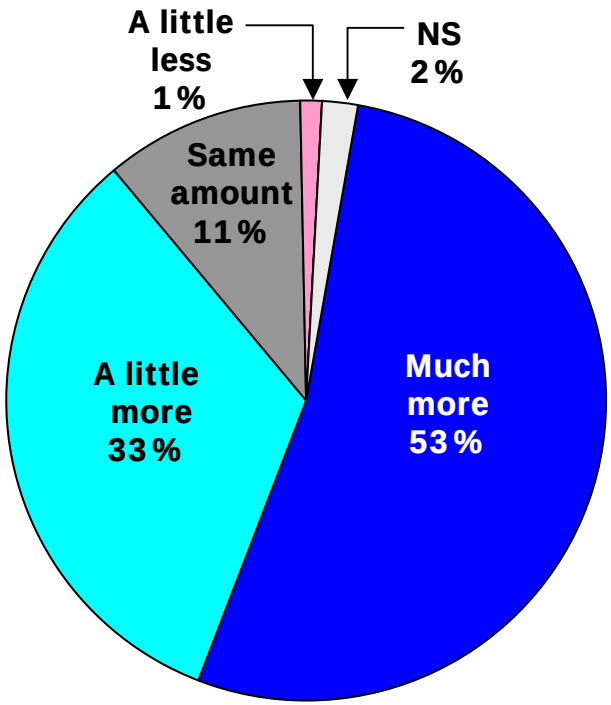
Security

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.



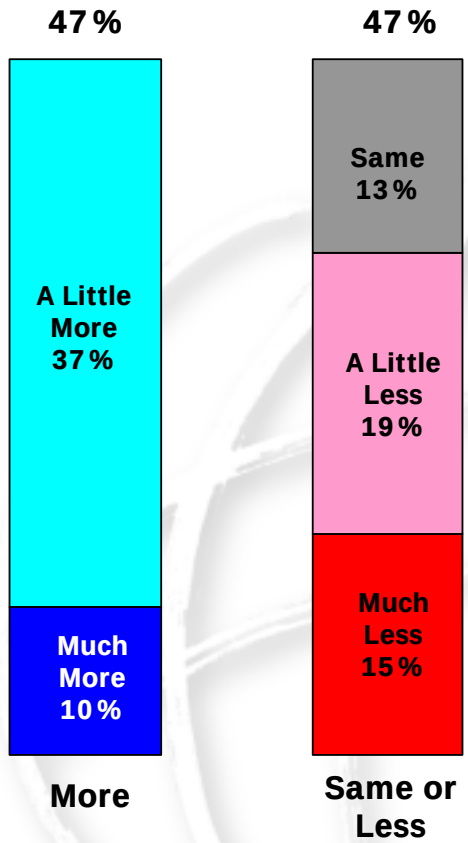
Time and Resources Devoted by U.S. Government to Cyber Attacks vs. Y2K

Do you think that the U.S. 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 it did to addressing Y2K issues?



Total More = *86%*
Total Less = *1%*

Do you think that the U.S. 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 it did to addressing Y2K issues?



Methodology and Sample

Methodology

- On-line interviews with 395 IT pros
- Interviews completed between June 5 and June 7, 2002
- Margin of error: ± 5%

Sample

- Company size:
  - Less than 100 employees: 27%
  - 100 to 500 employees: 18%
  - More than 500 employees: 50%
- Business Sector:
  - Manufacturing: 7%
  - Service: 18%
  - Technology: 43%
  - Sales: 6%
  - Other: 24%
- Level of involvement in purchasing or developing on-line security or cyber-security:
  - At least some input: 62%
  - No input: 35%
- Length of time as IT pro:
  - 5 years or less: 33%
  - 6 to 15 years: 38%
  - More than 15 years: 23%