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

U.S. Business Cyber Security Study

Research for the Business Software Alliance

Business Software Alliance
www.bsa.org

Media Partner

BUSINESS 2.0

July 24, 2002

Survey of 602 IT Professionals
Survey of 1,000 U.S. Adults
Survey of 1,094 U.S. Internet Users
Research Conducted Between July 8 and July 15, 2002

Executive Summary: IT Pros on Security

IT pros say the risk of a *major* cyber attack on U.S. businesses has increased since 9/11.

- Almost 2-in-3 IT pros **(62%)** say the risk of a **major** cyber attack has **increased** since 9/11.
  - Fewer than 1-in-10 IT pros **(7%)** say the risk of a **major** cyber attack has **decreased** since 9/11.

IT pros say U.S. businesses are likely to face a *major* cyber attack within the next year.

- Half of all IT pros **(47%)** say it is likely that U.S. businesses will be subject to a **major** cyber attack in the next 12 months.
  - Among those IT pros most expert on security issues – those responsible for their company's computer and Internet security – **60%** feel a **major** cyber attack is likely within the next year.

IT Pros on Security

A majority of IT pros say that U.S. businesses' ability to defend against a *major* cyber attack has improved since 9/11.

- More than half of IT pros **(58%)** say that U.S. businesses' ability to defend against a **major** cyber attack has gotten **better** since 9/11.
  - Few IT pros **(4%)** say U.S. businesses' ability to defend against a **major** cyber attack has gotten **worse** since 9/11.

Many IT pros, however, think U.S. businesses *are not* prepared for a *major* cyber attack.

- Nearly half of all IT pros **(45%)** say U.S. businesses are **not prepared** for a **major** cyber attack, and **7%** of IT pros say U.S. businesses are **not at all prepared.**
  - Only 1-in-5 IT pros **(18%)** say U.S. businesses are **prepared** for a **major** cyber attack, and only **1%** of IT pros say U.S. businesses are **extremely** prepared.

IT Pros on Security

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

- More than 2-in-3 IT pros **(68%)** say there is a gap between the threat of a **major** cyber attack in the U.S. and U.S. businesses' 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 – **75%** say there is a gap between the threat of a **major** cyber attack and businesses' ability to defend against it.
- 2-in-3 IT pros **(66%)** say the gap between the threat of a **major** cyber attack and U.S. businesses' ability to defend against it has either **increased (40%)** or **remained the same (26%)** since 9/11.
  - Few IT pros **(32%)** say the gap between the threat of a **major** cyber attack and U.S. businesses' ability to defend against it has **decreased** since 9/11.

IT Pros on Security

IT pros say that U.S. businesses' response to the threat of cyber attacks should be greater than its efforts on Y2K, but they sense the level of effort to defend against cyber attacks is actually less than businesses' Y2K efforts.

- Nearly 3-in-4 IT pros **(71%)** say U.S. businesses **should** devote **more** time and resources defending against cyber attacks than they did addressing Y2K issues.
  - Only **(10%)** of IT pros say U.S. businesses **should** devote **less** time and resources.
- Only a third of IT pros **(33%)** say U.S. businesses **are** devoting **more** time and resources defending against cyber attacks than they did addressing Y2K issues.
  - Half of all IT pros **(47%)** say U.S. businesses **are** devoting **less** time and resources.

IT Pros on Security

IT pros feel that, in general, their companies are making important strides to ensure that their computer networks are cyber secure.

- Among the BSA checklist items that IT pros say their company "has already undertaken" or "will undertake in the near term":
  - Nearly all IT pros say every computer has anti-virus software installed **(94%)**; every network uses a firewall to prevent unauthorized access by hackers **(92%)**; and their organization uses backup software daily **(83%)**.
  - About 2-in-3 IT pros say their company's IT staff has basic security training **(69%)**; that computer passwords are changed every 90 days **(69%)**; that their IT administration checks for security updates at least every 7 days **(67%)**; and that their organization explains to all employees on a regular basis the need to be cyber secure **(67%)**.

Executive Summary: Public, E-Commerce and Security

U.S. Internet users perceive greater concerns than IT pros about the net value relative to risk of doing business on the Internet.

- More than 2-in-3 IT pros **(70%)** say they are concerned about security on the Internet but the benefits and convenience of the Internet outweigh their concerns.
  - About half of all adults **(56%)** say they are concerned about security on the Internet but the benefits and convenience of the Internet outweigh their concerns.

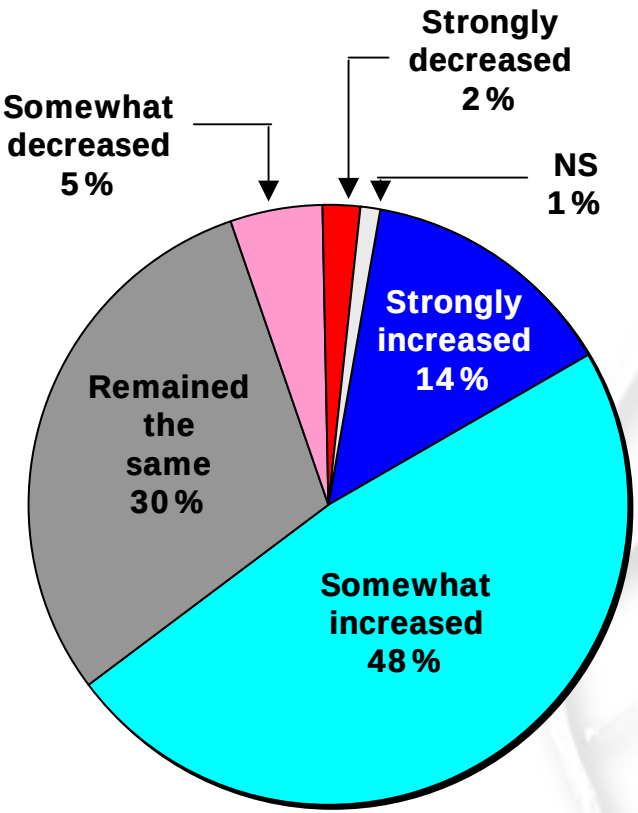
U.S. Internet users have as much faith as IT pros in the ability of the technology industry to solve the Internet security problems.

- Nearly all U.S. adults **(84%)** and nearly all IT pros **(89%)** say they have confidence in the technology industry to develop tools that will give them more control over online security.

Risk of Major Cyber Attack on U.S. Businesses

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?

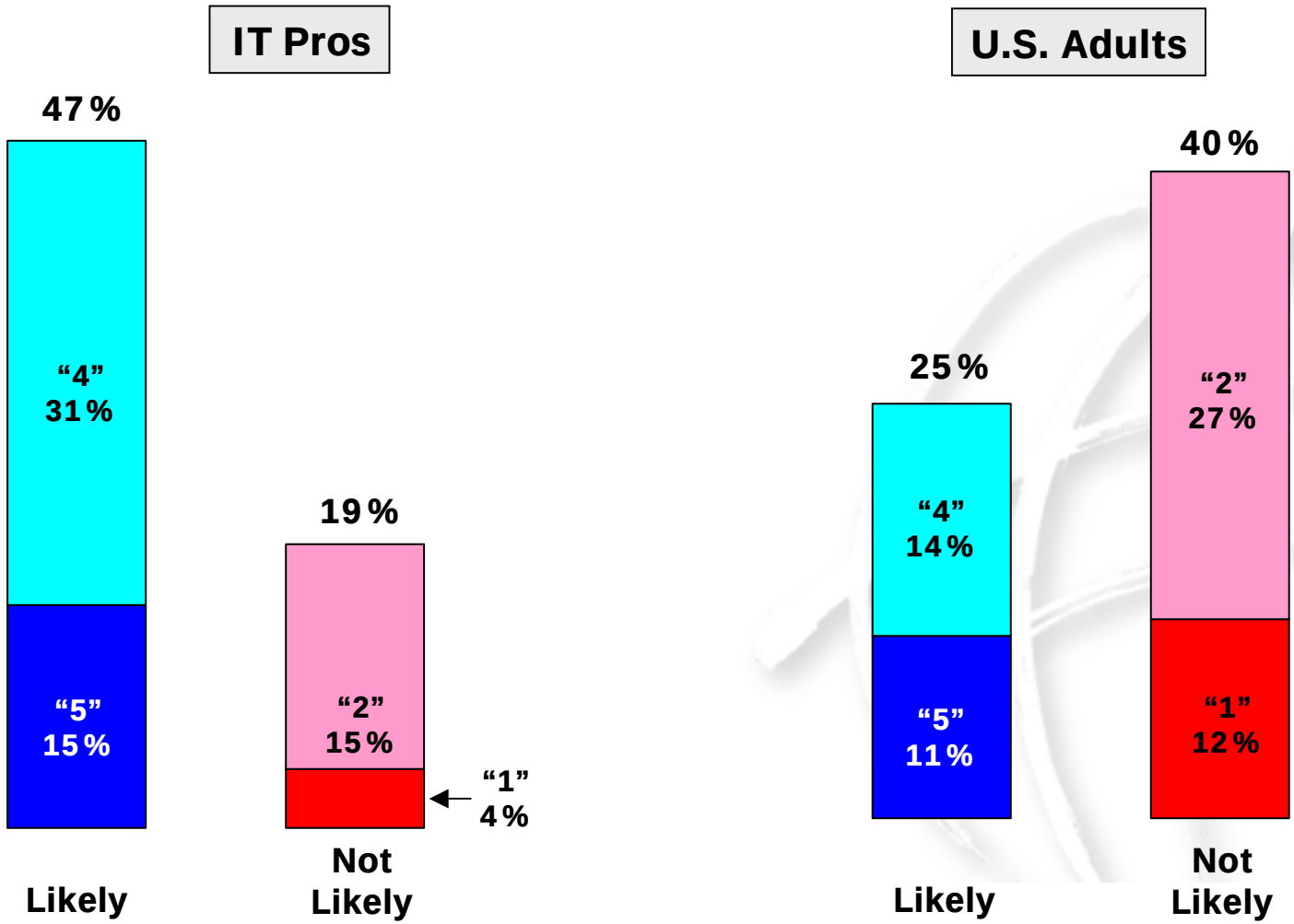
IT Pros



Total increased = *62%*
Total decreased = *7%*

Likelihood of Major Cyber Attack on U.S. Businesses

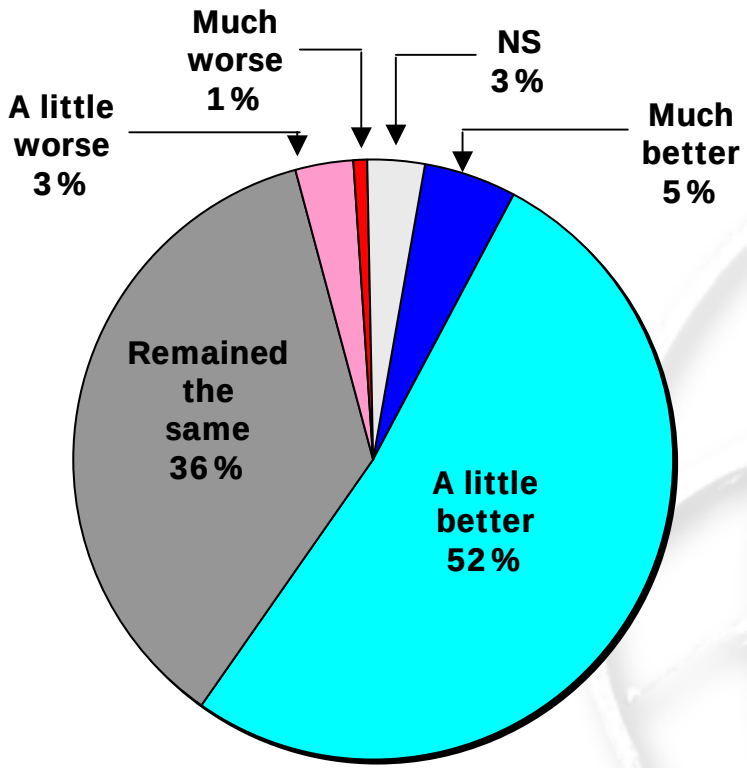
What is the likelihood that U.S. businesses will be subject to a **major** cyber attack in the next 12 months? Please use a scale of 1-to-5, where a 5 means extremely likely and a 1 means not at all likely.



Businesses' Ability to Defend since 9/11

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?

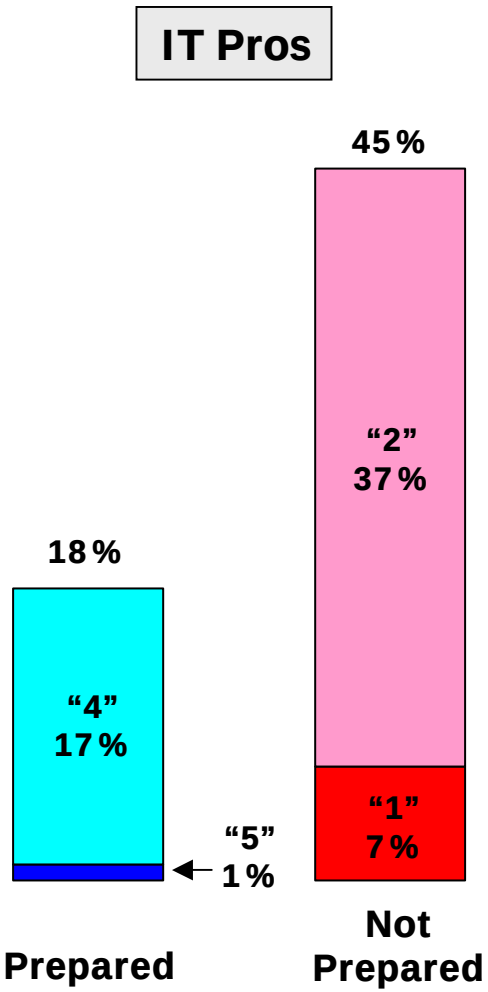
IT Pros

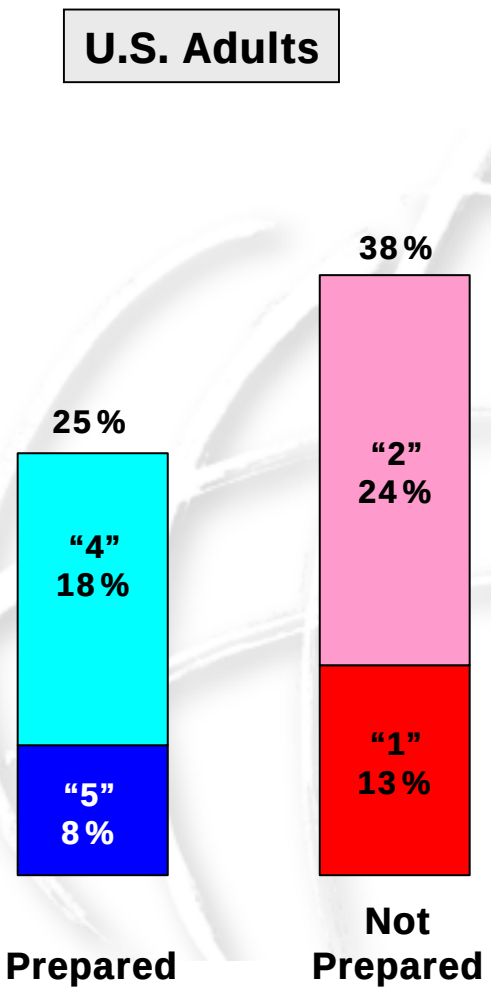


Total better = *58%*
Total worse = *4%*

Preparedness of U.S. Businesses for Major Cyber Attack

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

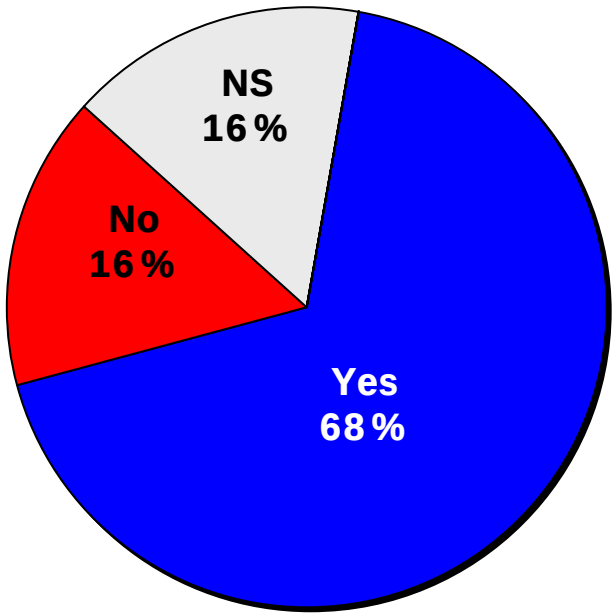




Gap Between Threat of Major Cyber Attack & U.S. Businesses' Ability to Defend

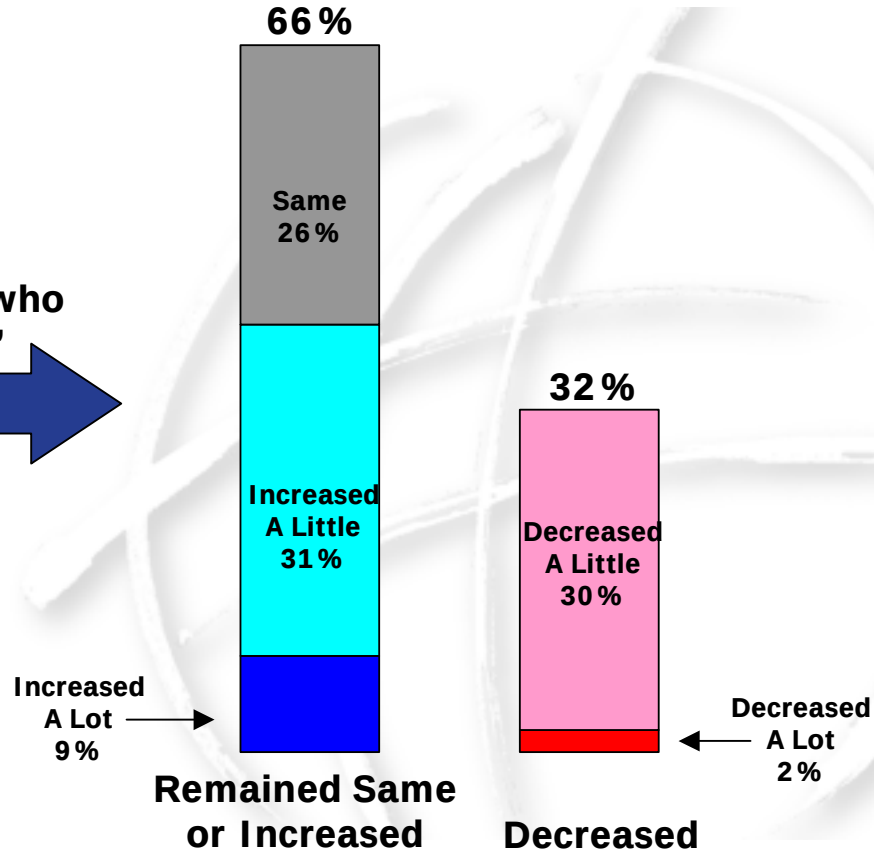
Do you think there is a gap between the threat of a **major** cyber attack in the U.S. and the ability of U.S. businesses to defend against a major cyber attack?

IT Pros



Of those who said "Yes"

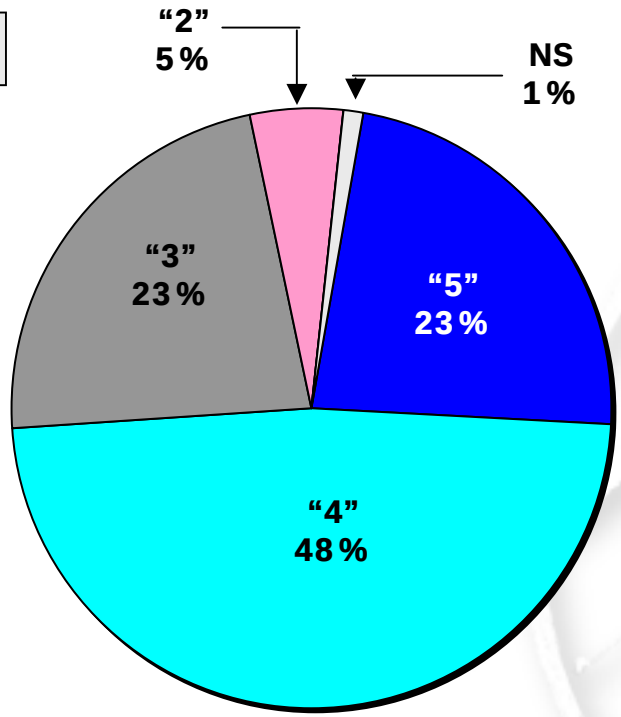
Has the gap between the threat of a **major** cyber attack in the U.S. and U.S. businesses' ability to defend against a major cyber attack increased a lot, increased a little, remained the same, decreased a little, or decreased a lot since 9/11?



Priority of Efforts to Defend Against Major Cyber Attack

Considering all the things that 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 on efforts to defend themselves against a major cyber attack? Use a scale of 1-to-5, where 5 means it should be among their top priorities and 1 means they should put it low on their list of priorities.

IT Pros



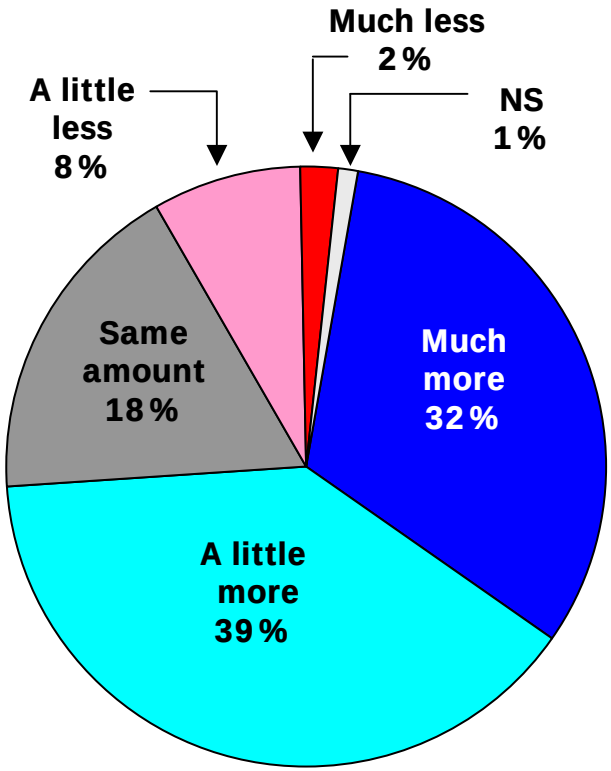
High priority = *71%*
Low priority = *5%*

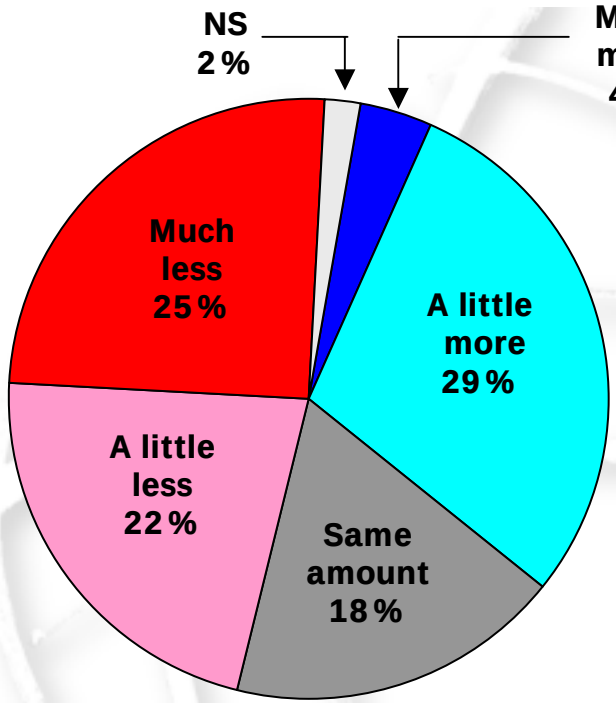
Time and Resources Devoted by U.S. Businesses to Cyber Attacks vs. Y2K

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 it did to addressing Y2K issues?

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?

IT Pros





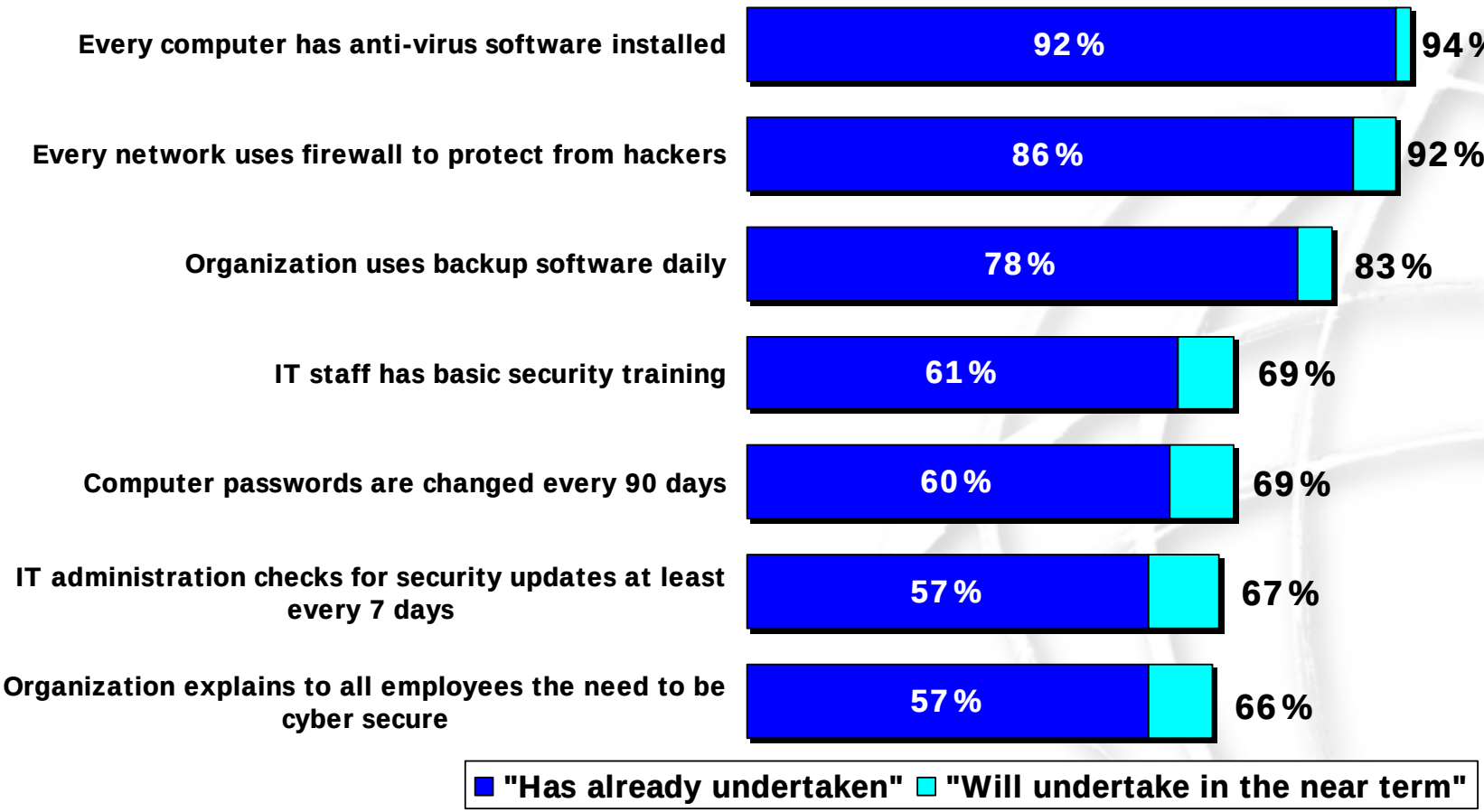
Businesses *should* devote... Total More = *71%*, Total Less = *10%* ...resources than to Y2K

Businesses *are* devoting... Total More = *33%*, Total Less = *47%* ...resources than to Y2K

Cyber-Security Checklist

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, or if it is not an action that your company is contemplating.

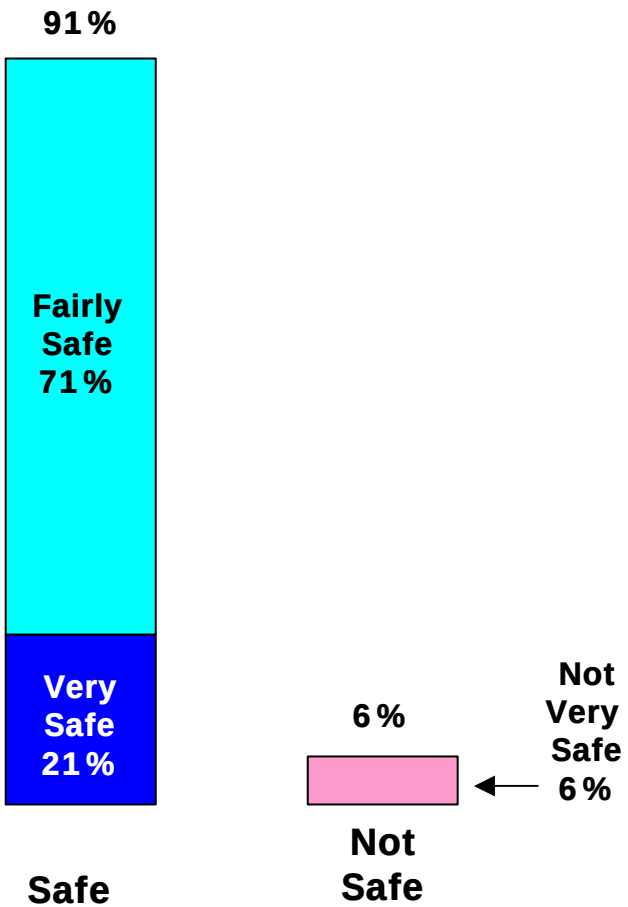
Ranked by Percent who Answer "Has already undertaken" or "Will undertake in the near term"



E-Commerce Security

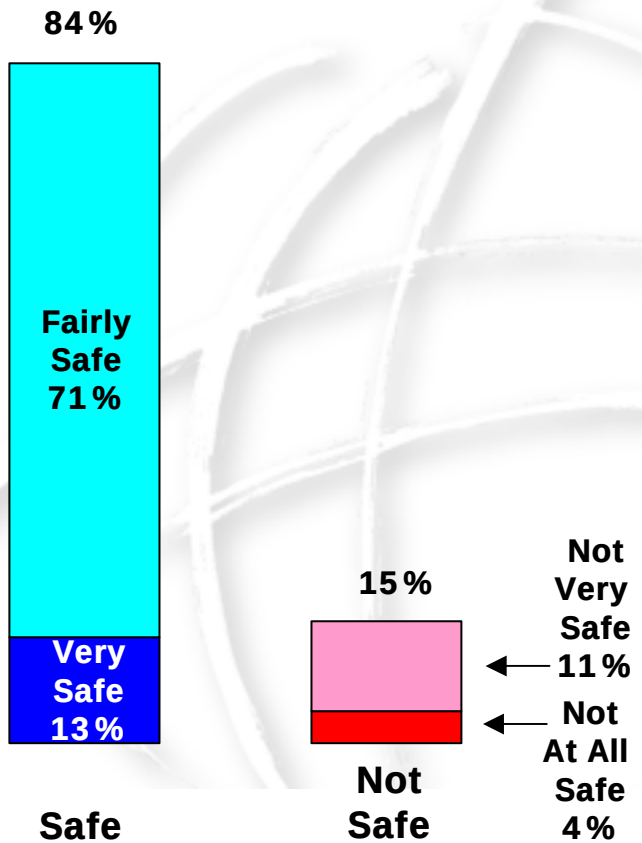
Do you think it is very safe, fairly safe, not very safe, or not at all safe for your company to conduct business online?

IT Pros



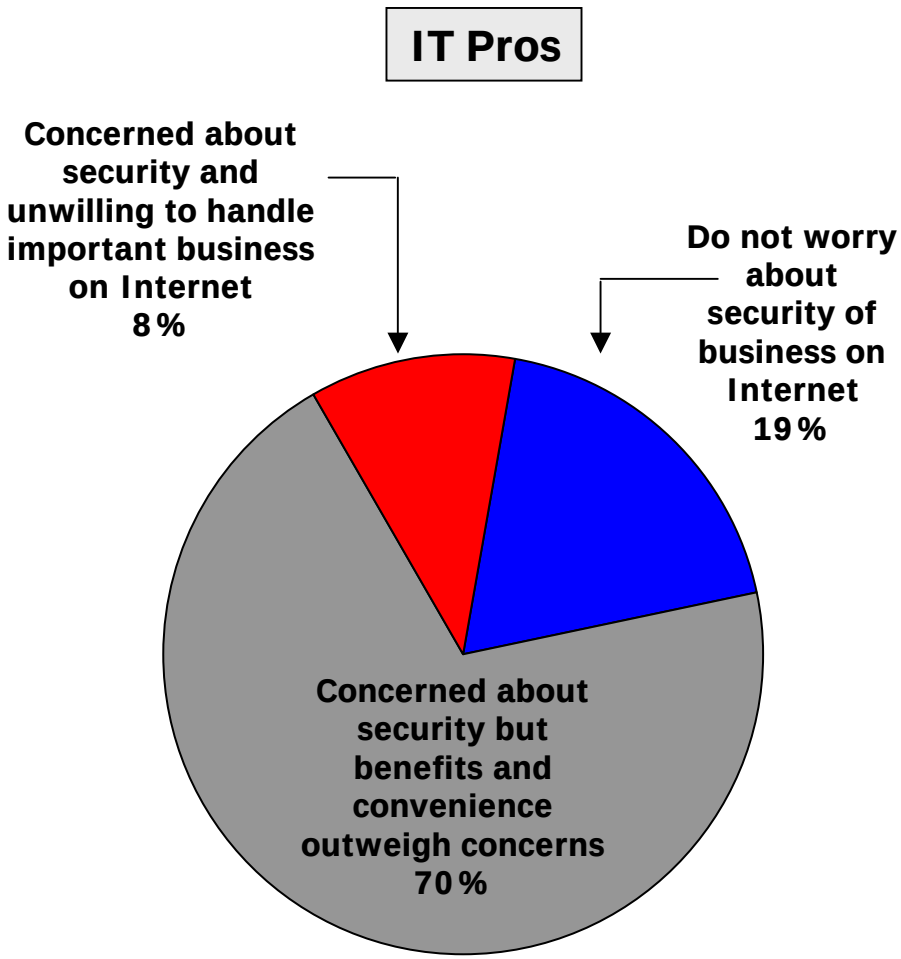
Do you think it is very safe, fairly safe, not very safe, or not at all safe to shop online with a credit card?

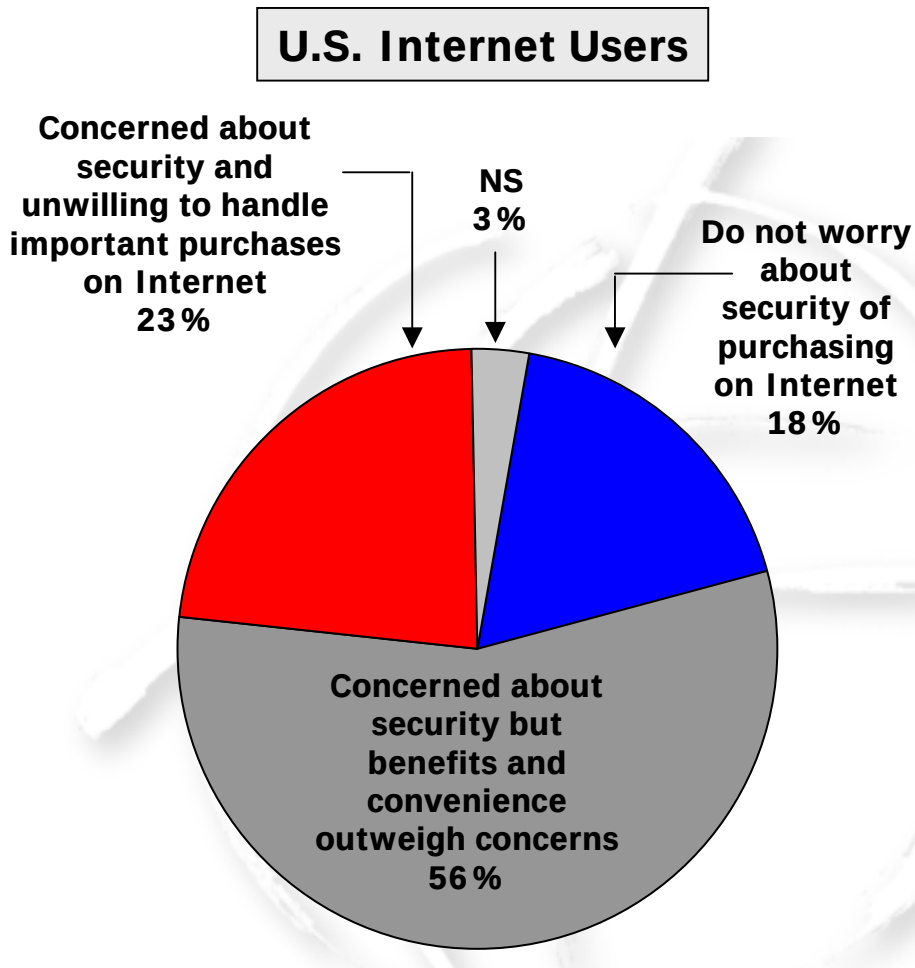
U.S. Internet Users



Weighing Concerns About E-Commerce

When it comes to *doing business / purchasing* on the Internet, which one of the following three statements comes closest to your view?

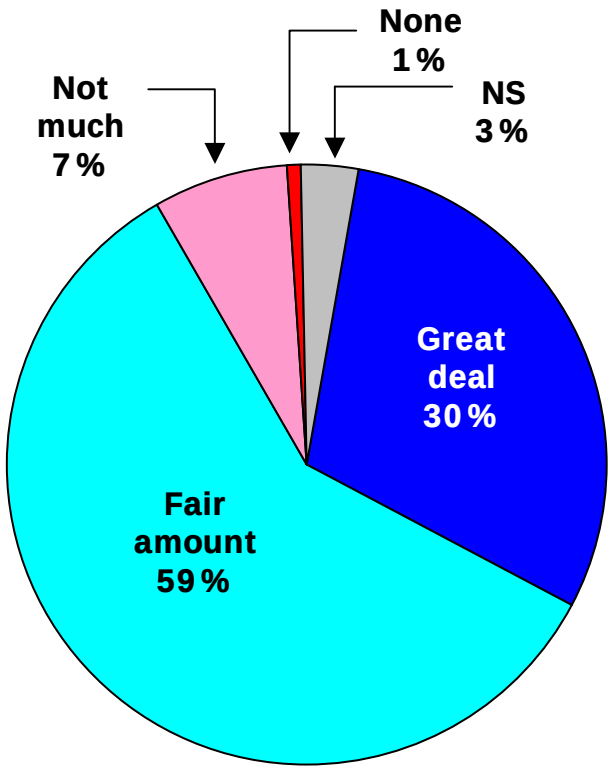




Confidence in Technology Industry

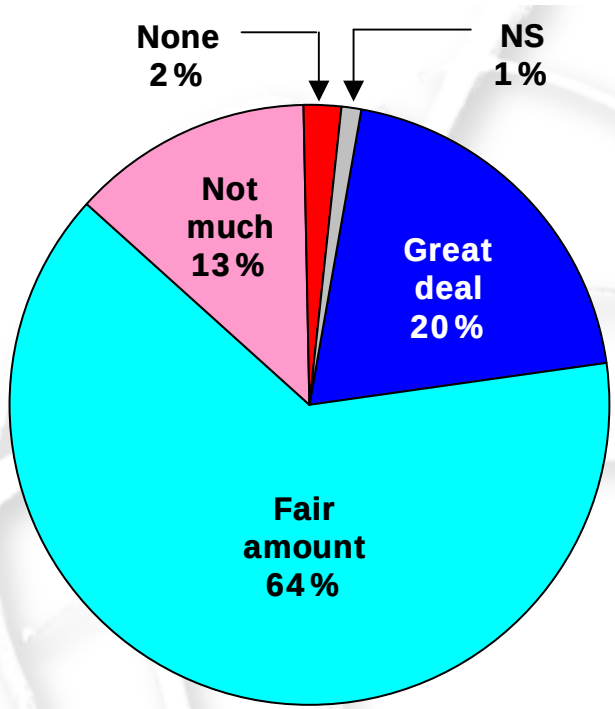
How much confidence do you have in the technology industry to develop tools to give *companies like yours / you* more control over your online security – a great deal, a fair amount, not much, or no confidence?

IT Pros



Total Confidence = *89%*
Total No confidence = *8 %*

U.S. Internet Users



Total Confidence = *84%*
Total No confidence = *15 %*

Methodology and Sample

Methodology

- Online interviews with 602 IT pros and 1,094 Internet users
- Telephone interviews with 1,000 adults
- Interviews completed between July 8 and July 15, 2002
- Margin of error: IT pros ± 4.1%; Internet users ± 3%; Adults ± 3.1%

Sample for IT pros study

- Company size:
  - Less than 100 employees: 25%
  - 100 to 500 employees: 13%
  - More than 500 employees: 60%
- Business Sector:
  - Manufacturing: 8%
  - Service: 18%
  - Technology: 35%
  - Sales: 5%
  - Government 11%
  - Other: 22%
- Level of involvement in purchasing or developing online security or cyber-security:
  - At least some input: 60%
  - No input: 39%
- Length of time as IT pro:
  - 5 years or less: 40%
  - 6 to 15 years: 30%
  - More than 15 years: 26%

Note: some numbers in charts may not add up due to rounding