

# BSA-ISSA Information Security Study

## Online Survey of ISSA Members



**December 3, 2003**

Research Conducted Between  
October 13 and October 29, 2003

# Key Findings

---

- I. A majority of security professionals believe that their organization is at risk of a major cyber attack
- II. Most security professional believe that despite the risk, their organization is prepared to defend against a major cyber attack
- III. Companies have taken steps to prepare themselves in order to keep their information secure. Some of these steps include:
  - A formal information security program function
  - New technologies that are either deployed or are planned for deployment within next 12 months
  - An active information security awareness and training program

# Key Findings

---

- IV. A majority of organizations have formal plans in place, such as:
- A documented business continuity plan covering personnel and facilities
  - A documented disaster recovery plan regarding critical business applications and supporting technology
- V. Senior management is increasingly aware of security issues and is taking information security seriously
- Once senior management gets involved, there is good chance of increased financial resources for improving information security within organization
- VI. Major challenges remain to get companies adequately prepared and information security programs implemented
- Lack of adequate of budgets, employee awareness, speed of change and sophistication of threats
  - Limited involvement of senior management in security information issues
  - Limited information security awareness and training programs for employees and non-employee users such as consultants or contractors

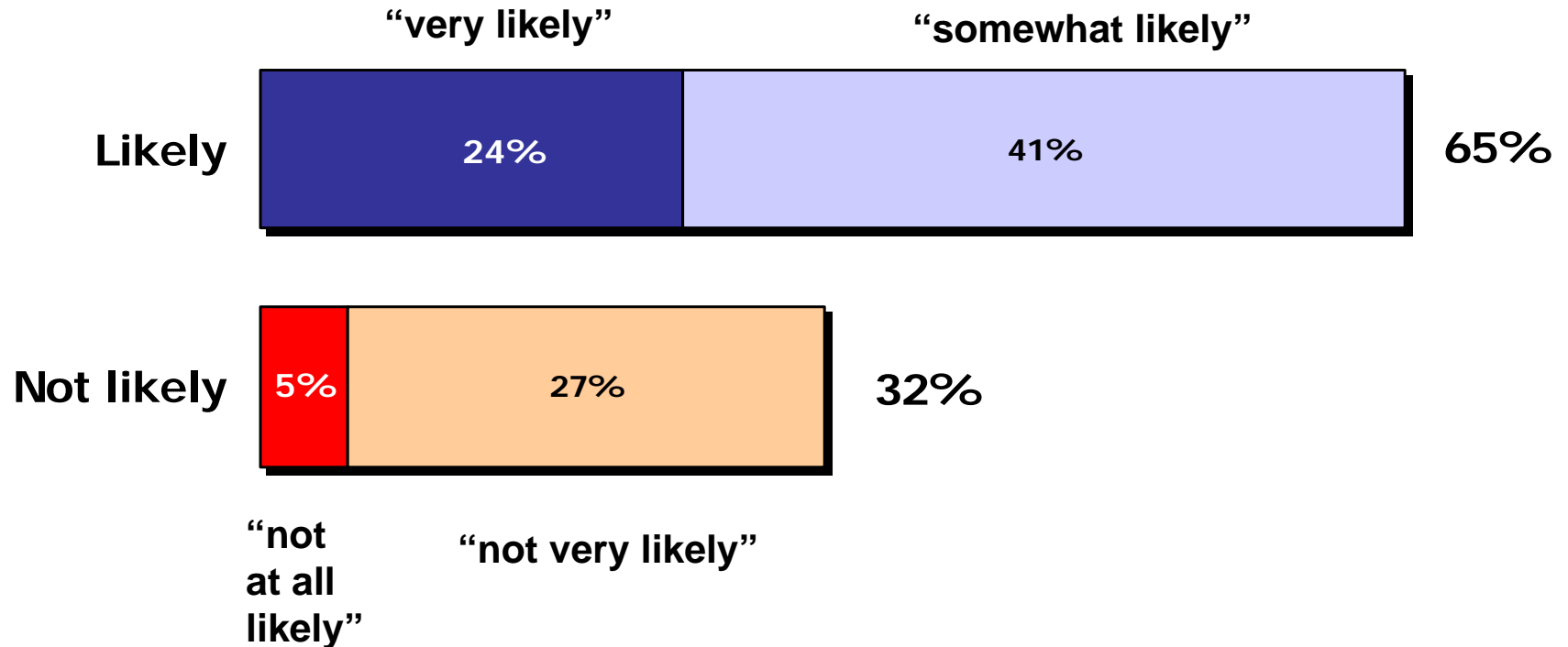
# Threats of Major Cyber Attack Real but Most Companies Prepared to Defend Themselves

---

- 2 of 3 security professionals (65%) say that the risk of a major cyber attack on their organization during the next 12 months is likely
  - 1 of 4 (24%) say the risk is “very likely”
- More than 3 of 4 security professionals (78%) say their organization is prepared to defend against a major cyber attack
  - Among those at the largest companies, more than 4 of 5 (84%) say their organization is prepared to defend against a major cyber attack

# 2 of 3 Security Professionals Say Risk of Major Cyber Attack Likely

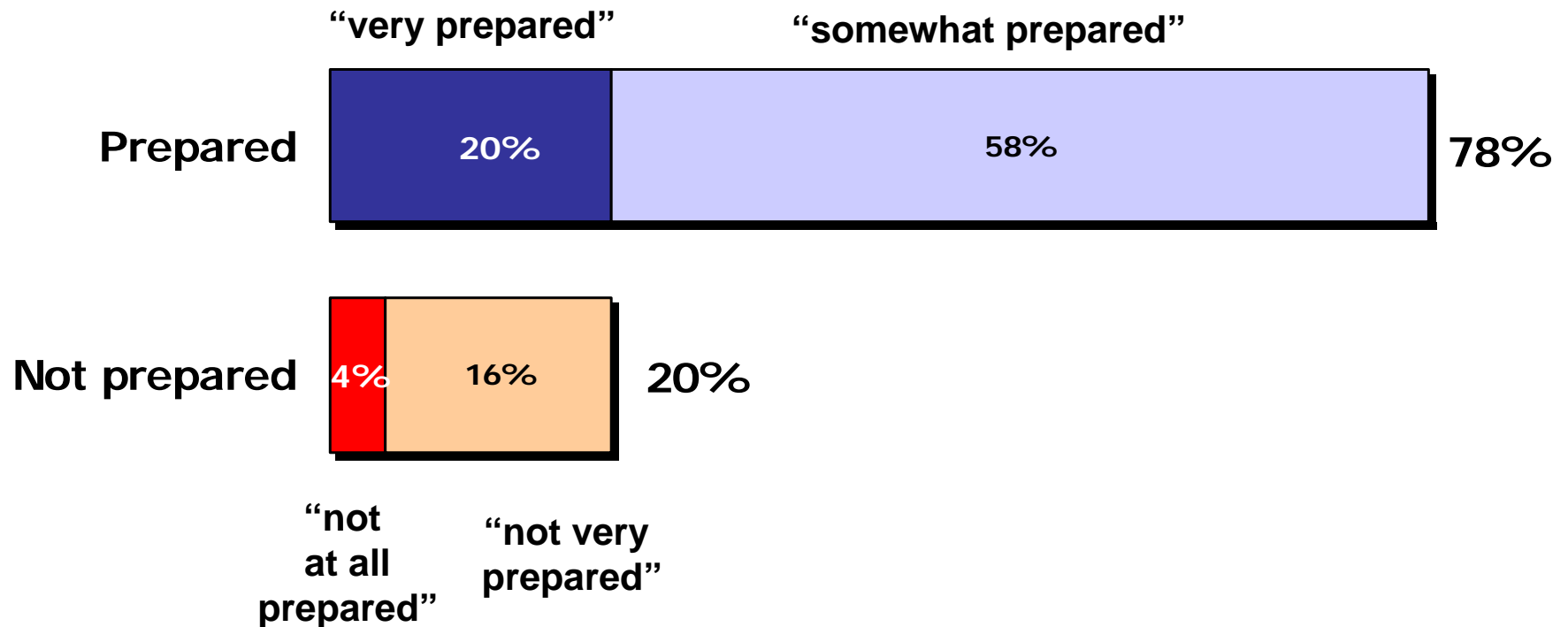
*Would you say the risk of a major cyber attack on your organization during the next 12 months is extremely likely, very likely, somewhat likely, not very likely, or not at all likely?*



# 3 of 4 Security Professionals Say Organization is Prepared to Defend Against Major Cyber Attack

---

*How prepared do you think your organization is to defend against a major cyber attack?*



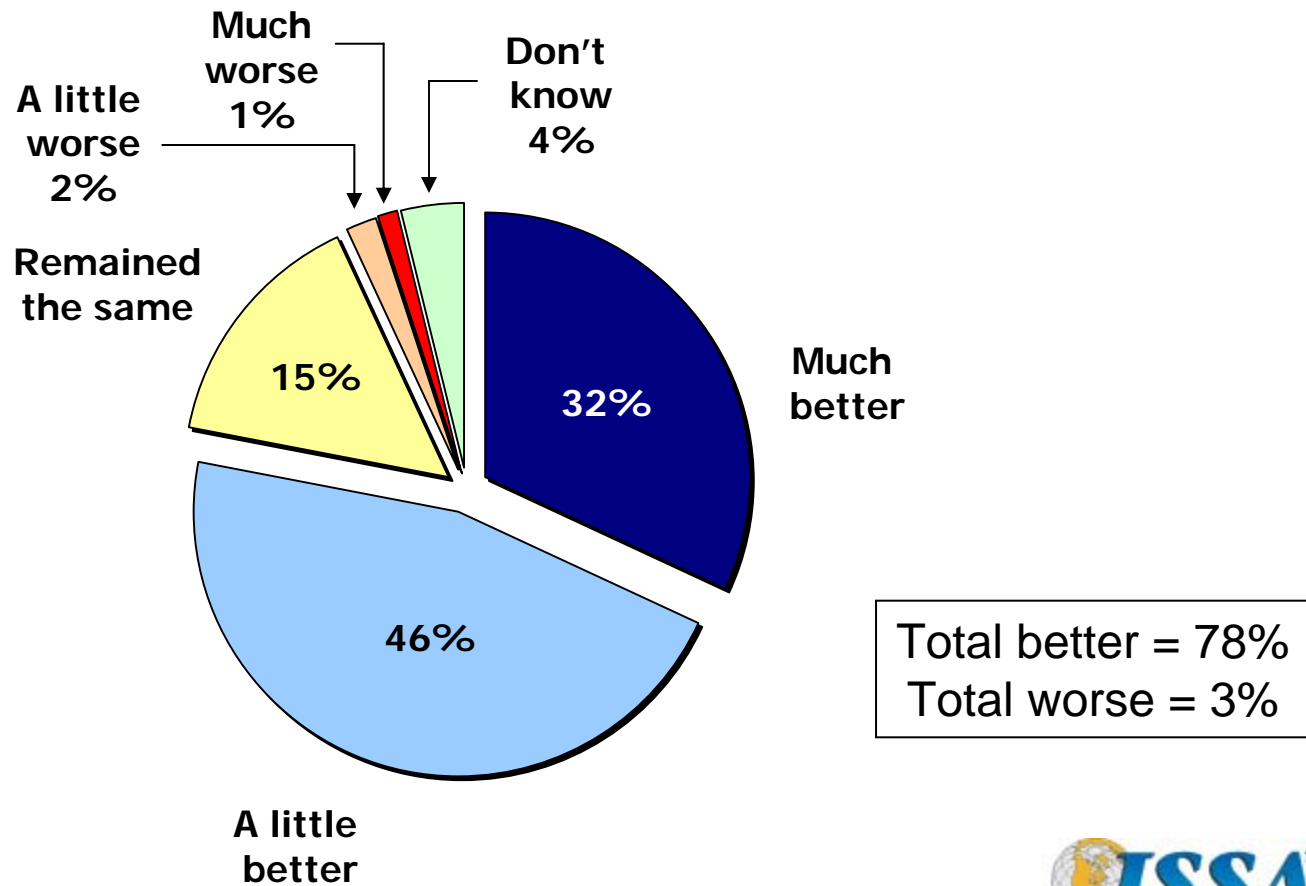
# Companies Are Improving Their Abilities to Defend Against Cyber Attacks

---

- More than 3 of 4 security professionals (78%) say that their organization's ability to defend itself against a major cyber attack has improved over the past 12 months
  - In fact, 1 of 3 (32%) say their company's ability to defend itself has gotten "much better" over the past 12 months
- 3 of 4 security professionals (76%) say that the recent threats and vulnerabilities have made their organization's capabilities to defend against a major cyber attack more secure
  - Among those at the largest companies, more than 4 of 5 (82%) say their companies are more secure
  - 1 of 5 (19%) say "much more secure"

# 3 of 4 Security Professionals Say Ability to Defend Against Major Cyber Attack Has Gotten Better

*Has the ability of your organization to defend itself against a major cyber attack gotten much better, a little better, remained the same, gotten a little worse or much worse over the past 12 months?*



# Organizations Have Begun to Put Formal Plans in Place to Build up Their Security Defenses

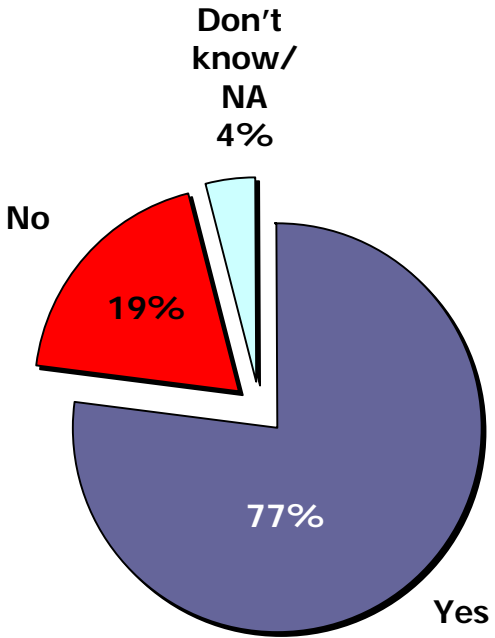
---

- Most organizations (77%) have a formal security program function in place, and of those companies that have a formal security program function, nearly all (96%) have that function approved by top management
  - The size of a company matters regarding the implementation of a formal security program function – in small companies (those with revenues under \$100 million) just over half (57%) have a formal information security function, whereas in the large companies (those with revenues over \$1billion) nearly all (93%) have a formal information security function
- Specific information security function practices include:

– Access controls	73%
– Written information security policy	72%
– Compliance with existing laws and regulations	66%
– Creation of organization and process to implement policy	59%
– Awareness and training program	57%
– Regular monitoring, reviewing and auditing	57%
– Business continuity planning	57%
– Risk assessment and risk management	56%

# Most Companies Have Formal Security Program Function

*Does your organization have a formal information security program function?*



**96% of companies with formal information security function have program approved by senior management**

*Which of the following practices is part of your information security program?*

Access controls	73%
Written information security policy	72%
Compliance with existing laws and regulations	66%
Creation of organization and process to implement policy	59%
Awareness and training program	58%
Monitoring, reviewing, and auditing	58%
Business continuity planning	57%
Risk assessment and risk management	56%
Life cycle management of products and processes	35%

# Organizations Have Implemented or Plan to Deploy an Array of New Technologies

---

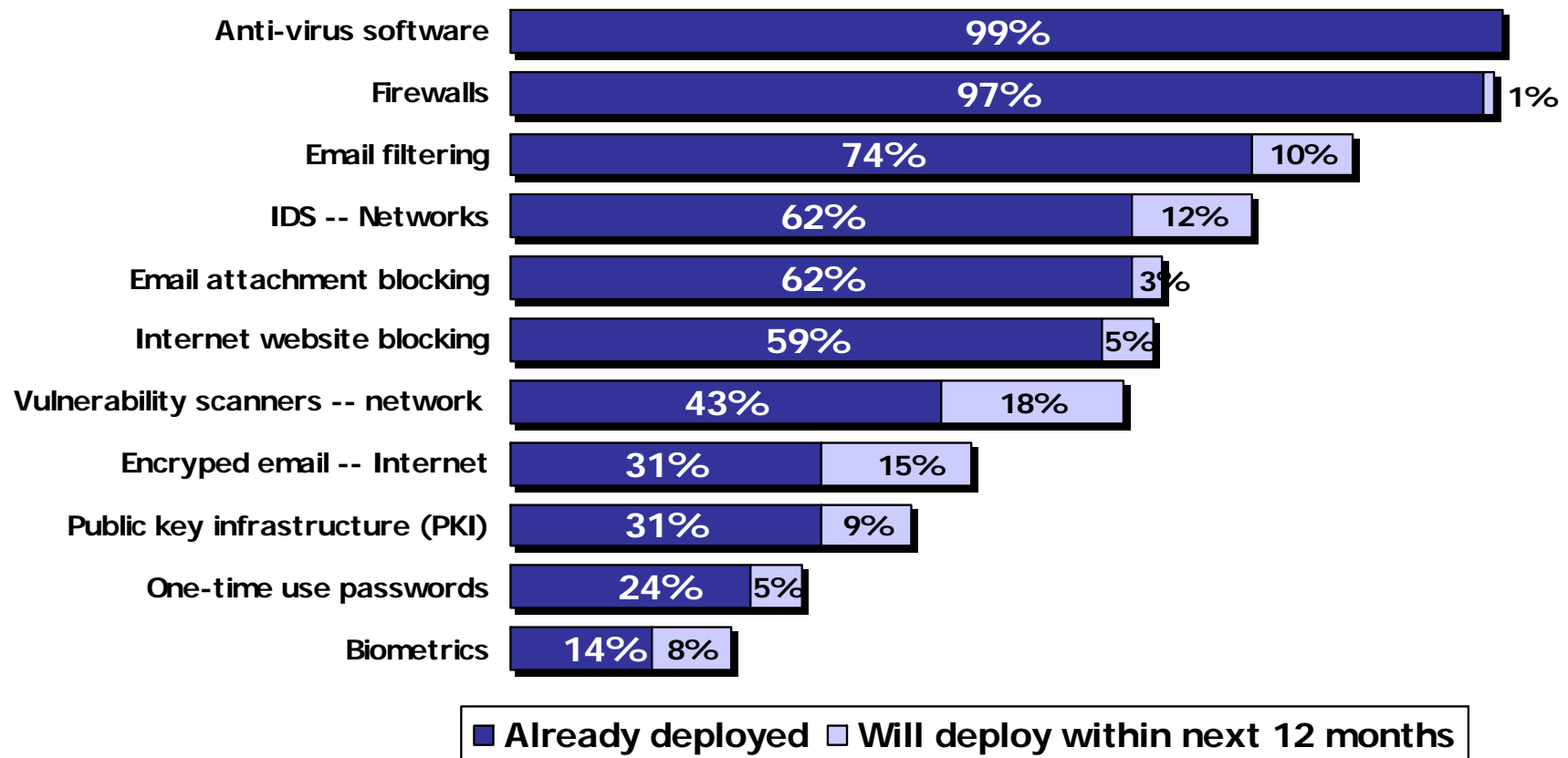
- New technologies either currently deployed or planned within the next 12 months include:

	<u>Currently Deployed</u>	<u>Plan to Deploy</u>
– Anti-virus software	99%	--
– Firewalls	97%	1%
– Email filtering	74%	10%
– Intrusion detection systems – network	62%	12%
– Email attachment blocking	62%	3%
– Internet website blocking	59%	5%
– Vulnerability scanners – network systems	43%	18%
– Encrypted email – Internet	31%	15%

- While even the smallest companies have anti-virus software and firewalls, for other information security technologies, there is a clear trend that the bigger the company, the more likely it has or plans to have these technologies deployed
- Additionally, most security professionals (87%), regardless of company size, say software security patches to known vulnerabilities are up-to-date

# Variety of Technologies Deployed/Planned to Keep Organization's Information Secure

*Which types of information security technologies are deployed/does your company plan to deploy within the next 12 months?*



# Companies Have Also Begun to Implement Various Personnel Security Measures

---

- More than half of security professionals (55%) say they have an active information security awareness and training program for all employees, including management
- For non-employee users, such as consultants, contractors, or temporary employees, however, this type of program exists in less than 1 of 3 (29%) companies
  - Larger companies are more likely to train both full time employees (64%) and non-employee users (34%) than smaller companies (46% and 23%, respectively)
- While the majority of security professionals (59%) say that they consider their company employees trained in their information duties and responsibilities, only 16% say their company employees are “adequately trained” and more than 1 of 3 (39%) say that their company employees are “not adequately trained”

# In the Event of a Successful Cyber Attack, Majority of Organizations Have Plan in Place

---

- More than half (61%) have documented business continuity plans covering personnel and facility issues
  - Among companies with less than \$100 million in revenue, only 43% have a business continuity plan in place, whereas among companies with over \$1 billion in revenue, 75% have such a plan in place
- Of those companies with a business continuity plan, 3 of 5 have tested the plan either within the past 6 months (42%) or between 6 months and 12 months ago (18%)
- Additionally, 2 of 3 organizations (67%) have a documented disaster recovery plan regarding critical business applications and supporting technology

# Few Companies Have Reported Cyber Incident to Law Enforcement or Other Government Agency

---

- Only 1 of 5 (19%) security professionals say their company has reported a cyber incident or intrusion to law enforcement or other government agency during the past year
  - Large companies (26%) are twice as likely as small companies (13%) to report a cyber incident or intrusion to law enforcement
- A strong majority (81%) of those companies who have reported a cyber incident or intrusion, however, have assisted law enforcement with the investigation

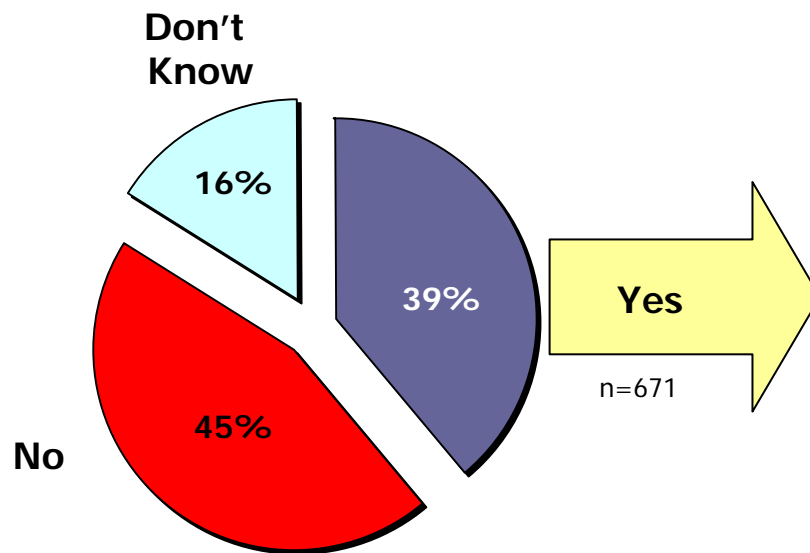
# Senior Management Aware of Security Issues and Taking Information Security Seriously

---

- About 2 of 3 security professionals (63%) say that their organization's top management receives periodic updates of the status of information security
- Fully half (53%) say their organization has a periodic review or audit of its information security function by an outside entity
  - 71% of companies earning more than \$1 billion, but only 29% of companies earning less than \$100 million
- About 2 of 5 (39%) say their organization treats information security as an issue that involves the active participation of the CEO and/or senior management and board of directors, resulting in regular risk assessment and reporting
- Of those organizations that do treat information security as an issue with the active involvement of executive management, nearly all (88%) say senior management would devote the resources and achieve the accountability necessary for better results

# Most Companies That Treat Information Security As Issue Involving Participation of Senior Management Devote Resources Necessary for Better Results

*Does your organization treat information security as an issue that involves the active participation of the Board, the CEO and/or senior management, resulting in regular risk assessment and reporting?*



*If your organization treats information security as an issue involving the active participation of executive management, regular risk assessment and reporting, how likely would it be to devote the resources and achieve the accountability necessary for better results?*

<b>Net: Likely</b>	<b>88%</b>
Very likely	36%
Somewhat likely	52%
<b>Net: Not likely</b>	<b>9%</b>
Not very likely	8%
Not at all likely	1%
Don't know	3%

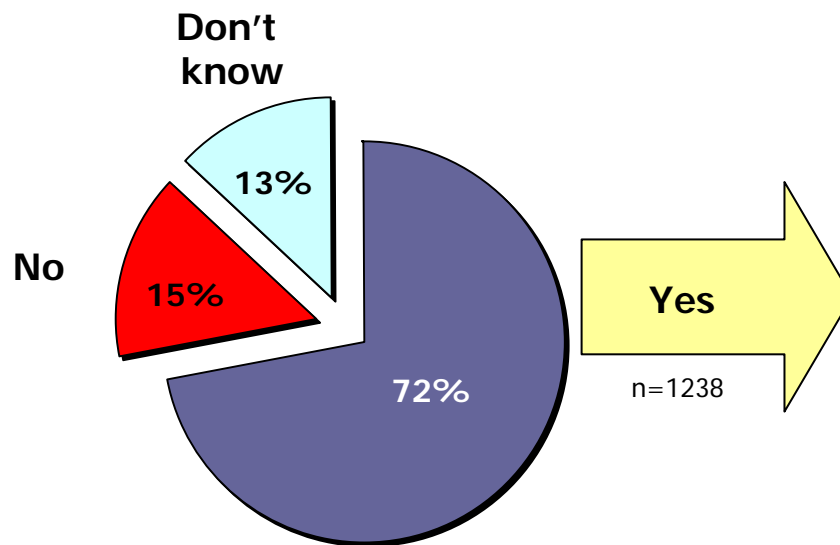
# Recent Cyber Threats Have Heightened Senior Management Awareness of Security Issues

---

- Nearly 3 of 4 security professionals (72%) say that the recent threats and vulnerabilities have increased awareness of security issues to the senior executive level in their organization
- Of those who say that senior management has been made aware of security issues:
  - 38% say financial resources for improving information security have increased
  - 48% say financial resources have stayed the same
  - Only 3% say financial resources have decreased once senior management has been made aware of security issues

# Majority Say Senior Executive Level Has Increased Awareness of Security Issues; Awareness Beginning to Have Positive Effect on Resources

*Have the recent cyber threats and vulnerabilities increased awareness of security issues to the senior executive level in your organization?*



*How has increased awareness of security issues to the senior level affected the financial resources for improving information security in your organization – have resources increased, decreased, or remained the same?*

Increased	38%
Decreased	3%
Remained the same	48%
Don't know	10%

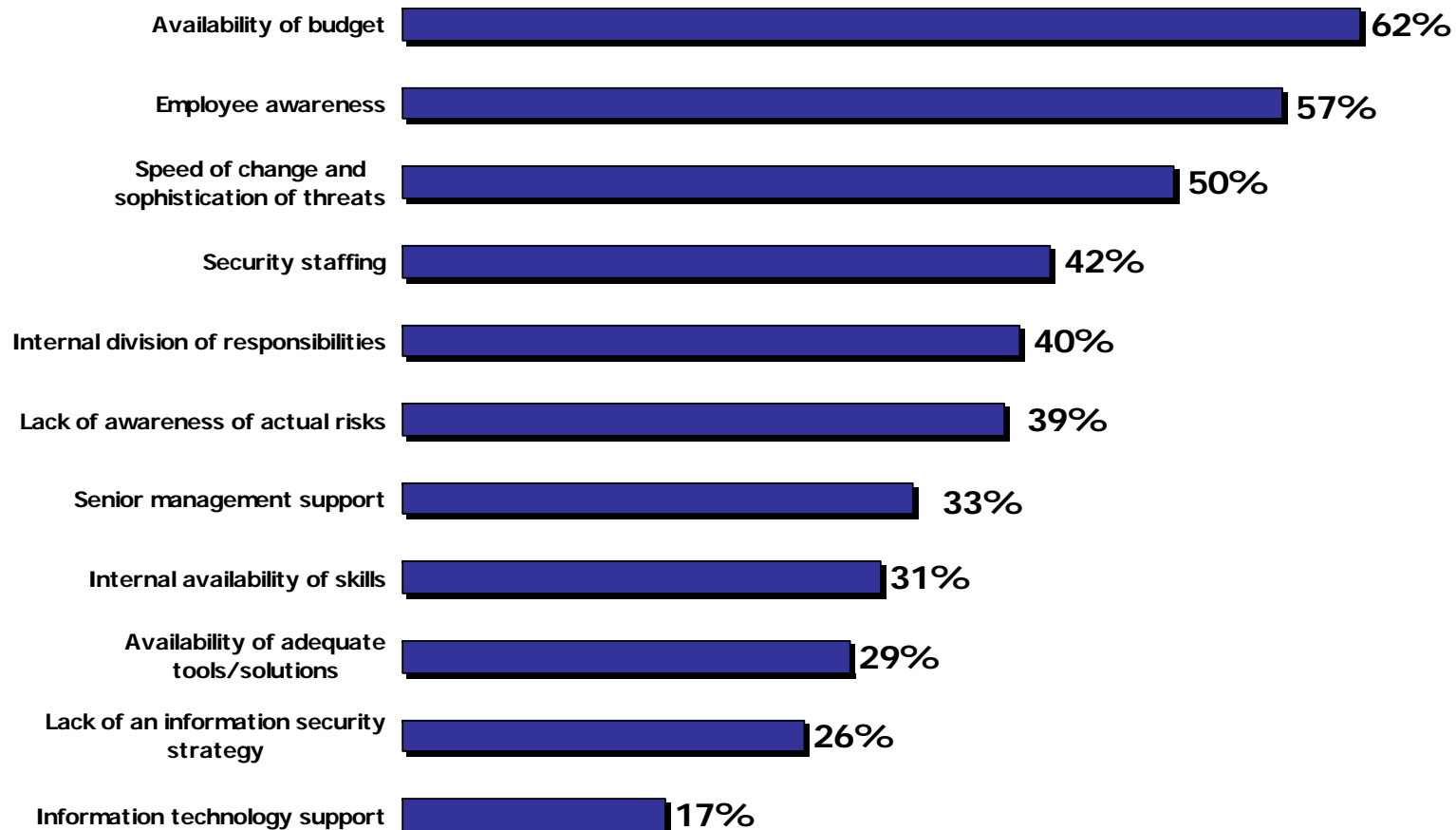
# Major Challenges Remain for Those Organizations Slow to Prepare for a Cyber Attack

---

- The three biggest challenges that organizations face in implementing an information security program are:
  - Availability of budget (62%)
  - Employee awareness (57%)
  - Speed of change and sophistication of threats (50%)
- Among smaller companies, availability of budget (66%) is far and away the most significant barrier. Other primary challenges include: employee awareness (47%), speed of change and sophistication of threats (45%), security staffing (37%), lack of awareness of actual risks (36%), senior management support (33%), and lack of an information security strategy (31%)
- Among larger companies, employee awareness (64%) is the most significant barrier. Other primary challenges include: availability of budget (58%), speed of change and sophistication of threats (54%), internal division of responsibilities (49%), and security staffing (47%)

# Companies Face Variety of Challenges in Implementing Information Security Program

*What are some of the primary challenges your organization faces in implementing an information security program?*



# Methodology and Sponsor Information

---

- Between October 13 and October 29, 2003 independent pollster, Andrew Stavisky, PhD, conducted online interviews with 1,716 members of the Information Systems Security Association (ISSA). The margin of error is  $\pm 2.4\%$ .
- The Business Software Alliance ([www.bsa.org](http://www.bsa.org)) is the foremost organization dedicated to promoting a safe and legal digital world. BSA is the voice of the world's commercial software industry and its hardware partners before governments and in the international marketplace. BSA programs foster technology innovation through education and policy initiatives that promote cyber security, copyright protection, trade and e-commerce.
- ISSA is the largest, international non-profit association specifically for security professionals. Its more than 10,000 worldwide members include practitioners at all levels of the security field in a broad range of industries, such as communications, education, healthcare, manufacturing, financial and government.

# Respondent Profile

## Organization Size

- 1 – 100 20%
- 100 – 999 21%
- 1,000 – 9,999 29%
- 10,000 or more 29%

## Organization Yearly Gross Revenue

- Less than \$100 million 30%
- \$100 million to \$1 billion 21%
- More than \$1 billion 25%
- Don't know 23%

## Tenure As Information Security Pro

- Less than 5 years 45%
- 6 – 10 years 30%
- More than 10 years 25%

## Industry Group

- Financial/Banking/Accounting 15%
- IT/Computer services 12%
- Consulting/Auditing 11%
- Government, Fed/State/Local 11%
- High-tech/Software/Hardware 7%
- Medicine/Healthcare/Pharma 7%
- Education 5%
- Insurance 4%
- Energy/Utilities/Electricity/Gas 3%
- Manufacturing/Chemical 3%
- Telecommunications 3%
- Aerospace 2%
- Internet/ISP/Web 2%
- Military/Defense 2%
- Retail/Wholesale/Distribution 2%