IT Security: Perceptions, Awareness, and Practices

computer economics

Leveraging IT Investments

5841 Edison Place, Carlsbad, CA 92008
Phone: 760-438-8100 Fax: 760-431-1126
Email: info@compecon.com
Website: computereconomics.com

TABLE OF CONTENTS

CHAPTER 1 — EXECUTIVE SUMMARY

Computer Economics developed and conducted a survey on IT security perceptions, awareness, and practices during May and June of 2002. We collected factual information about security management, policies, and practices. We also sought the opinions of executive managers, chief technology officers, and IS security managers and professionals about the state of security and the expectation of cyber attacks. Key findings from the survey include the following.

On the State of Security:

- 76.9% think IT security has improved in their organization during the last year.
- 85.5% think virus protection software in their organization is updated frequently enough.
- 79.8% think that the computer industry as a whole has NOT done enough to address security for IT products.
- 80.3% think that Microsoft has NOT done enough to address security for its products.
- 74.4% think that the government in their country has NOT done enough to address information systems security.

On Expectations About Cyber Attacks:

- 69.6% think that large-scale cyber attacks by terrorists will occur in less than two years.
- 48.4% think that large-scale cyber attacks by a military will occur in less than two years.
- 80.1% think that their country is NOT prepared to deal with large-scale cyber attacks.
- 57.1% think that their organization is NOT prepared to deal with large-scale cyber attacks.

On Security Management:

- 36.8% do NOT have an IS security director in their organization.
- 51.8% have NOT contracted with an IT security consulting firm during the last year.
- 23.7% spend less than 1% of their IT budget on security staff and products.
- The ratio of IS security staff to total employees is very low.

On Security Policy:

- 71.1% have written IT security policies in place.
- 49.1% have written IT security incident response procedures in place.
- 72.4% have written privacy policies covering customer and corporate data in place.
- 72.8% have written policies on appropriate use of information systems, networks, and email and inform employees of these policies.
- 56.3% require employees to sign statements that they understand the information systems security policies and will abide by them.

On Enforcing Security Policies:

- 36.8% use desktop warning banners to reinforce appropriate use of systems.
- 48.0% have terminated employees for misuse of computers or networks.
- 27.0% have reported a security breach to law enforcement.
- 56.1% have conducted IT security or virus protection training with employees.

On Testing Security:

- 65.7% have conducted vulnerability audits.
- 65.1% have conducted intrusion tests.

On the Cost of Incidents:

- 49.1% do not know how much intrusions and/or hacking incidents cost their organization during the last 12 months.
- 39.3% do not know how much virus and worm attacks cost their organization during the last 12 months.

CHAPTER 2 — INTRODUCTION

Through consultations and discussions with executive managers, chief technology officers, IS security managers and professionals, and law enforcement investigators Computer Economics developed this survey during May and June of 2002. We collected factual information about security management, policies, and practices. We also sought the opinions of executive managers, chief technology officers, and IS security managers and professionals about the state of security and the expectation of cyber attacks.

For many years, the General Accounting Office (GAO) had found weaknesses in the information systems of United States government agencies. To gain a broader understanding of how security programs can be successfully implemented, the GAO studied the management practices of eight nonfederal organizations to identify the management framework that the organizations had established. The GAO study was designed to provide organizations around the world with a look at how organizations can reorient their security programs to make them visible, integral components of their business operations. The organizations studied had adopted five principles of risk management:

1. Assess risk and determine needs
2. Establish a central management focus on risks and security
3. Implement appropriate policies and related controls
4. Promote awareness
5. Monitor and evaluate policy and control effectiveness.

The questions in the Computer Economics survey on IT security perceptions, awareness, and practices were designed, in part, to determine to what extent the five principles of risk management are being implemented.

Organization of the Report

The State of Security section reports on opinions of executive managers, chief technology officers, and IS security managers and professionals toward improvements in security in their organizations, IT industry efforts on improving security, and actions that governments have taken to address IT security.

The section on *Expectations About Cyber Attacks* also reports on opinions of executive managers, chief technology officers, and IS security managers and professionals. The survey questions focused on when they expect large-scale cyber attacks as well as their views on the level of current preparedness to deal with cyber attacks.

The *Security Management* section examines how organizations manage and staff security operations as well as how much money they spend on IT security. The *Security Policy* section examines where security policies are in place and where they are lacking.

The section on *Enforcing Security Policies* addresses how organizations are using desktop banners, training of employees and termination of abuser to enforce IT security policies. This section also covers the practice of reporting incidents to law enforcement.

The section on *Testing Security* examines the use of intrusion testing and vulnerability audits. The *Cost of Incidents* section examines what organizations know about the cost of incidents and what it has cost to recover from malicious attacks.

About the Participants

There were 233 participants in the survey. Virtually all of the organizations represented (99.1%) are connected to the Internet and have a website (96.7%). The majority of the responders are in IT positions, with the largest single group being information systems security managers. The job function of the responders is shown in Figure 2-1.

FIGURE 2-1

Job Function

Job Function	Percent of Organizations
Executive management	16.4%
Information systems management	15.5
Information systems staff	12.8
Information systems security management	18.3
Information systems security staff	10.5
Department management	4.6
Department staff	2.3
Enterprise security	5.9
Other	13.7

About six out of ten responders are located in the United States. The region or country where the responder works is shown in Figure 2-2. As we analyzed data we found little difference in perceptions, awareness, and practices in IT security from region to region.

FIGURE 2-2

Region/Country

Region/Country	Percent of Organizations
United States	61.6%
Canada	3.7
Asia/Pacific	12.0
Central/South America	3.7
Europe	16.7
Middle East/Africa	2.3

The industry sector that is most represented among the responders is professional services (33.5%) followed by government (16.5%) and then by banking, finance, and insurance (14.6%). The industry sector in which the responders are employed is shown in Figure 2-3.

FIGURE 2-3

Industry Sector

Industry Sector	Percent of Organizations
Banking, Finance, and Insurance	14.6%
Education	6.6
Government	16.5
Healthcare	4.7
Manufacturing	11.3
Professional Services	33.5
Retail/Wholesale Distribution	6.1
Trade Services	2.8
Transportation and Utilities	3.8

Survey respondents working in organizations with less than 25 employees represent 17.9% of the participants, while 19.8% work in organizations with over 10,000 employees. The number of employees in the organization in which the responder is employed is shown in Figure 2-4.

FIGURE 2-4

Number of Employees in the Organization

Number of Employees	Percent of Organizations
Less than 25	17.9%
26 to 50	5.2
51 to 100	9.0
101 to 250	8.5
251 to 500	7.5
501 to 1,000	6.6
1,001 to 2,000	7.5
2,001 to 5,000	9.9
5,001 to 10,000	8.0
Over 10,000	19.8

Responders working in organizations with under $1,000,000 in annual revenue represent 22.3% of the participants, while 21.3% work in organizations with over $1 billion in annual revenue. The annual revenue of the organization in which the responder is employed is shown in Figure 2-5.

FIGURE 2-5

Annual Revenue of Organizations

Annual Revenue	Percent of Organizations
Under $1,000,000	22.3%
$1,000,001 to $5,000,000	10.2
$5,000,001 to $10,000,000	6.6
$10,000,001 to $20,000,000	11.7
$20,000,001 to $50,000,000	8.1
$50,000,001 to $100,000,000	9.1
$100,000,001 to $1 Billion	10.7
Over $1 Billion	21.3

CHAPTER 3 — THE STATE OF SECURITY

History has shown that complacency courts disaster. Thus, in an age of increasing security threats it is important to examine how people perceive the state of IT security to determine if they are in fact giving security enough attention. Key points extracted from the analysis of perceptions toward security include the following:

- 76.9% think IT security has improved in their organization during the last year.
- 85.5% think virus protection software in their organization is updated frequently enough.
- 79.8% think that the computer industry as a whole has NOT done enough to address security for products.
- 80.3% think that Microsoft has NOT done enough to address security for its products.
- 74.4% think that the government in their country has NOT done enough to address information systems security.

IT Security Improvements

The majority of respondents (76.9%) think IT security has improved in their organization during the last year. Figure 3-1 shows the responses to the question: Do you think that information systems security has improved in your organization during the last year?

FIGURE 3-1

Has IT Security Improved?

Response	Percent of Respondents
Yes	76.9%
No	14.4
Don't Know	8.7

IS managers and IS security staff are the least likely to think IT security has improved in their organization during the last year. IS managers comprise only 15.5% of the total respondents and IS security staff comprise only 10.5% of the total respondents. However, of those who think IT security has NOT improved in their organization during the last year 32.1% were IS managers and 17.9% were IS security staff. Figure 3-2 shows the breakdown of the respondents who think that IS security has NOT improved in their organization during the last year.

FIGURE 3-2

Think IT Security Has NOT Improved

Job Function	Percent of Total Respondents	Percent of Respondents Who Think Security in Their Organization Has NOT Improved
Executive management	16.4%	7.1%
Information systems management	15.5	32.1
Information systems staff	12.8	10.7
Information systems security management	18.3	10.7
Information systems security staff	10.5	17.9
Department management	4.6	0.0
Department staff	2.3	3.6
Enterprise security	5.9	3.6
Other	13.7	14.3
Industry Sector		
Banking, Finance, and Insurance	14.6	10.7
Education	6.6	7.1
Government	16.5	10.7
Healthcare	4.7	0.0
Manufacturing	11.3	14.2
Professional Services	33.5	50.0
Retail/Wholesale Distribution	6.1	3.6
Trade Services	2.8	0.0
Transportation and Utilities	3.8	3.6
Number of Employees		
Less than 25	17.9	10.7
26 to 50	5.2	3.6
51 to 100	9.0	14.3
101 to 250	8.5	10.7
251 to 500	7.5	0.0
501 to 1,000	6.6	10.7
1,001 to 2,000	7.5	10.7
2,001 to 5,000	9.9	7.1
5,001 to 10,000	8.0	10.7
Over 10,000	19.8	21.4

FIGURE 3-2

Think IT Security Has NOT Improved—*Continued*

Annual Revenue	Percent of Total Respondents	Percent of Respondents Who Think Security in Their Organization Has NOT Improved
Under $1,000,000	22.3	12.0
$1,000,001 to $5,000,000	10.2	12.0
$5,000,001 to $10,000,000	6.6	8.0
$10,000,001 to $20,000,000	11.7	12.0
$20,000,001 to $50,000,000	8.1	4.0
$50,000,001 to $100,000,000	9.1	16.0
$100,000,001 to $1 Billion	10.7	16.0
Over $1 Billion	21.3	20.0

The majority of respondents (85.5%) think virus protection software in their organization is updated frequently enough. Figure 3-3 shows the responses to the question: Do you think that the virus protection software in your organization is updated frequently enough?

FIGURE 3-3

Is Virus Protection Software Updated Frequently Enough?

Response	Percent of Respondents
Yes	85.5%
No	13.4
Don't Know	1.2

IS managers and staff in functional departments are the least likely to think virus protection software is updated frequently enough. IS managers comprise only 15.5% of the total respondents. However, of those who think virus protection software is NOT updated frequently enough 25.0% were IS managers. Figure 3-4 shows the breakdown of the respondents who think that virus protection software is NOT updated frequently enough in their organization.

FIGURE 3-4

Think Virus Protection Software Is NOT Updated Frequently Enough

Job Function	Percent of Total Respondents	Percent of Respondents Who Think Virus Protection Is NOT Updated Frequently Enough
Executive management	16.4%	16.7%
Information systems management	15.5	25.0
Information systems staff	12.8	8.3
Information systems security management	18.3	16.7
Information systems security staff	10.5	4.2
Department management	4.6	0.0
Department staff	2.3	8.3
Enterprise security	5.9	4.2
Other	13.7	16.7
Industry Sector		
Banking, Finance, and Insurance	14.6	12.5
Education	6.6	12.5
Government	16.5	16.7
Healthcare	4.7	8.3
Manufacturing	11.3	4.2
Professional Services	33.5	29.2
Retail/Wholesale Distribution	6.1	4.2
Trade Services	2.8	8.3
Transportation and Utilities	3.8	4.2
Number of Employees		
Less than 25	17.9	20.8
26 to 50	5.2	8.3
51 to 100	9.0	8.3
101 to 250	8.5	12.5
251 to 500	7.5	16.7
501 to 1,000	6.6	4.2
1,001 to 2,000	7.5	8.3
2,001 to 5,000	9.9	12.5
5,001 to 10,000	8.0	4.2
Over 10,000	19.8	4.2
Annual Revenue		
Under $1,000,000	22.3	30.0
$1,000,001 to $5,000,000	10.2	25.0
$5,000,001 to $10,000,000	6.6	15.0
$10,000,001 to $20,000,000	11.7	5.0
$20,000,001 to $50,000,000	8.1	0.0
$50,000,001 to $100,000,000	9.1	10.0
$100,000,001 to $1 Billion	10.7	5.0
Over $1 Billion	21.3	10.0

IT Industry Efforts to Improve Security

The majority of respondents (79.8%) think that the computer industry as a whole has NOT done enough to address security for IT products. Figure 3-5 shows the responses to the question: Do you think that the computer industry as a whole has done enough to address security for IT products?

FIGURE 3-5

Has the Computer Industry Done Enough to Address Security for IT Products?

Response	Percent of Respondents
Yes	15.0%
No	79.8
Don't Know	5.2

IS security managers and executive managers are the most likely to think that the computer industry as a whole has done enough to address security for IT products. IS security managers comprise only 18.3% of the total respondents and executive managers comprise only 16.4% of the total respondents. However, of those who think that the computer industry as a whole has done enough to address security for products, 27.6% were IS security managers and 20.7% were executive managers. Figure 3-6 shows the breakdowns of the respondents who think that the computer industry as a whole has done enough to address security for IT products.

Respondents who work in organizations with under $1,000,000 in annual revenue comprise 22.3% of the total. However, of those who think that the computer industry as a whole has done enough to address security for IT products, 40.7% work in organizations with under $1,000,000 in annual revenue.

FIGURE 3-6

Has the Computer Industry Done Enough to Address Security for IT Products?

Job Function	Percent of Total Respondents	Percent of Respondents Who Think That the Computer Industry as a Whole Has Done Enough to Address Security for IT Products
Executive management	16.4%	20.7%
Information systems management	15.5	17.2
Information systems staff	12.8	13.8
Information systems security management	18.3	27.6
Information systems security staff	10.5	6.9
Department management	4.6	0.0
Department staff	2.3	3.4
Enterprise security	5.9	0.0
Other	13.7	10.3
Industry Sector		
Banking, Finance, and Insurance	14.6	21.5
Education	6.6	3.6
Government	16.5	21.4
Healthcare	4.7	3.6
Manufacturing	11.3	7.2
Professional Services	33.5	32.1
Retail/Wholesale Distribution	6.1	3.6
Trade Services	2.8	7.1
Transportation and Utilities	3.8	0.0
Number of Employees		
Less than 25	17.9	17.2
26 to 50	5.2	3.4
51 to 100	9.0	10.3
101 to 250	8.5	6.9
251 to 500	7.5	13.8
501 to 1,000	6.6	6.9
1,001 to 2,000	7.5	6.9
2,001 to 5,000	9.9	13.8
5,001 to 10,000	8.0	3.4
Over 10,000	19.8	17.2
Annual Revenue		
Under $1,000,000	22.3	40.7
$1,000,001 to $5,000,000	10.2	0.0
$5,000,001 to $10,000,000	6.6	7.4
$10,000,001 to $20,000,000	11.7	3.7
$20,000,001 to $50,000,000	8.1	14.8
$50,000,001 to $100,000,000	9.1	11.1
$100,000,001 to $1 Billion	10.7	11.1
Over $1 Billion	21.3	11.1

As shown in Figure 3-7 the majority of respondents (80.3%) think that Microsoft has NOT done enough to address security for its products. Only a slim 11.9% think that Microsoft has done enough. Figure 3-8 shows a breakdown of those who think Microsoft has done enough to address security for its products.

FIGURE 3-7

Has Microsoft Done Enough to Address Security for Its Products?

Response	Percent of Respondents
Yes	11.9%
No	80.3
Don't Know	87.8

FIGURE 3-8

Has Microsoft Done Enough to Address Security for Its Products?

Job Function	Percent of Total Respondents	Percent of Respondents Who Think That Microsoft Has Done Enough to Address Security for Its Products
Executive management	16.4%	16.7%
Information systems management	15.5	12.5
Information systems staff	12.8	16.7
Information systems security management	18.3	25.0
Information systems security staff	10.5	4.2
Department management	4.6	0.0
Department staff	2.3	0.0
Enterprise security	5.9	4.2
Other	13.7	20.8
Industry Sector		
Banking, Finance, and Insurance	14.6	17.4
Education	6.6	0.0
Government	16.5	21.7
Healthcare	4.7	4.3
Manufacturing	11.3	21.7
Professional Services	33.5	34.8
Retail/Wholesale Distribution	6.1	0.0
Trade Services	2.8	0.0
Transportation and Utilities	3.8	0.0
Number of Employees		
Less than 25	17.9%	16.7%
26 to 50	5.2%	8.3%
51 to 100	9.0	12.5
101 to 250	8.5	8.3
251 to 500	7.5	16.7
501 to 1,000	6.6	0.0
1,001 to 2,000	7.5	4.2
2,001 to 5,000	9.9	8.3
5,001 to 10,000	8.0	0.0
Over 10,000	19.8	25.0
Annual Revenue		
Under $1,000,000	22.3	39.1
$1,000,001 to $5,000,000	10.2	4.3
$5,000,001 to $10,000,000	6.6	13.0
$10,000,001 to $20,000,000	11.7	8.7
$20,000,001 to $50,000,000	8.1	17.4
$50,000,001 to $100,000,000	9.1	0.0
$100,000,001 to $1 Billion	10.7	8.7
Over $1 Billion	21.3	8.7

Government Efforts to Improve Security

The majority of respondents (74.4%) think that the government in their country has NOT done enough to address information systems security. Figure 3-9 shows the responses to the question: Do you think that the government in your country has done enough to address information systems security?

FIGURE 3-9

Has the Government in Your Country Done Enough to Address IT Security?

Response	Percent of Respondents
Yes	17.9%
No	74.4
Don't Know	7.7

IS staff and management represent the largest portion of the 17.9% of respondents who think the government in their country has done enough to address IT security. As shown in Figure 3-10, a higher percentage of IS staff and managers think the government in their country has done enough to address IT security than makeup their portion of the total respondents. Information systems staff, for example, are 12.8% of total respondents but represent 21.1% of those who think the government in their country has done enough to address IT security.

FIGURE 3-10

Has the Government in Your Country Done Enough to Address IT Security?

Job Function	Percent of Total Respondents	Percent of Respondents Who Think the Government in Their Country Has Done Enough to Address IT Security
Executive management	16.4%	13.2%
Information systems management	15.5	21.1
Information systems staff	12.8	21.1
Information systems security management	18.3	21.1
Information systems security staff	10.5	5.3
Department management	4.6	5.3
Department staff	2.3	0.0
Enterprise security	5.9	2.6
Other	13.7	10.5
Industry Sector		
Banking, Finance, and Insurance	14.6	7.9
Education	6.6	5.3
Government	16.5	21.1
Healthcare	4.7	7.9
Manufacturing	11.3	21.1
Professional Services	33.5	18.4
Retail/Wholesale Distribution	6.1	7.9
Trade Services	2.8	7.9
Transportation and Utilities	3.8	2.6
Number of Employees		
Less than 25	17.9	10.8
26 to 50	5.2	0.0
51 to 100	9.0	5.4
101 to 250	8.5	10.8
251 to 500	7.5	13.5
501 to 1,000	6.6	5.4
1,001 to 2,000	7.5	5.4
2,001 to 5,000	9.9	13.5
5,001 to 10,000	8.0	10.8
Over 10,000	19.8	24.3
Annual Revenue		
Under $1,000,000	22.3	25.7
$1,000,001 to $5,000,000	10.2	5.7
$5,000,001 to $10,000,000	6.6	2.9
$10,000,001 to $20,000,000	11.7	11.4
$20,000,001 to $50,000,000	8.1	14.3
$50,000,001 to $100,000,000	9.1	5.7
$100,000,001 to $1 Billion	10.7	5.7
Over $1 Billion	21.3	28.6

The majority of respondents from outside the United States (40.0%) do not know if the United States has taken action that will improve the ability of their country to address information systems security. As shown in Figure 3-11, 39.0% of the respondents think that United States has NOT taken action that will improve the ability of their country to address information systems security. Twenty-one percent of the respondents think that the United States has taken action that will improve the ability of their country to address information systems security.

FIGURE 3-11

Has the United States Taken Action That Will Improve the Ability of Your Country to Address Information Systems Security?

Response	Percent of Respondents
Yes	21.0%
No	39.0
Don't Know	40.0

Of the 39% of responders who do NOT think the United States has taken action that will improve the ability of their country to address information systems security, 47.1% are employed in professional services while only 32.9% of the total responders are employed in professional services. Again only responses from outside the United States are counted in this part of the analysis.

In addition, of the 39% of responders who do NOT think the United States has taken action that will improve the ability of their country to address information systems security, 80% think that the government in their country has NOT done enough to address information systems security.

CHAPTER 4 — EXPECTATIONS ABOUT CYBER ATTACKS

The theft of national security information from a government agency or the interruption of electrical power to a major metropolitan area obviously would have greater consequences for national security, public safety, and the economy than the defacement of a website. But even the less serious categories have real consequences and, ultimately, can undermine public confidence in web-based commerce and violate privacy or property rights. An attack on a website that closes down an e-commerce site can have disastrous consequences for a web-based business. An intrusion that results in the theft of millions of credit card numbers from an online vendor can result in significant financial loss and, more broadly, reduce consumers' willingness to engage in e-commerce.

When Large-Scale Cyber Attacks Will Occur

Because of the news coverage about cyber attacks and the various alerts by the FBI, we decided to ask survey respondents about their views on cyber attacks. It appears that most people have received the message about cyber threats. There were two related questions as to when cyber attacks would occur:

- When do you think that large-scale cyber attacks will be launched by military organizations?
- When do you think that large-scale cyber attacks will be launched by terrorists?

Considerably more people think that large-scale cyber attacks launched by terrorists will occur in less than two years (69.6%) than think that large-scale cyber attacks will be launched by a military in less than two years (48.4%). Figure 4-1 shows the responses for the questions about when large-scale cyber attacks will occur.

FIGURE 4-1

When Large-Scale Cyber Attacks Will Occur

Response	When Large-Scale Cyber Attacks Will Be Launched By a Military	When Large-Scale Cyber Attacks Will Be Launched By Terrorists
Less than 2 years	48.4%	69.6%
2 to 5 years	28.2	20.9
5 to 10 years	11.7	4.2
More than 10 years	5.9	1.6
Cyber attacks will never happen	5.9	3.7

Preparation to Defend Against Large-Scale Cyber Attacks

If people think that cyber attacks are imminent then the next logical question would be how prepared people think they are to deal with the attacks. We asked two related questions about preparation to defend against cyber attacks:

- Do you think that your country is prepared to defend against large-scale cyber attacks?
- Do you think that your organization is prepared to defend against large-scale cyber attacks?

Even though the majority of respondents think that cyber attacks are imminent and will come in less than two years, far fewer think that their country (9.4%) or their organization (36.1%) are prepared to defend against cyber attacks. Figure 4-2 shows what respondents think about the preparation to defend against cyber attacks.

FIGURE 4-2

Preparation to Defend Against Cyber Attacks

Response	Country Is Prepared to Defend Against Large-Scale Cyber Attacks	Organization Is Prepared to Defend Against Large-Scale Cyber Attacks
Yes	9.4%	36.1%
No	80.1	57.1
Don't Know	10.5	6.8

CHAPTER 5— SECURITY MANAGEMENT

The GAO study determined that one of the five principles of risk management is that there should be an adequately funded and centralized management point established to focus on risks and security. We collected data on several aspects of IT security management including staffing patterns, spending trends, and the use of outside consultants. Key findings on security management include the following:

- 36.8% of respondents do NOT have an IS security director in their organization.
- 51.8% of respondents have not contracted with an IT security consulting firm during the last year.
- 23.7% of respondents report that their organizations spend less than 1% of their total IT budget on security staff and products.
- The ratio of IT security staff to total employees is very low.

Staffing IT Security

One of the biggest challenges that organizations face is how to staff IT security functions. This is certainly an internal issue, but it has ramifications for incident response as well as obtaining law enforcement assistance.

Computer Economics has worked with the High Tech Crime Investigators Association (HTCIA) to develop recommended policies and procedures for organizations to deal with computer crime and get the most out of their experience when engaging law enforcement agencies if an incident occurs. Law enforcement agencies are starting to address computer crimes in a more sophisticated manner. They are also developing an understanding of how internal security processes function in the real world.

It is convenient for law enforcement agencies to have a single point of contact during an investigation. As shown in Figure 5-1 only 60.9% of organizations report having an IS security director. Figure 5-2 compares organizations that do NOT have an IS security director to the overall population of respondents.

FIGURE 5-1

Organizations That Have an IS Security Director

Response	Percent of Respondents
Yes	60.9%
No	36.8
Don't Know	2.3

FIGURE 5-2

Organizations That Do NOT Have an IS Security Director

Industry Sector	Percent of Total Respondents	Percent of Respondents Who Do NOT Have an IS Security Director in Their Organization
Banking, Finance, and Insurance	14.6%	12.5%
Education	6.6	9.4
Government	16.5	7.8
Healthcare	4.7	4.7
Manufacturing	11.3	9.4
Professional Services	33.5	45.3
Retail/Wholesale Distribution	6.1	3.1
Trade Services	2.8	6.2
Transportation and Utilities	3.8	1.6
Number of Employees		
Less than 25	17.9	18.5
26 to 50	5.2	13.5
51 to 100	9.0	6.2
101 to 250	8.5	7.7
251 to 500	7.5	12.3
501 to 1,000	6.6	10.8
1,001 to 2,000	7.5	7.7
2,001 to 5,000	9.9	4.6
5,001 to 10,000	8.0	6.2
Over 10,000	19.8	12.3
Annual Revenue		
Under $1,000,000	22.3	26.2
$1,000,001 to $5,000,000	10.2	16.4
$5,000,001 to $10,000,000	6.6	9.8
$10,000,001 to $20,000,000	11.7	13.1
$20,000,001 to $50,000,000	8.1	1.6
$50,000,001 to $100,000,000	9.1	13.1
$100,000,001 to $1 Billion	10.7	9.8
Over $1 Billion	21.3	9.8

Staffing for IT security functions remains erratic. Focus groups conducted with Computer Economics clients reveal that most IS security managers think their efforts are inadequately staffed. Figure 5-3 shows the number of IT security staff in relationship to the number of employees in an organization.

FIGURE 5-3

IT Security Staffing Levels

	Number of Security Staff				
	Zero	1 to 2	3 to 5	6 to 10	More than 10
Number of Employees	Percent of Organizations				
Less than 25	13.8%	48.2%	24.1%	3.4%	10.3%
26 to 50	9.1	81.9	0.0	9.1	0.0
51 to 100	0.0	56.2	25.0	0.0	18.8
101 to 250	14.3	42.8	21.4	14.3	7.1
251 to 500	0.0	26.7	46.7	6.7	20.0
501 to 1,000	15.4	46.2	23.1	0.0	15.4
1,001 to 2,000	7.1	7.1	35.7	28.6	21.4
2,001 to 5,000	12.5	6.2	18.8	18.8	43.7
5,001 to 10,000	0.0	7.1	42.9	21.4	28.6
Over 10,000	0.0	5.8	14.7	8.8	70.6
All organizations	7.0	29.6	24.4	10.5	28.5

Spending for IT Security

We found that spending for IT security also remains rather erratic. The percent of IT budgets spent on IS security personnel or products is shown in Figure 5-4. In a separate spring 2002 survey on security spending conducted by Computer Economics we found that since September 11, 2001, 34% of organizations had increased spending for IT security and 55% were holding security budgets steady while 11% had decreased spending. This is significant, especially given the fact that much IT spending has been decreased or curtailed during the economic downturn.

FIGURE 5-4

Percent of IT Budgets Spent on Security Personnel or Products

Response	Percent of Respondents
Less than 1%	23.7%
Between 1% and 2%	13.3
Between 2% and 3%	12.1
Between 3% and 4%	3.5
Between 4% and 5%	2.9
More than 5%	17.3
Don't Know	27.2

Use of Outside Consultants

Many people expected the rise in terrorism would help fuel the growth of the IT security consulting industry. As shown in Figure 5-5 the majority of organizations (51.8%) had not contracted with an IT security consulting firm during the last year.

FIGURE 5-5

Used a Security Consulting Firm During the Last Year

Response	Percent of Respondents
Yes	35.7%
No	51.8
Don't Know	12.5

The organizations that were most likely to contract with a security consulting firm during the last year were banking, finance, and insurance firms (27.9%) and government agencies (21.3%). As Figure 5-6 shows, large organizations are also more likely to have contracted with a security consulting firm. Of organizations with 5,000 to 10,000 employees, 13.1% contracted with a security consulting firm during the last 12 months, as did 31.1% of organizations with over 10,000 employees. From another perspective, 32.7% of organizations with an annual revenue of over $1 billion contracted for security services.

FIGURE 5-6

Organizations Contracting With a Security Consulting Firm During the Last Year

Industry Sector	Percent of Total Respondents	Percent of Respondents Who Have Contracted With a Security Consulting Firm During the Last Year
Banking, Finance, and Insurance	14.6%	27.9%
Education	6.6	4.9
Government	16.5	21.3
Healthcare	4.7	8.2
Manufacturing	11.3	13.2
Professional Services	33.5	14.8
Retail/Wholesale Distribution	6.1	8.2
Trade Services	2.8	1.6
Transportation and Utilities	3.8	0.0
Number of Employees		
Less than 25	17.9	9.8
26 to 50	5.2	4.9
51 to 100	9.0	3.3
101 to 250	8.5	3.3
251 to 500	7.5	6.6
501 to 1,000	6.6	9.8
1,001 to 2,000	7.5	8.2
2,001 to 5,000	9.9	9.8
5,001 to 10,000	8.0	13.1
Over 10,000	19.8	31.1
Annual Revenue		
Under $1,000,000	22.3	20.0
$1,000,001 to $5,000,000	10.2	9.1
$5,000,001 to $10,000,000	6.6	7.3
$10,000,001 to $20,000,000	11.7	7.3
$20,000,001 to $50,000,000	8.1	3.6
$50,000,001 to $100,000,000	9.1	5.5
$100,000,001 to $1 Billion	10.7	14.5
Over $1 Billion	21.3	32.7

CHAPTER 6 — SECURITY POLICY

The GAO study determined that one of the five principles of risk management is that appropriate policies and related controls should be implemented. Law enforcement agencies and prosecutors whom Computer Economics has consulted with feel that it is critical to have written policies in place. Responses to the survey questions related to policies show that the practice of having written policies in place is far from universal.

- 71.1% have written IT security policies in place.
- 49.1% have written IT security incident response procedures in place.
- 72.4% have written privacy policies covering customer and corporate data in place.
- 72.8% have written policies on appropriate use of information systems, networks, and email and have informed employees of these policies.
- 56.3% require employees to sign statements that they understand the information systems security policies and will abide by them.

Written Policies in Place

Having written security policies in place is key to the security management process. Security personnel, IT staff, and employees throughout the organization need policies and procedures in order to know how to secure data, systems, and networks. As shown in Figure 6-1, written IT security policies are in place in 71.1% of the responders' organizations while 26.0% do not have written IT security policies in place. Figure 6-2 shows the breakdown of organizations that do not have written IT security policies in place.

FIGURE 6-1

Written IT Security Policies

Response	Percent of Respondents
Yes	71.1%
No	26.0
Don't Know	2.9

FIGURE 6-2

Organizations Without Written IT Security Policies

Industry Sector	Percent of Total Respondents	Percent of Respondents Who Do NOT Have Written Information Systems Security Policies
Banking, Finance, and Insurance	14.6%	4.3%
Education	6.6	17.4
Government	16.5	8.7
Healthcare	4.7	2.2
Manufacturing	11.3	4.4
Professional Services	33.5	47.8
Retail/Wholesale Distribution	6.1	4.4
Trade Services	2.8	10.9
Transportation and Utilities	3.8	0.0
Number of Employees		
Less than 25	17.9	30.4
26 to 50	5.2	17.4
51 to 100	9.0	13.0
101 to 250	8.5	2.2
251 to 500	7.5	4.3
501 to 1,000	6.6	13.0
1,001 to 2,000	7.5	6.5
2,001 to 5,000	9.9	4.3
5,001 to 10,000	8.0	4.3
Over 10,000	19.8	4.3
Annual Revenue		
Under $1,000,000	22.3	38.1
$1,000,001 to $5,000,000	10.2	16.7
$5,000,001 to $10,000,000	6.6	7.1
$10,000,001 to $20,000,000	11.7	9.5
$20,000,001 to $50,000,000	8.1	2.4
$50,000,001 to $100,000,000	9.1	14.3
$100,000,001 to $1 Billion	10.7	7.1
Over $1 Billion	21.3	7.8

In addition to written security policies, it is also critical to have written IT security incident response procedures in place. This helps to assure that security personnel, IT staff, and employees throughout the organization know what to do when an incident occurs. As shown in Figure 6-3, IT security incident response procedures are in place in only 49.1% of the responders' organizations, while 43.4% do not have written IT security incident response procedures in place. Figure 6-4 shows the breakdown of organizations that do not have written IT security incident response procedures in place.

FIGURE 6-3

Written Incident Response Procedures

Response	Percent of Respondents
Yes	49.1%
No	43.4
Don't Know	7.5

FIGURE 6-4

Organizations Without Written Incident Response Procedures

Industry Sector	Percent of Total Respondents	Percent of Respondents Who Do NOT Have Written Information Systems Security Incident Response Policies
Banking, Finance, and Insurance	14.6%	10.4%
Education	6.6	11.7
Government	16.5	11.7
Healthcare	4.7	5.2
Manufacturing	11.3	5.2
Professional Services	33.5	37.7
Retail/Wholesale Distribution	6.1	7.8
Trade Services	2.8	6.5
Transportation and Utilities	3.8	2.6
Number of Employees		
Less than 25	17.9	21.1
26 to 50	5.2	13.0
51 to 100	9.0	13.0
101 to 250	8.5	6.5
251 to 500	7.5	5.2
501 to 1,000	6.6	11.7
1,001 to 2,000	7.5	9.1
2,001 to 5,000	9.9	6.5
5,001 to 10,000	8.0	6.5
Over 10,000	19.8	6.5
Annual Revenue		
Under $1,000,000	22.3	26.4
$1,000,001 to $5,000,000	10.2	15.3
$5,000,001 to $10,000,000	6.6	8.3
$10,000,001 to $20,000,000	11.7	12.5
$20,000,001 to $50,000,000	8.1	4.2
$50,000,001 to $100,000,000	9.1	13.9
$100,000,001 to $1 Billion	10.7	12.5
Over $1 Billion	21.3	6.9

As shown in Figure 6-5, 72.4% of the responders' organizations have written privacy policies in place, while 21.3% do not have written privacy policies in place. This is relatively consistent with other research Computer Economics has conducted including the 13th annual *Information Systems and E-Business Spending* study conducted in early 2002. Figure 6-6 shows a breakdown of the organizations without written privacy policies in place.

FIGURE 6-5

Have Written Privacy Policy

Response	Percent of Respondents
Yes	72.4%
No	21.3
Don't Know	6.3

FIGURE 6-6

Organizations Without Written Privacy Policies

Industry Sector	Percent of Total Respondents	Percent of Respondents Who Do NOT Have Written Privacy Policy for Corporate or Customer Data
Banking, Finance, and Insurance	14.6%	7.7%
Education	6.6	10.3
Government	16.5	23.1
Healthcare	4.7	2.6
Manufacturing	11.3	2.6
Professional Services	33.5	46.2
Retail/Wholesale Distribution	6.1	2.6
Trade Services	2.8	5.1
Transportation and Utilities	3.8	0.0
Number of Employees		
Less than 25	17.9	25.6
26 to 50	5.2	17.9
51 to 100	9.0	12.8
101 to 250	8.5	7.7
251 to 500	7.5	5.1
501 to 1,000	6.6	12.8
1,001 to 2,000	7.5	2.6
2,001 to 5,000	9.9	7.7
5,001 to 10,000	8.0	2.6
Over 10,000	19.8	5.1
Annual Revenue		
Under $1,000,000	22.3	35.1
$1,000,001 to $5,000,000	10.2	18.9
$5,000,001 to $10,000,000	6.6	5.4
$10,000,001 to $20,000,000	11.7	10.8
$20,000,001 to $50,000,000	8.1	2.7
$50,000,001 to $100,000,000	9.1	13.5
$100,000,001 to $1 Billion	10.7	10.8
Over $1 Billion	21.3	2.7

Policies on Appropriate Use by Employees

Law enforcement agencies and prosecutors that Computer Economics has consulted with believe that it is critical to have written policies defining appropriate use of computers and networks owned or operated by an organization. As shown in Figure 6-7, 72.8% of the responders' organizations have policies on appropriate use of information systems, networks, and email and they have informed employees of these policies. Figure 6-8 shows a breakdown of organizations without policies on appropriate use.

FIGURE 6-7

Policies on Appropriate Use

Response	Percent of Respondents
Yes	72.8%
No	20.8
Don't Know	6.4

FIGURE 6-8

Organizations Without Policies on Appropriate Use

Industry Sector	Percent of Total Respondents	Percent of Respondents Who Have NOT Formulated Policies as to What Is Appropriate Use of Information Systems, Networks, and Email and Informed Employees of These Policies
Banking, Finance, and Insurance	14.6%	5.4%
Education	6.6	13.5
Government	16.5	13.5
Healthcare	4.7	2.7
Manufacturing	11.3	2.7
Professional Services	33.5	48.6
Retail/Wholesale Distribution	6.1	2.7
Trade Services	2.8	10.8
Transportation and Utilities	3.8	0.0
Number of Employees		
Less than 25	17.9	40.5
26 to 50	5.2	8.1
51 to 100	9.0	8.1
101 to 250	8.5	5.4
251 to 500	7.5	5.4
501 to 1,000	6.6	10.8
1,001 to 2,000	7.5	5.4
2,001 to 5,000	9.9	8.1
5,001 to 10,000	8.0	2.7
Over 10,000	19.8	5.4
Annual Revenue		
Under $1,000,000	22.3	44.1
$1,000,001 to $5,000,000	10.2	17.6
$5,000,001 to $10,000,000	6.6	2.9
$10,000,001 to $20,000,000	11.7	8.8
$20,000,001 to $50,000,000	8.1	2.9
$50,000,001 to $100,000,000	9.1	11.8
$100,000,001 to $1 Billion	10.7	5.9
Over $1 Billion	21.3	5.9

Law enforcement agencies and prosecutors that Computer Economics has consulted with also believe that it is critical that employees are required to sign statements that they understand the information systems security policies and will abide by them. As shown in Figure 6-9, 56.3% of the responder's organizations require employees to sign statements. Figure 6-10 shows a breakdown of organizations that do NOT require employees to sign statements on appropriate use.

FIGURE 6-9

Organizations Requiring Signed Statements

Response	Percent of Respondents
Yes	56.3%
No	41.4
Don't Know	2.3

FIGURE 6-10

Organizations NOT Requiring Signed Statements

Industry Sector	Percent of Total Respondents	Percent of Respondents Who Do NOT Require Employees to Sign Statements That They Understand the Information Systems Security Policies and Will Abide By Them
Banking, Finance, and Insurance	14.6%	9.5%
Education	6.6	16.4
Government	16.5	13.7
Healthcare	4.7	0.0
Manufacturing	11.3	8.2
Professional Services	33.5	42.5
Retail/Wholesale Distribution	6.1	2.8
Trade Services	2.8	5.5
Transportation and Utilities	3.8	1.4
Number of Employees		
Less than 25	17.9	27.0
26 to 50	5.2	10.8
51 to 100	9.0	12.2
101 to 250	8.5	5.4
251 to 500	7.5	4.1
501 to 1,000	6.6	13.5
1,001 to 2,000	7.5	8.1
2,001 to 5,000	9.9	6.8
5,001 to 10,000	8.0	2.7
Over 10,000	19.8	9.5
Annual Revenue		
Under $1,000,000	22.3	34.3
$1,000,001 to $5,000,000	10.2	12.9
$5,000,001 to $10,000,000	6.6	4.3
$10,000,001 to $20,000,000	11.7	11.4
$20,000,001 to $50,000,000	8.1	4.3
$50,000,001 to $100,000,000	9.1	14.3
$100,000,001 to $1 Billion	10.7	8.6
Over $1 Billion	21.3	10.0

CHAPTER 7 — ENFORCING SECURITY POLICIES

Once security policies are in place it prudent to consistently enforce the policies. To evaluate how and to what extent policies are being enforced we asked several related questions. Key results from this part of the survey include the following:

- 36.8% use desktop warning banners to reinforce appropriate use of systems.
- 48.0% have terminated employees for misuse of computers or networks
- 27.0% have reported a security breach to law enforcement.
- 56.1% have conducted IS security or virus protection training with employees.

Desktop Banner Warnings

Law enforcement agencies and prosecutors believe that it is critical to constantly reinforce to employees what constitutes appropriate use. One favored way, according to prosecutors, of reinforcing policies on a daily basis is through the use of a banner that appears on desktop systems every time the systems are turned on. The banner is to inform employees that their use of corporate computers can be monitored and that they should not expect privacy in the workplace. Figure 7-1 shows that only 36.8% of the responder's organizations are using desktop warning banners. Figure 7-2 shows a breakdown of the organizations that do NOT use desktop warning banners on appropriate use.

FIGURE 7-1

Use Desktop Warning Banners

Response	Percent of Respondents
Yes	36.8%
No	60.3
Don't Know	2.9

FIGURE 7-2

Organizations That Do NOT Use Desktop Warning Banners

Industry Sector	Percent of Total Respondents	Percent of Respondents Who Do NOT Use a Banner on Desktops
Banking, Finance, and Insurance	14.6%	8.5%
Education	6.6	10.4
Government	16.5	15.1
Healthcare	4.7	3.8
Manufacturing	11.3	11.4
Professional Services	33.5	39.6
Retail/Wholesale Distribution	6.1	4.7
Trade Services	2.8	3.8
Transportation and Utilities	3.8	2.7
Number of Employees		
Less than 25	17.9	19.8
26 to 50	5.2	8.5
51 to 100	9.0	11.3
101 to 250	8.5	6.6
251 to 500	7.5	11.3
501 to 1,000	6.6	8.5
1,001 to 2,000	7.5	8.5
2,001 to 5,000	9.9	8.5
5,001 to 10,000	8.0	3.8
Over 10,000	19.8	13.2
Annual Revenue		
Under $1,000,000	22.3	26.3
$1,000,001 to $5,000,000	10.2	13.1
$5,000,001 to $10,000,000	6.6	8.1
$10,000,001 to $20,000,000	11.7	13.1
$20,000,001 to $50,000,000	8.1	4.0
$50,000,001 to $100,000,000	9.1	12.1
$100,000,001 to $1 Billion	10.7	8.1
Over $1 Billion	21.3	15.2

Termination of Employees for Misuse

Once appropriate use policies are established, agreements to use computers and networks properly are signed by employees, and warnings about policies are reinforced, organizations are confronted with terminating employees who violate policies. As shown in Figure 7-3, 48.0% of responders indicated that their organizations have terminated employees for misuse of computers or networks. Figure 7-4 provides a breakdown of organizations that have NOT terminated an employee for misuse.

FIGURE 7-3

Terminated an Employee for Misuse

Response	Percent of Respondents
Yes	48.0%
No	34.1
Don't Know	17.9

FIGURE 7-4

Have NOT Terminated an Employee for Misuse

Industry Sector	Percent of Total Respondents	Percent of Respondents Who Have NOT Terminated an Employee for Misuse of Information Systems, Networks, or Email
Banking, Finance, and Insurance	14.6%	8.3%
Education	6.6	10.0
Government	16.5	18.3
Healthcare	4.7	5.0
Manufacturing	11.3	5.0
Professional Services	33.5	41.7
Retail/Wholesale Distribution	6.1	3.4
Trade Services	2.8	6.7
Transportation and Utilities	3.8	1.7
Number of Employees		
Less than 25	17.9	33.9
26 to 50	5.2	15.3
51 to 100	9.0	16.9
101 to 250	8.5	8.5
251 to 500	7.5	6.8
501 to 1,000	6.6	6.8
1,001 to 2,000	7.5	1.7
2,001 to 5,000	9.9	5.1
5,001 to 10,000	8.0	0.0
Over 10,000	19.8	5.1
Annual Revenue		
Under $1,000,000	22.3	35.1
$1,000,001 to $5,000,000	10.2	15.8
$5,000,001 to $10,000,000	6.6	12.3
$10,000,001 to $20,000,000	11.7	15.8
$20,000,001 to $50,000,000	8.1	8.8
$50,000,001 to $100,000,000	9.1	3.5
$100,000,001 to $1 Billion	10.7	3.5
Over $1 Billion	21.3	5.3

Reporting to Law Enforcement

Very few organizations report system intrusions, hacking, or computer-related crime to law enforcement agencies. There are many reasons for this including the desire to avoid negative publicity and the time and effort that it takes to go through the reporting process and perhaps participate in a legal proceeding. As shown in Figure 7-5, only 27.0% of the respondents indicated that their organization had reported a security breach to law enforcement. Figure 7-6 shows a breakdown of organizations that have NOT reported a security breach to law enforcement.

FIGURE 7-5

Reported a Security Breach to Law Enforcement

Response	Percent of Respondents
Yes	27.0%
No	50.0
Don't Know	23.0

FIGURE 7-6

Have NOT Reported a Security Breach to Law Enforcement

Industry Sector	Percent of Total Respondents	Percent of Respondents Who Have NOT Reported a Security Breach to Law Enforcement
Banking, Finance, and Insurance	14.6%	11.4%
Education	6.6	5.7
Government	16.5	15.9
Healthcare	4.7	5.7
Manufacturing	11.3	9.1
Professional Services	33.5	40.9
Retail/Wholesale Distribution	6.1	4.5
Trade Services	2.8	3.4
Transportation and Utilities	3.8	3.4
Number of Employees		
Less than 25	17.9	23.9
26 to 50	5.2	10.2
51 to 100	9.0	11.4
101 to 250	8.5	5.7
251 to 500	7.5	12.5
501 to 1,000	6.6	8.0
1,001 to 2,000	7.5	9.1
2,001 to 5,000	9.9	4.5
5,001 to 10,000	8.0	5.7
Over 10,000	19.8	9.1
Annual Revenue		
Under $1,000,000	22.3	28.2
$1,000,001 to $5,000,000	10.2	12.9
$5,000,001 to $10,000,000	6.6	9.4
$10,000,001 to $20,000,000	11.7	14.1
$20,000,001 to $50,000,000	8.1	7.1
$50,000,001 to $100,000,000	9.1	12.9
$100,000,001 to $1 Billion	10.7	8.2
Over $1 Billion	21.3	7.1

Employee Training Practices

The GAO study determined that an important principle of risk and security management is to promote awareness in an organization. To evaluate the extent to which organizations do training we asked the question: Has your organization ever conducted information systems security or virus protection training with employees? As shown in Figure 7-7, 56.1% of the respondents reported that their organizations have conducted some type of training. Figure 7-8 provides a breakdown of organizations that have NOT trained employees on IT security.

FIGURE 7-7

Trained Employees on IT Security or Virus Protection

Response	Percent of Respondents
Yes	56.1%
No	36.4
Don't Know	7.5

FIGURE 7-8

Have NOT Trained Employees on IT Security

industry Sector	Percent of Total Respondents	Percent of Respondents Who Have NOT Conducted Information Systems Security or Virus Protection Training With Employees
Banking, Finance, and Insurance	14.6%	9.3%
Education	6.6	10.9
Government	16.5	17.2
Healthcare	4.7	4.7
Manufacturing	11.3	6.2
Professional Services	33.5	39.1
Retail/Wholesale Distribution	6.1	3.1
Trade Services	2.8	4.7
Transportation and Utilities	3.8	4.7
Number of Employees		
Less than 25	17.9	17.2
26 to 50	5.2	6.2
51 to 100	9.0	10.9
101 to 250	8.5	9.4
251 to 500	7.5	10.9
501 to 1,000	6.6	14.1
1,001 to 2,000	7.5	3.1
2,001 to 5,000	9.9	7.8
5,001 to 10,000	8.0	7.8
Over 10,000	19.8	12.5
Annual Revenue		
Under $1,000,000	22.3	24.1
$1,000,001 to $5,000,000	10.2	13.8
$5,000,001 to $10,000,000	6.6	13.8
$10,000,001 to $20,000,000	11.7	10.3
$20,000,001 to $50,000,000	8.1	3.4
$50,000,001 to $100,000,000	9.1	10.3
$100,000,001 to $1 Billion	10.7	12.1
Over $1 Billion	21.3	12.1

CHAPTER 8 — TESTING SECURITY

As the dependency on computers and network communications increases so does an organization's vulnerability to information security compromises. Almost every week the media reports on new computer crimes, system break-ins, malicious code attacks, and the ever-growing threat of cyber terrorism. Current research on security shows the following:

- Threats to computer systems and networks are increasing.
- Damage caused by malicious attacks is rising.
- Systems without appropriate security are easy hits for hackers.

Assessing the effectiveness of current security measures is a very complex process. Data can be collected in three different ways. First, an analysis of known incidents over the last two to three years is very helpful. This data can be collected from IT security staff, department managers, corporate security offices, and server logs. This combination of data will demonstrate where security has been weak as well as how many and what kinds of attempts have been made to break into systems.

A second method to collect data on effectiveness is to conduct a vulnerability audit. A vulnerability audit assesses the security of networks and host systems, identifies vulnerabilities, and provides a report that IT staff can use to make any necessary security adjustments. Automated vulnerability testing uses software to scan networks, servers, firewalls, routers, and applications for vulnerabilities. Generally, the scan can detect known security flaws or bugs in software and hardware, determine if the systems are susceptible to known attacks and exploits, and search for system vulnerabilities such as settings contrary to established security policies. The detailed report on vulnerabilities will include the following:

- The vulnerable host(s)
- Operating system weaknesses
- Level of security risk of the vulnerability
- Description of the vulnerability
- Recommendation for correcting the problem.

Vulnerabilities are classified as having high, medium, and low severity. High-risk vulnerabilities are those that provide unauthorized access to your workstation. Medium risk vulnerabilities are those that provide access to sensitive data on your workstation, and which may lead to the exploitation of higher risk vulnerabilities. Low risk vulnerabilities are those that provide access to potentially sensitive information.

A third method is to conduct intrusion tests against an organization's systems and networks. Intrusion tests, like vulnerability audits, are structured processes designed to identify and catalog system and network weaknesses. Some people refer to intrusion testing as a white hat hacking process, where trained security people test the security of systems with a variety of scanning tools. In some cases actual attempts at breaking into systems are made.

Use of Vulnerability Audits

As shown in Figure 8-1, vulnerability audits have been conducted by 65.7% of the respondent's organizations. Figure 8-2 shows a breakdown of the organizations that have NOT conducted a vulnerability audit.

FIGURE 8-1

Conducted a Vulnerability Audit

Response	Percent of Respondents
Yes	65.7%
No	25.0
Don't Know	9.3

FIGURE 8-2

Have NOT Conducted a Vulnerability Audit

Industry Sector	Percent of Total Respondents	Percent of Respondents Who Have NOT Conducted a Vulnerability Audit
Banking, Finance, and Insurance	14.6%	9.1%
Education	6.6	9.1
Government	16.5	13.6
Healthcare	4.7	4.5
Manufacturing	11.3	4.5
Professional Services	33.5	47.7
Retail/Wholesale Distribution	6.1	2.3
Trade Services	2.8	6.8
Transportation and Utilities	3.8	2.3
Number of Employees		
Less than 25	17.9	25.0
26 to 50	5.2	9.1
51 to 100	9.0	9.1
101 to 250	8.5	11.4
251 to 500	7.5	6.8
501 to 1,000	6.6	6.8
1,001 to 2,000	7.5	11.4
2,001 to 5,000	9.9	6.8
5,001 to 10,000	8.0	6.8
Over 10,000	19.8	6.8
Annual Revenue		
Under $1,000,000	22.3	23.8
$1,000,001 to $5,000,000	10.2	21.4
$5,000,001 to $10,000,000	6.6	7.1
$10,000,001 to $20,000,000	11.7	9.5
$20,000,001 to $50,000,000	8.1	2.4
$50,000,001 to $100,000,000	9.1	14.3
$100,000,001 to $1 Billion	10.7	19.0
Over $1 Billion	21.3	2.4

Use of Intrusion Testing

As shown in Figure 8-3 intrusion tests have been conducted by 65.1% of the respondents' organizations. Figure 8-4 shows a breakdown of the organizations that have NOT conducted an intrusion test.

FIGURE 8-3

Conducted an Intrusion Test

Response	Percent of Respondents
Yes	65.1%
No	21.3
Don't Know	13.6

FIGURE 8-4

Have NOT Conducted an Intrusion Test

Industry Sector	Percent of Total Respondents	Percent of Respondents Who Have NOT Conducted an Intrusion Test
Banking, Finance, and Insurance	14.6%	5.4%
Education	6.6	2.7
Government	16.5	16.4
Healthcare	4.7	5.4
Manufacturing	11.3	8.1
Professional Services	33.5	48.6
Retail/Wholesale Distribution	6.1	2.7
Trade Services	2.8	8.1
Transportation and Utilities	3.8	2.7
Number of Employees		
Less than 25	17.9	18.9
26 to 50	5.2	8.1
51 to 100	9.0	10.8
101 to 250	8.5	8.1
251 to 500	7.5	8.1
501 to 1,000	6.6	8.1
1,001 to 2,000	7.5	10.8
2,001 to 5,000	9.9	5.4
5,001 to 10,000	8.0	10.8
Over 10,000	19.8	10.8
Annual Revenue		
Under $1,000,000	22.3	21.2
$1,000,001 to $5,000,000	10.2	21.2
$5,000,001 to $10,000,000	6.6	9.1
$10,000,001 to $20,000,000	11.7	9.1
$20,000,001 to $50,000,000	8.1	3.0
$50,000,001 to $100,000,000	9.1	12.1
$100,000,001 to $1 Billion	10.7	21.2
Over $1 Billion	21.3	3.0

CHAPTER 9 — COST OF INCIDENTS

Computer Economics has collected and analyzed data on the impact of malicious code attacks, hacking and intrusion incidents, and the cost of system downtime for several years. Much of this work dates backs as far as the early 1990s. The analysis of malicious code attacks intensified recently as major virus incidents such as Melissa, I Love You, Code Red, and Nimda became commonplace.

The research has largely been client driven. When Computer Economics clients needed to determine the return on investment for security and virus protection, an in-depth and ongoing research process was initiated. Data collection is ongoing and involves the following:

- Review of numerous statistical reports and studies on computer crime and malicious attacks of all sorts.
- Data collection on the economic aspects of malicious attacks.
- Benchmarking clean-up and recovery costs from major incidents.
- Benchmarking the impact on productivity that attacks have on different types of organizations.
- Benchmarking lost revenue from downtime.
- Monitoring the activity reports of security companies including the frequency of different types of attacks and the recurrence of virus activity.
- Ongoing surveys of IT spending, security practices, and the cost of malicious attacks.

To add to our data on the cost of intrusions and malicious code incidents we asked two questions of this survey group:

- How much have intrusions and/or hacking incidents cost your organization during the last 12 months?
- How much have virus/worm attacks cost your organization during the last 12 months?

Cost of Intrusions

Many organizations have difficulties determining how often their systems are penetrated. It is even more difficult for most organizations to determine the cost or economic impact of those intrusions. Computer Economics has worked with many organizations to establish tracking and modeling systems to determine costs. Most organizations, however, are way behind the curve in getting good internal data on costs of incidents. As shown in Figure 9-1 most respondents (49.1%) do not know how much intrusions and/or hacking incidents cost their organization during the last 12 months.

FIGURE 9-1

Cost of Intrusions/Hacking Incidents During the Last 12 Months

Costs	Percent of Respondents
Less than $10,000	39.2%
Between $10,001 and $20,000	1.8
Between $20,001 and $50,000	5.8
Between $50,001 and $100,000	1.8
Between $100,001 and $500,000	0.6
Between $500,001 and $1,000,000	0.0
Over $1,000,000	1.8
Don't Know	49.1

Cost of Virus and Worm Attacks

Many organizations also have difficulties determining the cost or economic impact of virus and worm attacks. Computer Economics has worked with many organizations to establish tracking and modeling systems to determine costs as well as to evaluate the return on investment for virus protection. Most organizations, however, are way behind the curve in getting good internal data on costs of incidents. As shown in Figure 9-2 most respondents (39.3%) do not know how much virus and worm attacks cost their organization during the last 12 months.

FIGURE 9-2

Cost of Virus/Worm Attacks During the Last 12 Months

Costs	Percent of Respondents
Less than $10,000	32.9%
Between $10,000 and $20,000	9.8
Between $20,001 and $50,000	7.5
Between $50,001 and $100,000	4.6
Between $100,001 and $500,000	2.3
Between $500,001 and $1,000,000	0.6
Over $1,000,000	2.9
Don't Know	39.3