2001 industry survey

2,545 information security practitioners give the lowdown on security budgets, purchasing trends, security breaches and defenses, obstacles to security and much more.

"If you're connected to the Internet, there's no such thing as security. It's called controlled access. If you control the access, everything should be fine. However, if you lose control of the access, that's when there are problems."

Sage words, indeed, from one of the more than 2,500 infosecurity officers, managers, consultants, engineers and administrators who responded to *Information Security*'s fourth annual

BY ANDY BRINEY

HIGHLIGHTS

- **Corporate funding for infosecurity continues to grow overall, though the pace has slowed from that of recent years. Nearly one-third of companies froze security spending sometime in 2001 due to adverse economic conditions.**
- **PKI, wireless and enterprise security management will be among the hot technology markets in 2002, according to a survey of purchasing trends. Biometrics and managed security services may struggle.**
- **Viruses, worms, Trojans and other malware infected 90 percent of the organizations in the survey, despite the fact that 88 percent of these companies have antivirus protection in place.**
- **The number of organizations hit by Web server attacks doubled from 2000 to 2001.**
- **Overall, "insider" security incidents occur far more frequently than "external" incidents. Nevertheless, the number one priority of security professionals is securing the network perimeter against external attack.**

2,545

SURVEY BACKGROUND

The 2001 *Information Security* Industry Survey was conducted online in late July and early August 2001. The survey, now in its fourth year, was completed by 2,545 information security professionals drawn from approximately 45,000 subscribers to the magazine's Security Wire Digest newsletter. Statistical analysis was performed by *Information Security*'s editorial staff in conjunction with the survey's sponsors, **TruSecure** (**www.trusecure.com**) and **Predictive Systems** (**www.predictive.com**).

Sponsored by:

INFORMATION SECURITY®

TRUSECURE CORPORATION

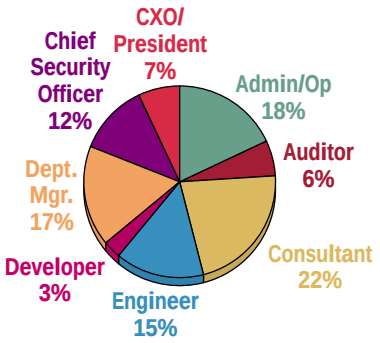
PREDICTIVE SYSTEMS

Industry Survey. If only controlling access was as easy as it sounds. Ubiquitous connectivity, complex systems and networks, the push for point-and-click commerce and the proliferation of easy-to-abuse attack tools have created an environment of ever-increasing risk.

Statistics from the 2001 Industry Survey prove that managing risk will get even more challenging in coming months. The global economic slowdown has forced organizations across all business sectors to cut or freeze security spending at a time when massive layoffs have put tens of thousands of workers on the streets, some of whom will have axes to grind with their former employers.

FIGURE 1

JOB TITLES

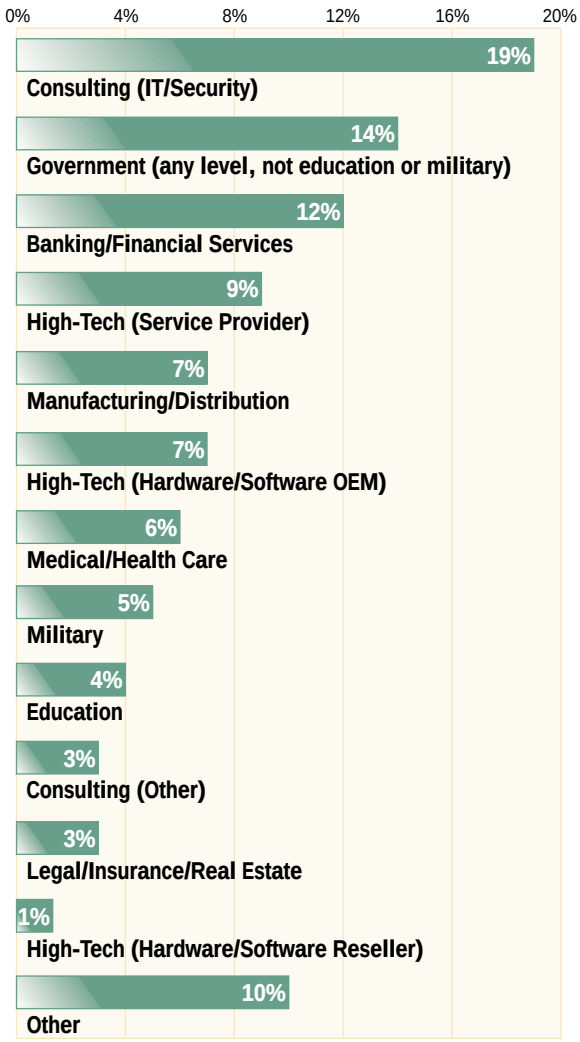


It's not an exaggeration to say that at no time in the history of the Internet has infosecurity been more important to the success and stability of the business enterprise. Yet at no time have security departments been more in danger of failure—failure to protect the confidentiality, integrity and availability of data and communications, not to mention the corporation's public image and reputation.

The 2001 Industry Survey explores critical areas of interest to those responsible for ensuring such failures never happen—or, at least, minimizing their impact when they do. Conducted in late summer 2001, the survey reflects the input of security professionals on all business levels across a broad spectrum of public and private organizations in North America, Europe and the Far East *(see Figures 1 and 2, left)*.

FIGURE 2

INDUSTRY BREAKOUT



Security Budgets: Slowing Growth

Infosecurity practitioners often measure security's status in their organizations by the size and annual growth of their infosecurity budgets. Talk is cheap. Show me the money. Money talks. Whatever your favorite cliché, the message is the same: Executive management may pay lip service to the importance of data protection, threat management and risk mitigation, but greenbacks speak louder than words.

The 2001 *Information Security* Industry Survey reveals mixed

FIGURE 3

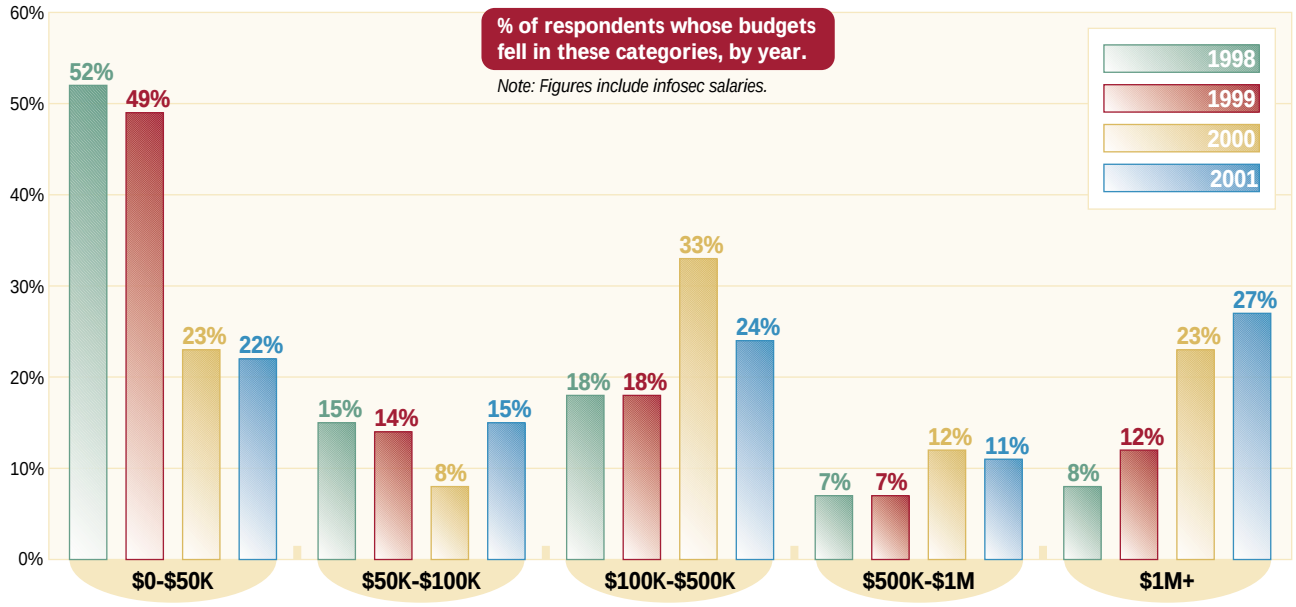
2001 INFOSEC BUDGETS

INDUSTRY	MEAN	MEDIAN
Banking/financial services (n=208)	$3,069,262	$750,000
Consulting (IT/security) (n=320)	$1,869,644	$835,000
Consulting (other) (n=48)	$1,406,094	$325,000
Education (n=75)	$756,013	$100,000
Government (not incl. military) (n=239)	$2,011,839	$500,000
High-Tech (OEM) (n=121)	$1,502,488	$300,000
High-Tech (reseller) (n=39)	$693,641	$75,000
High-Tech (service provider) (n=157)	$1,954,535	$275,000
Legal/Insurance/Real Estate (n=52)	$2,061,846	$500,000
Manufacturing/Distribution (n=131)	$2,476,874	$400,000
Medical/Health Care (n=104)	$1,284,596	$250,000
Military (n=67)	$2,577,343	$450,000
Other (n=185)	$1,798,135	$550,000
TOTAL (n=1746)	**$1,963,375**	**$260,000**

n *= number of respondents in each category.* ***Mean*** *= average budget for all organizations reporting.* ***Median*** *= budget for "middle" organization (equal number of organizations have higher and lower budgets).*

FIGURE 4

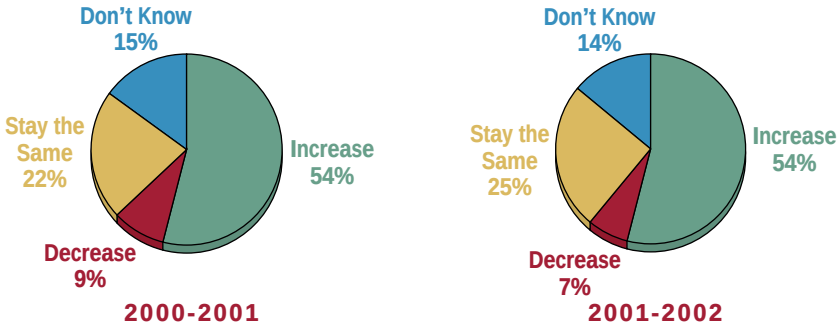
INFOSEC BUDGET GROWTH, 1998-2001



FIGURES 5 & 6

FISCAL YEAR BUDGET GROWTH

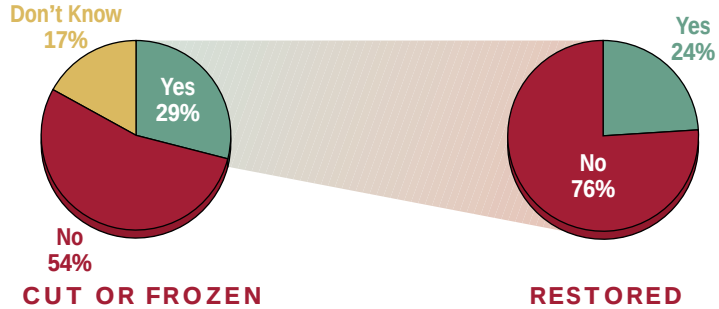
From FY 2000 to FY 2001, did your infosec budget increase, decrease or stay the same? What do you expect your budget will do from FY 2001 to FY 2002?



FIGURES 7 & 8

BUDGET CUTS & FREEZES, 2001

At any time this year (FY 2001), has your infosec budget been cut or frozen due to economic slowdown? If "Yes," was funding later restored?



results when it comes to infosec funding. On a positive note, overall (industry-wide) security budgets climbed for the fourth year in a row, with most respondents (54 percent) saying their budgets increased from fiscal year 2000 to 2001. An almost identical number of companies expect their budgets to increase again next year *(see Figures 5 and 6, left)*.

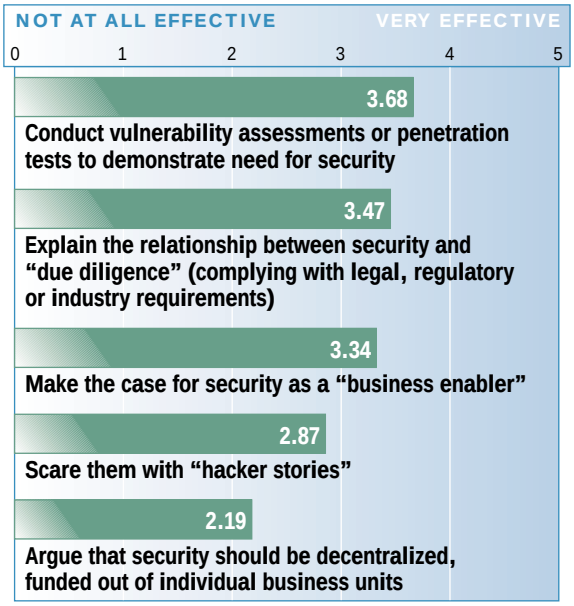
Another way to gauge budget growth is to analyze industry-wide shifts in total security spending. Infosecurity's "millionaire's club"—organizations with infosec budgets topping $1 million—welcomed a few more members this year, with some 27 percent of the pool falling within that category *(see Figure 4, above)*. However, the growth rate of companies with $1 million-plus security budgets has slowed considerably compared to recent years. At the same time, there's been a dramatic 20 percent increase in the number of com-

> "Our customers insist on security as a fact of life, and it's an important selling point."
>
> **–CHIEF SECURITY OFFICER,**
> U.S. financial institution

FIGURE 9

SELLING SECURITY

How effective are the following methods in getting management to fund infosecurity at your organization?



panies spending less than $100,000 on security annually.

In other words, the separation between the "haves" and "have-nots" is becoming more pronounced. Banks, brokerage houses, investment firms, insurance companies, manufacturers and military organizations are seeing healthy increases in security budgets, while universities and health care institutions, among others, remain relatively security poor *(see Figure 3, p. 35)*.

"Our customers insist on security as a fact of life, and it's an important selling point," says one survey respondent, a chief security officer at a Northeastern U.S. financial institution. "We undertake significant liabilities for security breaches as part of our provision of service."

Information security may be a selling point at a few companies, but global economic instability—and its impact on all corporate budgets—is a stark reality for all. It's widely assumed that security budgets should be spared during a recession (or near recession), for two primary reasons: (1) corporate downsizing and unstable markets increase corporate risk, which naturally increases the importance of risk mitigation; and (2) infosecurity already represents such a small portion of the overall corporate budget—by some estimates, less than $250 for every $1 million in top-line revenues—that cutting it further wouldn't make much of a difference.

While these are perfectly logical assumptions, the 2001 survey shows they're invalid. Nearly one-third (29 percent) of all respondents said their security budget has been cut or frozen

FIGURE 10

SECURITY PRODUCT/ SERVICE ADOPTION

% of respondents acquiring/ deploying these products/services

	ITEM	ACQUIRED/DEPLOYED IN 2000 OR EARLIER	ACQUIRED/DEPLOYED IN 2001	PLAN TO ACQUIRE IN 2002	NO PLANS TO ACQUIRE	DON'T KNOW
HARDWARE/SOFTWARE	Authentication software/servers	58%	9%	9%	9%	8%
	Authentication tokens	31%	9%	12%	26%	15%
	Smart cards/physical access control	34%	8%	13%	27%	11%
	PKI/digital certs	19%	15%	21%	23%	15%
	Biometrics	6%	5%	10%	47%	24%
	Password security/SSO	31%	9%	18%	20%	14%
	Firewalls	74%	12%	3%	2%	3%
	File/doc access control	41%	8%	8%	16%	19%
	Web access control/authorization	42%	17%	10%	12%	12%
	Laptop security (hardware)	27%	11%	11%	24%	18%
	Air gap products	7%	3%	5%	32%	44%
	IS audit tools	36%	16%	15%	12%	14%
	Vulnerability assessment	33%	20%	15%	11%	14%
	Data/e-mail encryption	30%	16%	15%	17%	14%
	VPNs	39%	25%	12%	8%	9%
	Wireless security	8%	11%	17%	30%	26%
	Antivirus products	79%	8%	2%	2%	3%
	Web content filters	38%	15%	9%	16%	14%
	Network sniffers	50%	14%	8%	9%	12%
	Port scanners	45%	16%	8%	10%	14%
	Enterprise Sec. Mgmt.	21%	10%	16%	21%	24%
	OS/app hardening/vaults	20%	10%	11%	22%	29%
	DoS prevention tools	19%	14%	12%	21%	26%
	Other products	11%	3%	6%	9%	24%
SERVICES	Managed security services	22%	9%	7%	39%	15%
	Policy development	39%	17%	10%	17%	10%
	Product installation/deployment	42%	16%	7%	16%	11%
	Vulnerability analysis/penetration	36%	21%	13%	13%	10%
	Co-location/hosting	29%	12%	7%	27%	17%
	Other services	6%	2%	2%	9%	18%

Note: Categories left blank excluded.

this year. Worse, only 24 percent of slashed budgets were later restored to the original funding level *(see Figures 7 and 8, p. 36)*.

Comments provided by survey respondents underscore the reality of security funding: your budget may never be satisfactory, and what you have is always subject to "reforecasting" in tough economic times. From an insider's perspective, it's obvious that security should have an integral role in any business. But what's obvious to some will always be misunderstood by others, some of whom control the infosecurity purse strings.

"There are only two things that management will respond to: spending less money and making more money," says a chief security officer from Canada. "Everything has to be explicitly reduced to one of those two, or it will fail."

"[Financial] support is obtained (or not) based on the requirement for security and the potential impact on the business operations," adds a chief security officer based in the mid-Atlantic U.S. "If [management's] perception is 'this is security for security's sake,' then support is unlikely. If the perception is 'real requirement, real threat, real benefit to business operations,' then support is much more likely."

> "If [management's] perception is 'this is security for security's sake,' then support is unlikely.
>
> **–CHIEF SECURITY OFFICER,** mid-Atlantic U.S.

Security: Getting the Message

So, what are the best ways to communicate the "real benefit" of security all the way up the corporate ladder? And what are the most effective ways to maintain or increase funding for new and ongoing security projects?

Respondents to the 2001 survey say that the best way to demonstrate the need for security is through vulnerability assessments or penetration tests, which can be conducted by in-house staff (with permission) or outsourced to a third party *(see Figure 9, p. 38)*. Such tests demonstrate a one-to-one relationship between a specific security expenditure and a specific return on investment, financial or otherwise.

"A few case studies and a few examples of just how easy it is to get key corporate data go a long way to funding specific solutions," says a Midwest security manager, who's quick to add that such techniques are usually temporary. "The real goal should be to integrate security into the minds and hearts of everyone in the company. Once we have people thinking about security issues—even marginally—it makes layering in security solutions that much easier."

Legal and regulatory requirements for data integrity/confidentiality and consumer privacy are also strong motivating factors, according to the survey. Several respondents pointed to emerging regulations for financial institutions (GLBA) and health care organizations (HIPAA) as the most compelling argument for a strong security program.

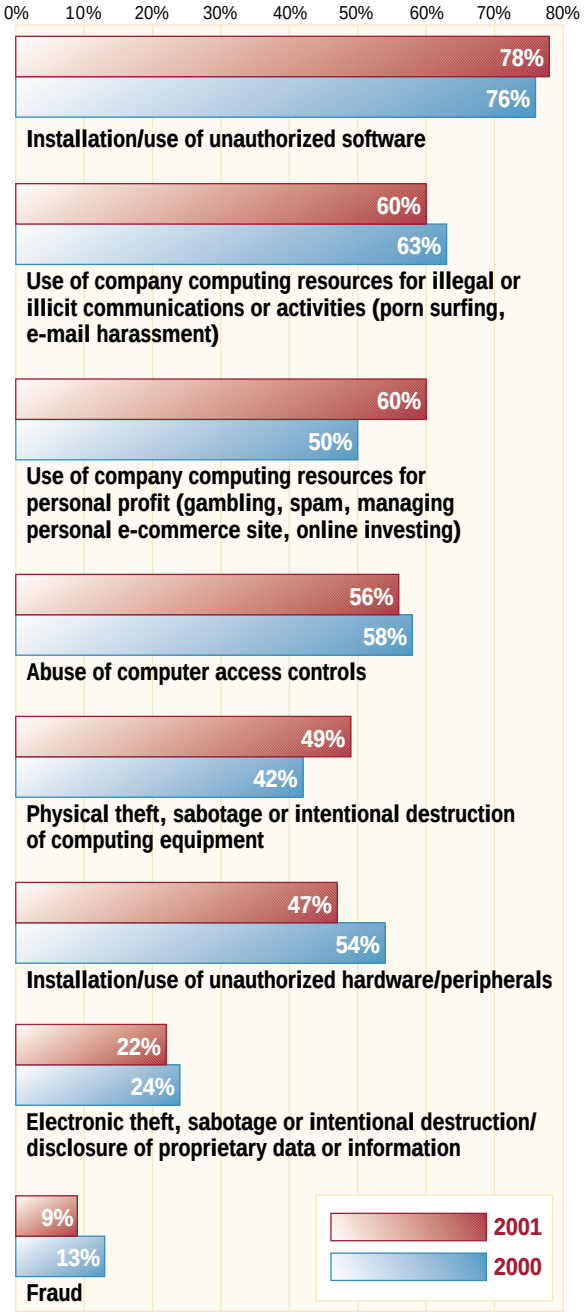
"Federal mandates seem to be helping," says a security manager at a West Coast-based health care organization. "But [they] are still too ambiguous to be truly effective." Another respondent, a chief security officer at a Texas-based health care organization, puts it more bluntly: "Until it's legislated, it ain't happening."

Though "hacker horror stories" make for interesting water

FIGURE 11

INSIDER/INTERNAL BREACHES[1]

% of respondents experiencing these security breaches, 2000-2001

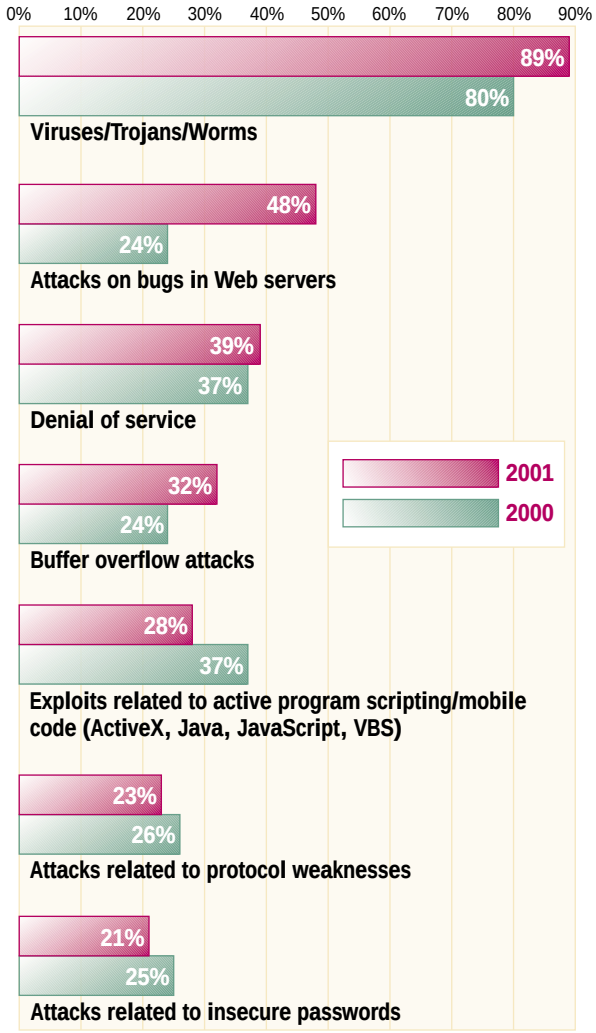


[1] "Insider" refers to full- or part-time employees, contracted workers, consultants, company partners or suppliers.

FIGURE 12

OUTSIDER/EXTERNAL BREACHES[2]

% of respondents experiencing these security breaches, 2000-2001



[2] "Outsider" refers to everyone not included in the description for "insider" in Figure 11.

cooler fodder, survey respondents found them to be a temporary motivational tool at best. "I find hacker stories that happen to someone else provide interesting conversation, but no funding," says a Midwest security manager. "You need to relate concerns to issues within your own IT infrastructure and then prove an ROI on your security investment."

Other respondents insist that the only thing that will make a difference is an actual incident. For all the damage, downtime and headaches caused by Melissa, DDoS, LoveLetter, SirCam, Code Red, Nimda and other global security viruses and attacks, they provided irrefutable evidence of the importance of computer security and risk management. Of course, increases in security awareness are often short lived, and funding increases are often earmarked for fixing only what's broken.

"This nut can't be cracked," says a Canadian IT auditor. "The only way to get any focus on security-related matters is for something bad to happen. When it does, there's momentary focus [on security], but even that is lost within two weeks, not enough time to accomplish anything meaningful."

Adds a Midwest CSO working for a government agency, "With managers from the old school and technology changing every day, there is a reluctance to move to something that's not familiar. Until a significant event occurs, change doesn't occur."

To illustrate his point, the CSO talks about when the SirCam

FIGURE 13

INFOSEC CONCERNS

Indicate your level of concern about the following infosec-related issues and challenges.

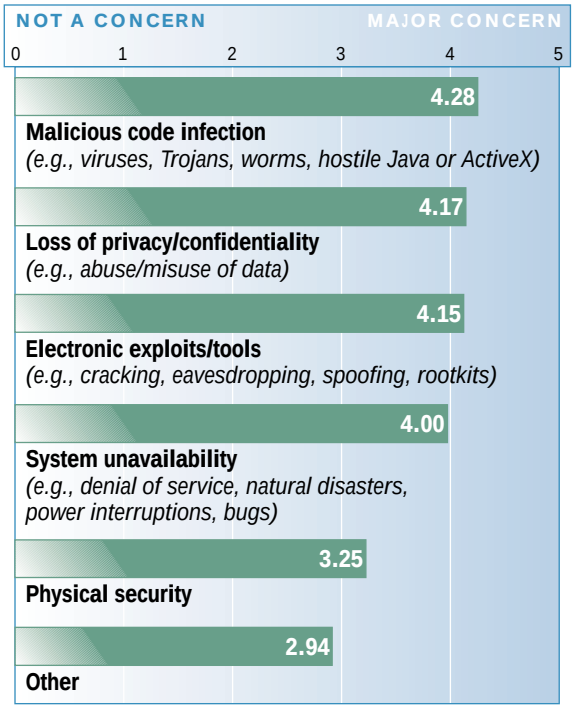
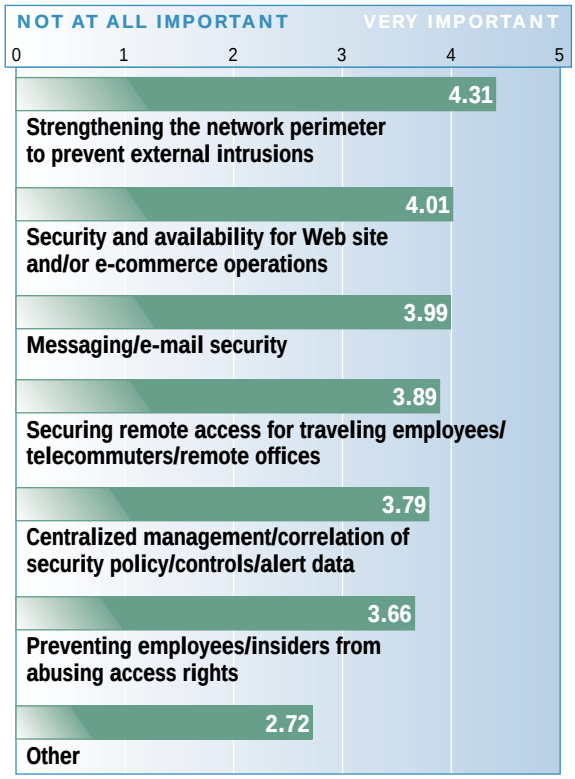


FIGURE 14

INFOSEC PROJECTS

How important are the following projects or programs at your organization?



worm hit his organization. "We purchased an SMTP filter for e-mail filtering/virus detection over a year ago. Not until SirCam had stopped several machines did someone bring up installing the product. Now that it's in and working quite well, the questions are 'why didn't we do this before?' and 'what took so long?'"

> "Anyone in a large company who did not have all of the listed internal breaches occur in the last 12 months is either incompetent or a liar."
>
> –SURVEY RESPONDENT

Security Spending: What's Hot and Not

No other security technology knows the trials and tribulations of a turbulent IT market like public key infrastructure (PKI) solutions. Once hailed as the savior of secure e-commerce, PKI has become the industry's latest whipping boy, ridiculed for its deployment complexity and lack of interoperability and scalability. At the same time, quarterly revenues and stock prices of publicly traded PKI providers have plummeted *(see story, p. 20)*.

While no one would dispute that PKI has suffered its share of black eyes this year, the technology won't be down for long, according to the 2001 Industry Survey. When asked which products and services they plan to purchase next year, 21 percent of survey respondents said they plan to acquire PKI solutions, making it the number one technology buy for 2002 *(see Figure 10, p. 39)*. Other hot technologies for 2002 include password security/single sign-on (SSO) products (18 percent of respondents plan to acquire), wireless security (17 percent) and enterprise security management solutions (16 percent).

At the other end of the spectrum, biometrics solutions appear to be the least desirable technology in 2002. In the wake of last month's terrorist attacks on the World Trade Center and Pentagon, use of face-recognition and finger-scanning solutions will likely grow for select physical access control applications. However, nearly half of the security practitioners in this year's survey said they have no plans to acquire biometrics for network access control.

On the security services side, survey respondents are taking a wait-and-see approach to another hotly debated security offering: managed security services. Only 7 percent of respondents said they plan to outsource their operations to an MSSP in 2002, and 39 percent said they have no plans to do so.

Trends in Cyberattacks and Security Breaches

There are several ways to measure the growth rate of cyberattacks and security incidents. You could compare the rate of a certain attack or incident to that of a similar attack in the past. Or you could quantify the monetary damages resulting from attacks or classes of attacks, and compare those damages to the costs of previous, similar attack vectors. The problem with both of these approaches is there's usually a lot of guesstimating involved, which may undermine the reliability of the statistics and overshadow

more important information, including the reasons why certain attack vectors are more successful than others, or the degree to which you should be concerned about the growth of a certain attack category.

The *Information Security* Industry Survey takes a different approach to quantifying attack and breach growth rates, by measuring the total number of organizations experiencing different classes of attacks or intrusions from one year to the next *(see Figures 11 and 12, p. 40)*. This type of comparison provides an accurate measurement of which attack/exploit vectors are growing the fastest—data that can be used to pinpoint the areas you might want to address in your organization, depending on your company's relative risk exposure.[1]

FIGURE 15

CHANGING PRIORITIES

% of respondents who pinpointed the following as their number one security concern/project/program, 2000-2001

CONCERN	2001	2000
1. Loss of Privacy/ Confidentiality[1]	28%	25%
2. Electronic Exploits/ Tools[2]	25%	20%
3. Malicious Code[3]	21%	26%
4. System (Un)availability[4]	18%	20%
5. Other	5%	5%
6. Physical Security	3%	4%

[1] Includes abuse/misuse of data.
[2] Includes cracking, eavesdropping, spoofing and rootkits.
[3] Includes viruses, Trojans, worms and hostile ActiveX and Java.
[4] Includes denial of service, natural disasters, power interruptions and bugs.

PROGRAM/PROJECT	2001	2000
1. Strengthening the Perimeter to Prevent External Intrusions	31%	20%
2. Security for Web and/or E-Commerce Operations	20%	25%
3. Centralized Management of Secure Policies and Controls	16%	16%
4. Secure Remote Access	12%	13%
5. Preventing Unauthorized Employee Access	12%	9%
6. Messaging/E-Mail Security	8%	8%
7. Other	2%	6%

The good news is that, in eight of the 15 internal/external breach/attack categories measured in the survey, the number of companies hit in 2001 decreased compared to 2000. It's important to note, however, that in many cases the amount of decline was negligible, less than 10 percent. For example, while the number of companies experiencing data theft or sabotage from company insiders decreased by 8 percent, more than one-fifth of all companies still experienced this type of attack.

The most alarming statistic from this data set concerns the dramatic spread of Web-related hacks. From 2000 to 2001, the number of companies whose Web servers were attacked doubled, from

[1] For a discussion of how to quantify risk for your organization, see **www.infosecuritymag.com/articles/march01/columns_executive_view.shtml**.

FIGURE 16

OBSTACLES TO SECURITY

24 percent of the survey pool to nearly half. Similarly, there was a 33 percent increase in the number of organizations hit with buffer-overflow attacks, which often exploit Web server bugs. The growth in both categories is likely due to the increasing number of publicized (and easily exploitable) vulnerabilities in Microsoft's IIS Web server, which was a target in some of the year's most pervasive attacks, such as Code Red and Nimda.

Comments from survey respondents underscore the seriousness of such attacks. "The Web site is the public's view of our company," says one engineer from a Southeastern U.S. IT vendor. "If it goes down, or is hacked or defaced, our reputation is immediately impacted. There is no stopping the cat (news) from getting out of the bag (Internet), [because] the bag is always open."

Viruses, worms and Trojan infections continue to be the most common security incident, with nearly 90 percent of all organizations infected by malware this year, up 11 percent from last year. With new, previously unseen strains appearing in the wild every week, it's easy to understand why malicious code infection is a top concern for infosec professionals *(see Figure 13, p. 42; and Figure 15, p. 43)*. Plus, there's the ever-problematic human factor. "You can't teach people not to open file attachments," comments one systems administrator.

The impact of virus infections in the organization is often measured in terms of damaged data and resources as well as lost worker productivity due to downtime. But the continued high prevalence of virus incidents also carries a reputational risk for the security profession in general. Despite the fact that nearly 90 percent of organizations have server and desktop AV protection in place, viruses still cause millions of dollars in damages and downtime every year. As one computer security consultant puts it, "Try having clients take you seriously about being an infosecurity professional after your corporate e-mail system just infected their e-mail system for the third time in six months."

Given tightening security budgets and limited staff resources, several respondents spoke about their inability to detect many of the survey's attack/breach areas. "We are unaware of any specific external attacks except for [known] viruses, worms and Trojans," says a chief security officer of a Northeastern U.S. health care firm. "We have no measures in place to track or record their affect on our systems."

"They tend to be hard to find," says another respondent, a consultant currently working at a Canadian service provider. "There are so many tools for script-kiddies available that they create problems. We are p-scanned in our network several times a day, people from everywhere just looking for a place to walk in."

Some respondents speculated that, when push comes to shove, most companies experience all of the listed attacks and/or breaches in the survey. "Anyone in a large company who did not have all of the listed internal breaches occur in the last 12 months is either incompetent or a liar," says one respondent.

> "In a layoff economy you are tempting fate with poor security. Company loyalty does not exist when companies do not reciprocate it."
>
> –SURVEY RESPONDENT

Inside Out

This year's survey reinforces the fact that "insider" security incidents are more common than "external" security breaches. For instance, far more corporations reported insider access abuses and equipment theft than denial-of-service or buffer-overflow attacks.

While viruses, Web defacements and stolen credit card databases are the stuff of news headlines, less-publicized incidents such as data theft or destruction by disgruntled former employees can result in far more actual damage. "We have lost a good deal of equipment to theft in the past 12 months," says a security manager at a Midwest military installation. "That has hurt our ability to recover from hardware and software failures."

Says another respondent: "In a layoff economy you are tempting fate with poor security. Unhappy people do not care. Company loyalty does not exist when companies do not reciprocate it."

However, in some ways, comparing internal security incidents to external incidents is like comparing apples to oranges. While more companies experience insider-related problems, some of these problems are more easily controlled than, say, viruses and certain electronic exploits.

"The [insider] abuses tended to occur by persons 'exploring' the system," says a security manager at a mid-Atlantic government agency. "The greater concern was that those who installed the initial systems did not do the appropriate work to prevent some of the access problems. There was no indication that probes were being conducted by persons with talent."

Moreover, what one company defines as a policy infraction or breach may be permitted in another company. It all depends on the business environment and corporate culture. "A lot of stuff is overrated," says a European infosec consultant. "I am not too concerned about unauthorized software and hardware for users. Likewise, Web surfing is not my greatest worry."

With lax security policies, inconsistent enforcement and a growing incidence of viruses and Web hacks, it's not surprising that survey respondents ranked "strengthening the network perimeter to prevent external intrusions" ahead of all other security priorities *(see Figure 14, p. 42)*. Similarly, when asked to pinpoint their number one security challenge for coming months, more respondents pointed to perimeter security than any other project or program *(see Figure 15, p. 43)*.

Running the High Hurdles

If you asked an IT/infosec manager to name the top obstacles to adequate security, most would reply with a wry smile. "I'm better off listing what *isn't* an obstacle," is a common refrain.

While the security hurdles are high and many, budget constraints and a lack of end user awareness continue to top the list, according to the 2001 survey *(see Figure 16, p. 44)*.

While lack of management support is third in this ranking, many would cite it as the source or cause of most other obstacles to security. Fortunate indeed is the security department with a security-aware management team, one that demonstrates a clear understanding of the relationship between risk and the bottom line and—more importantly—acts on it with sustained financial backing.

In commenting on this survey question, one clearly exasperated security administrator summed up the frustrations of many: "If management could just understand how much it would affect our business if we're '0wn3d,' I think the rest of the problems would be taken care of. Although I talk about it, write reports about it, and so on, and they nod their heads, the lack of financial and policy support for my security operations clearly shows that they don't really understand the nature of the problem.

"Sometimes I get the feeling that no one is really listening to me about this stuff," the admin adds. "If I run around like Chicken Little, I'll be dismissed. But if I only communicate earnestly in the typical corporate-speak manner, then the urgency of the message is lost." ◗

SURVEY ARCHIVE, 1998-2001

1998
www.infosecuritymag.com/articles/1998/junesurvey.shtml

1999
www.infosecuritymag.com/articles/1999/julycover.shtml

2000
www.infosecuritymag.com/articles/september00/pdfs/Survey1_9.00.pdf

2001
www.infosecuritymag.com/articles/october01/survey.shtml

ANDY BRINEY (**abriney@infosecuritymag.com**) is *Information Security*'s editor-in-chief. Contributing editor KIRK FRETWELL assisted in the data collection and analysis for this report.

from the trenches

SELECT COMMENTS FROM 2001 INDUSTRY SURVEY RESPONDENTS

"WE FOUND SOME employees letting other workers know their passwords so they could help them perform some work at their computer workstation. These employees didn't have the same level of access and could have (they said they didn't) accessed information in other directories containing sensitive financial information that, if exposed, could have resulted in pretty severe reputational damage."

C-level manager,
West Coast banking/financial services firm

"YOU EXPECT INTERNAL sabotage and take steps to protect the data. You are concerned when the access controls are insufficient to keep out those with evil intent."

C-level manager,
Southwest U.S. military base

"WITHOUT SECURITY POLICIES that have been accepted by management, [and] unless criminal activity occurs, there is little concern. The blasé attitude is like an ostrich hiding its head in the sand."

Administrator,
Northwest U.S. government agency

"EVERY SECURITY CONFERENCE
I attend drills in the fact that most security breaches occur from within. While I believe that is true, I think that internal security problems are as much a management issue as an infosec issue. I can make a totally secure internal network, but it will be unusable for all practical purposes."

Security engineer,
mid-Atlantic U.S.

"OUR SITUATION ISN'T as bad as the general [attack/incident/breach] categories make it sound. Mostly it's just the employees trying to spy on each other. In addition to our manufactured product, we also produce an astounding quantity of gossip and spite."

Security manager,
U.S. manufacturing company

"IF SANS CAN get defaced, and if DRI can lose members' data, how can ordinary businesses be expected to avoid those situations? Execs will say, 'If we cannot prevent situations, why bother spending the money on them at all? Let's put our money elsewhere for more bang for the buck.'"

Computer security consultant,
Canada

"MY BIGGEST CHALLENGE is attempting to get an actual security position created in our job system. Following that, getting free of mundane legacy tasks unrelated to security."

Administrator,
Southwest U.S. university

"WE'RE CONCERNED ABOUT wireless security. Managers, salespeople and service engineers have been getting encrypted access through Lotus Notes. Now they want the same data on Blackberry devices to cellphones. Our security model can't keep up."

Developer,
Northeast U.S. manufacturing firm

"THE GREATEST THREATS to date continue to be malware exploitation attempts from the e-mail vector. Stringent adherence to OS and application product revisions, patches and hot fixes, along with firewall and NIDS software updates and maintenance of AV signatures, has been instrumental in our success."

Consultant,
Southwest IT firm

"LAST YEAR, PROGRESS was made toward security awareness. However, this year, due to economic concerns, we are back to the drawing board. The security industry as a whole is just about starting over."

Manager,
Southeast U.S. security consultancy

"PEOPLE WILL ALWAYS be my key concern. The desire to click through far outweighs the reasons not to."

Consultant,
Midwest U.S. security firm

"MIDDLE MANAGEMENT DOESN'T get it. Upper management understands the direct financial result from an inferior security program, but middle management doesn't see the relationship. Without a direct report relationship/accountability to upper management, my team doesn't stand a chance."

Security manager,
Midwest U.S. manufacturer

"HIPAA IS A NIGHTMARE!"

Administrator,
Midwest U.S. insurance firm

"IT'S CLEAR THAT automated tools (such as 'Hack in the Box') are getting more sophisticated, widely available and easy to use. Any sociopath who wants to do damage with such tools has easy access and little or no risk of getting caught."

Consultant,
Southeast U.S. bank

"WE WILL CONTINUE to see an increase in exploits as long as the media and industry insist on glorifying hackers and crackers as 'brilliant' computer experts. There is a true need to label them what they are: criminals and vandals."

IT auditor,
Canadian manufacturer

"WHY IS CULPABLE ISP negligence, by failing to implement secure subscriber logins and e-mail server authentications, an allowable standard of doing business?"

Consultant,
Southeast U.S.

"SECURITY CAUSES USER inconvenience, so security takes a back seat."

Chief security officer,
mid-Atlantic military agency