2002 SURVEY

SURVEY OVERVIEW

Does Size Matter?

THE SIZE OF YOUR ORGANIZATION MAY BE THE SINGLE BIGGEST BAROMETER OF IT SECURITY'S EFFECTIVENESS.

BY ANDREW BRINEY AND FRANK PRINCE

Admit it: the reason many of us got into IT security was, well, *sex*. Technological sex, to be more specific, the stuff of Clifford Stoll, *Take Down* and BugTraq postings, stack overflows, reflected DDoS, polymorphic worms...and so on. It's cool. It's sexy. It's OK to admit it.

Sure, IT security is sexy, but it turns out all the technological glitz has very little to do with the long-term success of a real-life enterprise IT security program. What's eminently more important—and what must be at the root of how infosecurity practitioners make their decisions, spend their budget and defend their enterprise—is something much more mundane: organizational dynamics.

The problem with many off-the-shelf "security best practices" is that they don't consider the vagaries of complex organizational dynamics, such as vertical industry, operational models, company location, user distribution and corporate financial health. The fifth annual *Information Security* Magazine (ISM) Survey is the first study of its kind to establish security benchmarks for another critical yet under-examined organizational dynamic: company size.

The survey, based on data gathered from 2,196 IT security practitioners[1] in May and June 2002, reveals that organizations of different sizes adhere to distinct patterns of organizational behavior when it comes to IT security. How security is conducted, who in the IT department is responsible for it, how security dollars are spent, how policy is implemented, how the organization responds to breaches and incidents, how security budgets and head count are procured—the success of infosecurity's caretakers at accomplishing these and other central tasks is shaped in large part by the size of the organization in which they work.

[1] 2,196 practitioners completed some portion of the survey. The statistics in this report reflect responses from 215 qualified respondents—those that met five selective criteria for providing reliable information.

INSIDE...

Survey Stats By Organization Size

SURVEY ONLINE

PDF of the Complete Survey
www.infosecuritymag.com/2002/sep/2002survey.pdf

Survey Respondent Comments by Organization Size
www.infosecuritymag.com/2002/sep/2002survey/voices.shtml

Sizing Up Organizational Infrastructures

Many IT security practitioners dream about working in a high-profile job at a big Fortune 500 firm, surrounded by dozens of like-minded security experts all focused on locking down the enterprise network. While very large organizations do have dozens of full- and part-time security staffers—60 in all, according to the 2002 ISM Survey *(see Snapshot B, p. 38)*—it turns out that the lowly security admin at a small-sized organization has a much easier time securing his digital infrastructure.

- The majority of **small organizations** (10-100 machines) have centralized IT organizational models and, given the size of their IT budgets, spend a huge amount on security *(see Snapshot C)*. While security staffing is low—averaging only one full-time and two part-time employees—small organizations spend the most security dollars per user and per machine of any size category. Meanwhile, more than two-thirds say all or most of their security decisions are guided by management-approved policies, and 57 percent say that all or most of their responses to incidents were guided by a predefined IR plan. *(See "Probably More by Luck Than by Design," p. 40.)*

- From an IT security point of view, **medium-sized organizations** (100-1,000 users) are much worse off than their small organizational brethren. They have less budget dollars, proportionally, and are still likely to have only one full-time security staffer, who must increasingly depend on part-time IT personnel to carry out effective security practices. Their ability to set policy, handle incidents in a regular manner and effectively allocate resources are, overall, worse than any other group. Considering their size, the number of incidents they recognize is skyrocketing. Some 70 percent of them had damages from security breaches, a 48 percent increase over small organizations. *(See "Call Me a Firefighter," p. 44.)*

EXECUTIVE SUMMARY

- **IT SECURITY REMAINS a cottage industry when it comes to the establishment and implementation of formal policies and procedures. In multiple ways, IT security is still trying to gain a foothold in the day-to-day activities that govern an organization's operations and culture.**

- **AS ORGANIZATIONS GET larger in size, their security departments are not keeping up with the demands of increasingly complex organizational infrastructures. Security spending per user and per machine declines exponentially as organizations grow, leaving most handcuffed when it comes to implementing effective security practices.**

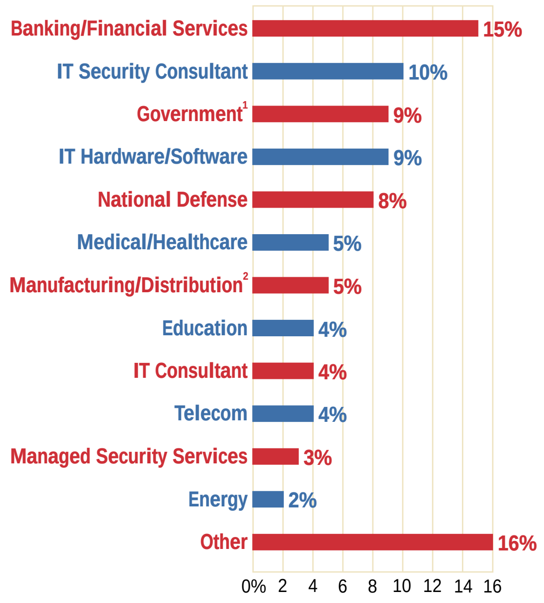
- **SPENDING MONEY ON security does not reduce the number of incidents or the probability or extent of loss stemming from those incidents. But allocating more budget and resources to security does increase an organization's ability to detect loss.**

- **THE GREAT MAJORITY of organizations do not respond to security incidents according to a pre-approved incident response plan. Typically, as organizations increase in size, they rely more and more on structured responses to all types of problems. But that's not the case when it comes to incident response.**

- **IT SECURITY PRACTITIONERS are more concerned about malicious code and the security of authorized users than anything else.**

FIGURE 1

RESPONDENTS BY INDUSTRY

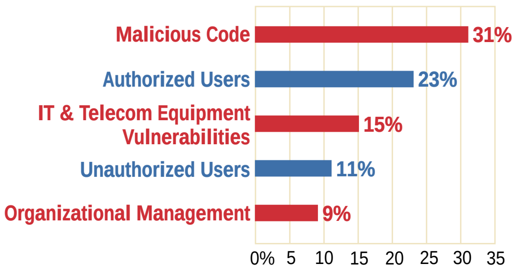


[1] Doesn't include police, national defense or education.

[2] Doesn't include IT software/hardware, transportation or telecom.

FIGURE 2

IT SECURITY'S MOST IMPORTANT PROBLEMS[1]



[1] Multiple answers allowed.

- In **large organizations** (1,000-10,000 machines), security has become institutionalized into the corporate culture via policies—eight in 10 organizations say at least some of their security decisions are guided by them. However, considering their large user base and complex operational infrastructures, large organizations skimp a great deal on security funding and staffing, resulting in systemic "people" problems on all levels of the organization—from uninformed end users to ambivalent upper management. *(See "Training Remains the Weakest Link," p. 48.)*

- **Very large organizations** (more than 10,000 machines) enjoy a growth spurt in security budgets, which are increasing at a much faster rate than overall IT budgets. But given their increasingly complex IT organizational models and burgeoning user base, the $6 million average security budget is actually spread more thinly than at any other organization. Where small organiza-

SURVEY NOTE

The charts below apply to the *entire* pool of qualified survey respondents. To review these charts by organization size, refer to the following pages:

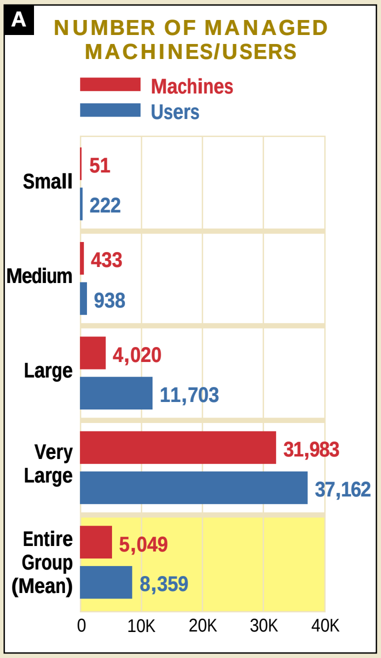
Small Orgs
(10-100 machines) **41**

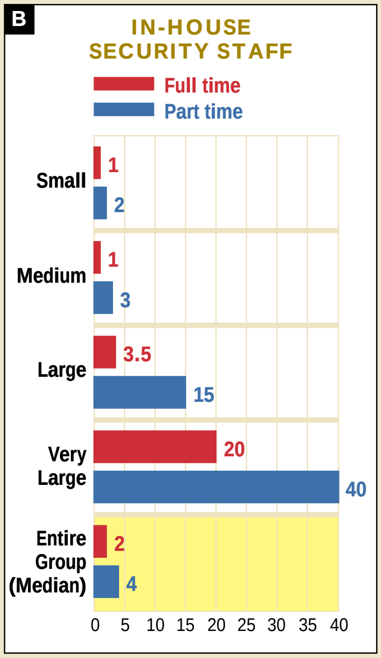
Medium Orgs
(100-1,000 machines) **45**

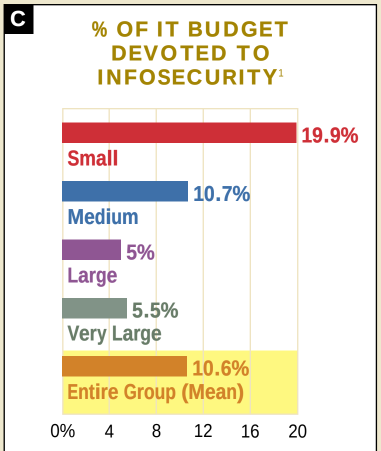
Large Orgs
(1,000-10,000 machines) **49**

Very Large Orgs
(10,000+ machines) **53**

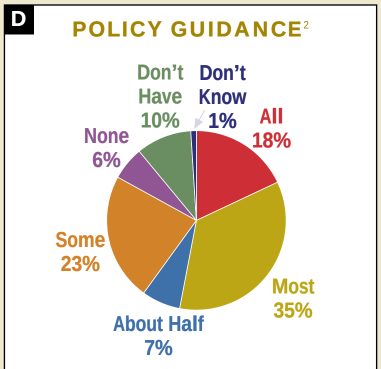
Survey Snapshot


A NUMBER OF MANAGED MACHINES/USERS

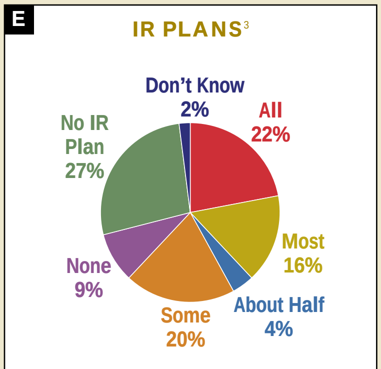

B IN-HOUSE SECURITY STAFF


C % OF IT BUDGET DEVOTED TO INFOSECURITY[1]

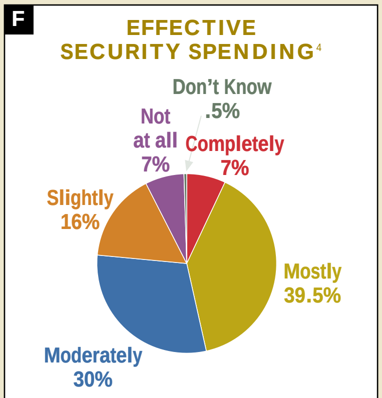
[1] Calculated on a per-respondent basis.


D POLICY GUIDANCE[2]

[2] To what extent were your IT security decisions in the last year guided by policies approved by senior management?


E IR PLANS[3]

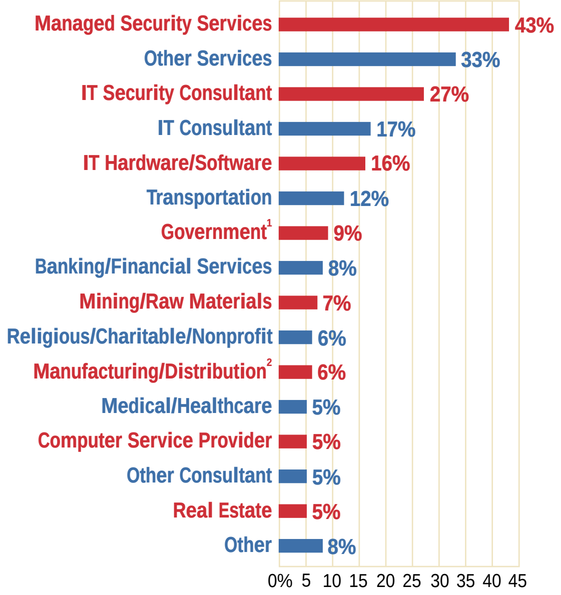
[3] To what extent were your responses to security incidents guided by a predefined incident response plan?


F EFFECTIVE SECURITY SPENDING[4]

[4] How effective was your organization at allocating security resources last year?

FIGURE 3

SECURITY BUDGET AS A PORTION OF IT BUDGET BY INDUSTRY TYPE



[1] Doesn't include police, national defense or education.
[2] Doesn't include IT software/hardware, transportation or telecom.

tions spend more than $5,000 per user on security, very large organizations spend about one-eighteenth of that, roughly $300 per user. Overall, policy adoption and resource allocation is better than at large organizations, though only about a third of organizations in this demographic handled incidents according to an IR plan. *(See "Reputations Can Be Damaged by Poor Security," p. 52.)*

Greatest Threats

While security practices vary greatly from small to very large organizations, security practitioners generally agree about their most pressing problems *(see Figure 2, p. 37)*. When asked what their greatest threat was over the next 24 months, nearly a third mentioned malicious code, while another quarter of respondents worried about securing authorized users. Interestingly, only one in 10 mentioned organizational management, despite the survey's evidence that it is one of the single greatest factors in overall enterprise security effectiveness.

"[Our greatest threat] is viruses, primarily the new polymorphic threats that adapt and change as they spread," says one survey respondent. "Also, the lag time between the time a new virus is recognized and [when] the fix is posted." (For a list of respondent comments by organizational size, see **www.infosecuritymag.com/2002/sep/2002survey/voices.shtml**) ◗

ANDREW BRINEY (**abriney@infosecuritymag.com**) is editor-in-chief of *Information Security*. The 2002 ISM Survey is the fifth in a series of annual surveys that he has conducted for the magazine.

FRANK PRINCE (**fpsec1@grumpybear.com**) is an independent IT research consultant in Nashua, N.H. Prior to starting his own firm, he was a senior analyst at Forrester Research in Cambridge, Mass.

UPCOMING ISM SURVEYS

November 2002	**Threats Survey** www.infosecuritymag.com/2002/nov/minipoll.shtml
December 2002	**Product Survey**
January 2003	**Law, Regulation and IT Security**

TABLE 1

WHO DOES WHAT?*

Job Category	Full-Time Security	Configure Devices/ SW	Monitor Devices/ SW	Manage Individual Contributors	Prepare Budget	Approve Budget	P&L Responsibility	Report to Division	Report to CXO	Report to Board
Administrator/ Operator	54%	**100%**	**100%**	23%	54%	8%	15%	**54%**	15%	8%
Analyst	56%	63%	**81%**	19%	25%	0%	6%	38%	13%	6%
Engineer	**87%**	**73%**	**73%**	60%	27%	0%	7%	33%	13%	0%
Consultant	55%	55%	55%	36%	41%	27%	32%	23%	23%	18%
Unit/Department/ Division Manager	42%	**64%**	69%	**62%**	**64%**	22%	16%	31%	31%	9%
Chief Security Officer	**93%**	34%	56%	**73%**	**88%**	37%	17%	24%	44%	10%
CIO	**80%**	50%	50%	**60%**	**80%**	**80%**	**70%**	30%	**50%**	**50%**
Other Corporate Officer	44%	13%	25%	25%	44%	**56%**	**50%**	6%	25%	25%
Other	51%	51%	59%	43%	54%	19%	8%	38%	30%	11%

*Red numbers represent top three job categories responsible for this function (≥ 50%).

SMALL ORGANIZATIONS
(10-100 machines)

"Probably More by Luck Than by Design"

–Manager, small Canadian government agency

IT SECURITY AT SMALL ORGANIZATIONS IS A BALANCING ACT IN WHICH EVERY PERSON'S ACTIONS CAN TIP THE SCALES.

BY ANDREW BRINEY AND FRANK PRINCE

Every organization is different—but for small organizations, every difference means more. Their success or failure depends in large part on the strengths and weaknesses of a few key individuals, typically those in leadership positions. As a result, a management approach or business philosophy that works well at one may fail miserably at another, if only because their key people have different approaches to similar problems.

IT security doesn't escape this effect. More to the point: IT security in small organizations is often a balancing act in which every person's actions can tip the scales.

"When you're a tiny company, and everybody's doing everything and you're flat out all the time, there's just not a lot of room for organizational structure and titles and roles," says Terry Jones, CTO and acting COO of Eatoni Ergonomics, a New York-based company that makes predictive text entry solutions for handheld devices. "Everyone's wearing all the hats, and it's not so easy to say who's a 'normal user' and who has restrictive privileges. It's much more of a free-for-all."

Upshot

IT org. model	43% centralized
IT budget	$1.454 million
IT security budget	$132,243
# of incidents responded to (per year)[1]	5.78
Pct. suffering loss or damage due to incidents	49%
Biggest impact on security	44% – preventing intrusions

[1] "Incidents" refers to a malicious disruption of normal operating procedures that requires human intervention (Mandia and Prosise).

Staffing

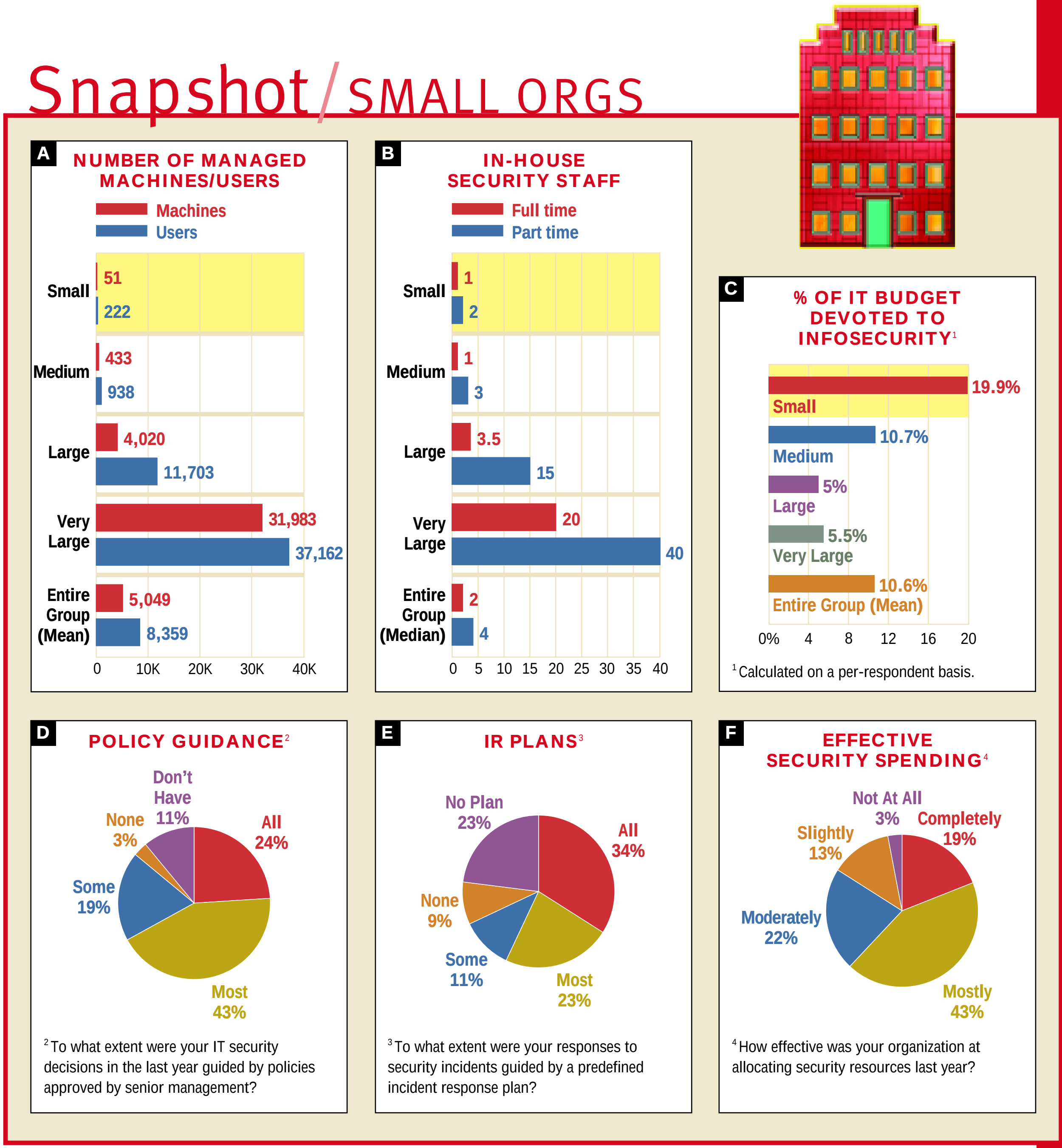
According to the 2002 ISM Survey, half of small organizations have only one full-time security employee, with two other part-timers chipping in when necessary *(see Snapshot B, p. 41)*. But there's a deeper story: Many small organizations have *no* dedicated security staff. For those that do, the security program's success (or lack thereof) is often a direct reflection of the knowledge and skill of just one individual.

"Small companies don't have the resources to pay for a team of people to look after security," says Jones. "It's also a question of expertise. You just want someone who knows enough to deal with security properly."

Spending

Given the size of their IT budgets, small companies spend a huge amount of money on security *(see Snapshot C)*. And most survey respondents feel they're getting bang for their buck: Nearly two-thirds said their security spending was completely (19 percent) or mostly effective (43 percent)—far more than that reported by larger companies *(see Snapshot F)*.

Snapshot/SMALL ORGS



[1] Calculated on a per-respondent basis.

[2] To what extent were your IT security decisions in the last year guided by policies approved by senior management?

[3] To what extent were your responses to security incidents guided by a predefined incident response plan?

[4] How effective was your organization at allocating security resources last year?

That being said, security spending at small organizations remains a tale of the "haves" and "have-nots." They either have an ingrained security culture and spend whatever's necessary to secure their technical infrastructure, or they suffer from a lack of security head count and don't make significant security investments. There is very little in between.

Eatoni's Terry Jones falls into the first camp. "The problem is actually not that difficult," says Jones, who oversees the uptime and security of approximately two-dozen workstations. "If you set up a reasonable network architecture with security in mind, then there are only so many entry points into your system, and presumably everything else that needs to be locked down is locked down. Then it's just a matter of monitoring those holes that have been left open."

As for the small firms without the ingrained security culture or management support…well, many are out of luck.

"No set portion of [our] IT budget is reserved for security," says a manager at a computer service provider, underscoring the reality at far too many small organizations. "Security is approved on an as-needed basis."

Policy Effectiveness

Overall, small organizations have an easier time than their larger counterparts implementing successful infosec policies *(see Snapshot D)*. This is partly a reflection of their size and relatively simple operational model. Nearly half of small companies in the survey have a centralized IT infrastructure, and 50 percent allocate one full-time security person to 21 or fewer users and 25 or fewer machines—a much more favorable ratio than at larger companies.

While their policy adoption and incident response planning is solid overall *(see Figure 4, right)*, a disproportionate number of small firms don't have security or incident response policies at all—putting them at greater risk than larger companies that may be able to absorb an attack.

"Smaller companies have a lack of policies about what they let their users do," says Jones. "Anything goes and quite literally, sometimes anything *does* go."

FIGURE 4

GUIDED RESPONSE

Portion of respondents who said most or all of their responses to security incidents were guided by an incident response plan.

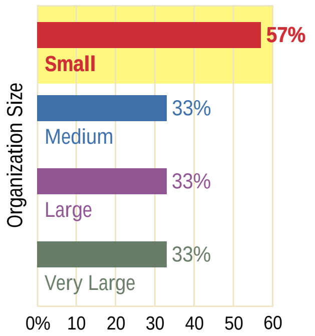
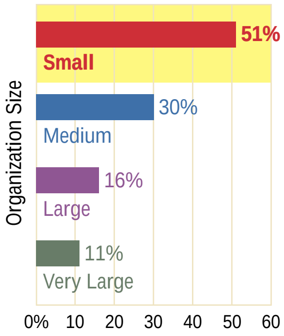


FIGURE 5

NO LOSS

Portion of respondents reporting no loss of any kind from security incidents



Security Incidents and Loss

On average, each small organization responds to roughly six security incidents per year. However, the most compelling statistic of this portion of the survey may be the number of small organizations that say they suffered no loss from security incidents in the last year: 51 percent *(see Figure 5, above)*. There are several possible explanations for this:

- Small companies have less exposure as "hacker targets" compared to larger companies. "[Our lack of incidents] is probably more by luck than by design," says one survey respondent. "Who we are (small government organization) and where we live (small Canadian province) likely has a bearing, since we're not a big multinational, and the financial pickings are pretty slim."
- Security professionals at small organizations manage a less-complex infrastructure and fewer machines and users, proportionally.
- The 23 percent of small organizations that have no incident response plan at all may be detecting fewer breaches, which would bring down the overall average number of incidents reported for the category.

"Although we have not had any damage," says a CIO from a managed security service provider, "we've had a couple of close calls and a lot of aggravation over false positives." ◗

VOICES Security practitioners at small organizations sound off.

On time commitments...
"I don't think buying more products necessarily helps you. In a way, the place where people fall down very often is they don't put enough time into it. They think security is a static task. It's not; it's an ongoing activity that requires an investment of time."

TERRY JONES
CTO and Acting COO, Eatoni Ergonomics

"The more time you have to stay on top of things, the better off you are, because automated tools can only go so far. You need to read your e-mail and find out if someone found a hole. You need to look for the patch, then install it and make sure it works. And that all takes time."

On security spending...
"What you tend to see happen is a smaller organization will buy new machines…and the default configurations are insecure. They put them on the network and that's about it. They think because it's a brand-new machine and it has the latest version of an operating system that it's somehow secure, and they don't need to worry about it. That's not true. Or they think if they install, say, some virus detection software, then they can relax. And that's not the case."

On the lack of manpower and expertise...
"The big problem with network security is you have a huge number of machines and a small number of people actually able to secure them. Even when you're keeping an eye on things, it's quite nerve-racking, because when you see someone trying to attack your machine, your pulse tends to increase and you start to wonder and worry. And if you look at the log files, you see that every day—sometimes many, many times each day. You get used to it, but you can't relax entirely."

From the Survey

"All members of the firm have access, but that access is restricted based on department and function within the department. [We have] very tight access controls. We practice what we preach."
–IT security consultant

"[Our greatest threat is] the unknown, [and] Microsoft's lack of building security into their products and their inability to produce good patch/service pack distribution models and analysis tools."
–CIO, managed security services firm

"Our organization lacks a strong security stance and policy coming from management."
–Consultant, manufacturing/distribution

FOR MORE SURVEY VOICES, SEE www.infosecuritymag.com/2002/sep/2002survey/voices/small.shtml

MEDIUM ORGANIZATIONS

(100-1,000 machines)

“Call Me a Firefighter”

–High school technology coordinator

IT SECURITY PERSONNEL AT MEDIUM-SIZED ORGANIZATIONS ARE BETWEEN A ROCK AND A HARD PLACE.

BY ANDREW BRINEY AND FRANK PRINCE

Compared to small organizations, medium-sized companies have more complex operational environments and suffer far more damage from cybersecurity incidents. Yet their security budgets and staffing are proportionally less than that of their smaller compatriots. Indeed, nearly one-third of medium-sized companies have *no* full-time security personnel, and another third employ only one full-time security staffer *(see Figure 6, p. 46)*.

And compared to large or very large organizations, medium-sized organizations can’t leverage economies of scale. Across-the-board security policies are hard to implement because they lack large clusters of uniform users or equipment. What’s more, more than a third of the respondents in this category don’t have an incident response plan. Of those that do, 16 percent said their plan didn’t guide *any* of their responses to security incidents *(see Snapshot E, p. 45)*.

In a nutshell, medium-sized organizations have a harder time setting policies, handling incidents and effectively allocating security resources than small, large or very large organizations.

No wonder one survey respondent, a high school technology coordinator, likened his job more to firefighting than security administration.

Adds another respondent, a security architect at a financial institution, “Senior management [doesn’t] realize that security administration is a full-time position and not something the network admin can do ‘on the side.’”

Upshot

IT org. model	42% hub/spoke; 28% distributed
IT budget	$7.571 million
IT security budget	$359,631
# of incidents responded to (per year)[1]	5.87
Pct. suffering loss or damage due to incidents	70%
Biggest impact on security	31% – user awareness; 30% – preventing intrusions

[1] “Incidents” refers to a malicious disruption of normal operating procedures that requires human intervention (Mandia and Prosise).

And this from an IS director at a health care organization: “Security is only one small, but important, part of my position. We are severely underfunded and understaffed, so I provide [both] management and hands-on administration.”

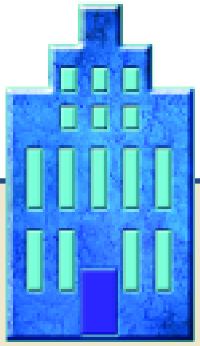
Policies

Data from the ISM 2002 Survey shows why the high school tech coordinator feels he’s being burned. Only 40 percent of medium-sized organizations say all or most of their security decisions are guided by management-approved policies—lowest among all organizational categories *(see Snapshot D)*. Worse, more than a quarter of respondents said they either don’t have management-approved policies or, when they do, the policies are like mom’s rules about smoking: they seldom guide actual practices.

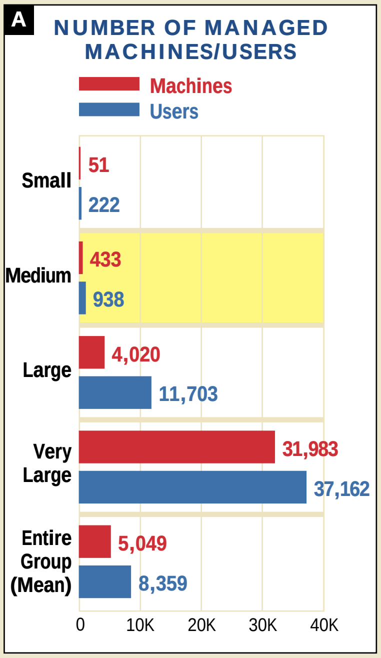
The problem, according to some survey respondents, is a lack of commitment and education on the part of senior management.

“We are just beginning to try to implement true policies,” says one engineer. “We have a few ‘loose’ guidelines. [But the] culture here is very open, and [management] is

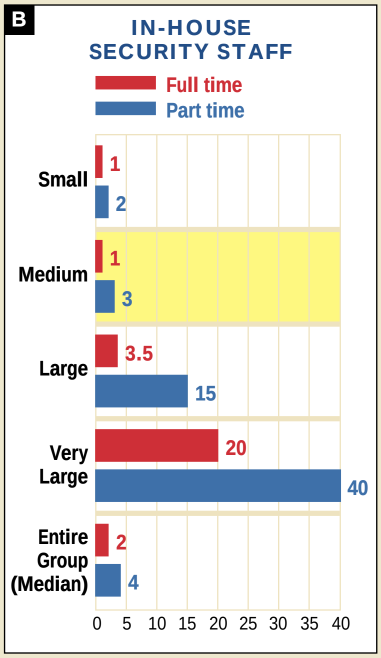
Snapshot/MEDIUM ORGS



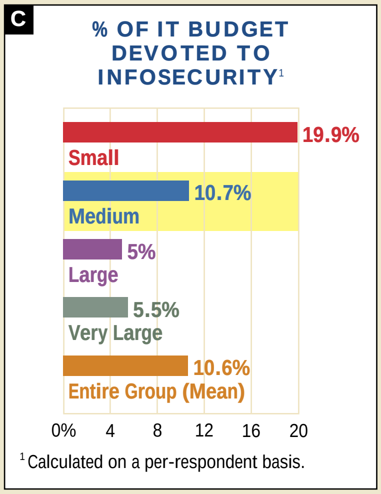
A NUMBER OF MANAGED MACHINES/USERS



B IN-HOUSE SECURITY STAFF

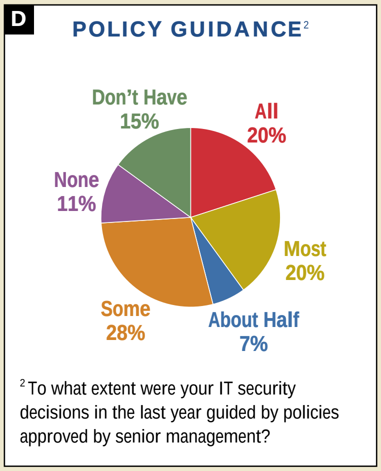


C % OF IT BUDGET DEVOTED TO INFOSECURITY[1]



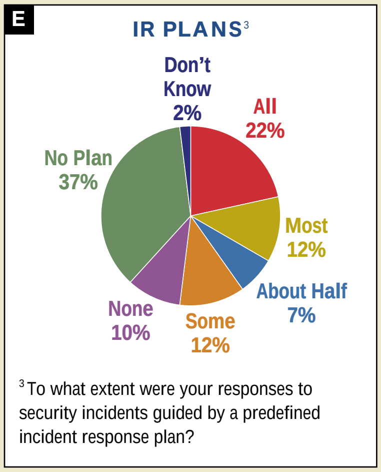
[1] Calculated on a per-respondent basis.

D POLICY GUIDANCE[2]



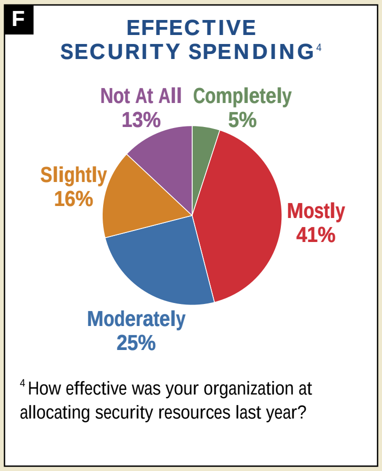
[2] To what extent were your IT security decisions in the last year guided by policies approved by senior management?

E IR PLANS[3]



[3] To what extent were your responses to security incidents guided by a predefined incident response plan?

F EFFECTIVE SECURITY SPENDING[4]



[4] How effective was your organization at allocating security resources last year?

hesitant to close [access to] anything at all."

Adds an admin at an educational institution, "[Policies are] guided by senior management who don't know the difference between Windows and Office. It's like having preschoolers run the military."

Another respondent puts it even more succinctly: "I *am* the policy," he says.

Incident Response

Nearly 70 percent of medium-sized organizations suffered financial, material or reputational losses due to security incidents *(see Upshot, p. 44)*. That's a 48 percent increase over small organizations, even though both groups report the same number of security incidents per year: six.

Comments from respondents suggest that, given their stretched resources and comparatively more complex environments, medium-sized organizations have more difficulty detecting breaches and cyberattacks. Combine that with their greater exposure on the Internet, and we see how attacks might not be recognized until they cause some damage.

"Last year, we discovered that our environment was not completely patched to prevent some of the basic ways to get into the site," says Teresa Pudi, VP of information systems for Georgia-based Habitat for Humanity International. "We had to do much more in that area of work because there were break-ins."

So there may be a silver lining in the black cloud of management indifference: Pudi says the security lapses at Habitat for Humanity were the driving force for better security.

"Those break-ins elevated the issue of security—that's extremely important. It also made people realize that if we don't spend the right resources, we'll have to…undo something. That undoing can take a long time and be costly. We can't afford for certain systems to be down."

FIGURE 6

SCHIZOPHRENIC STAFFING

Full-time security staffing at medium-sized organizations.

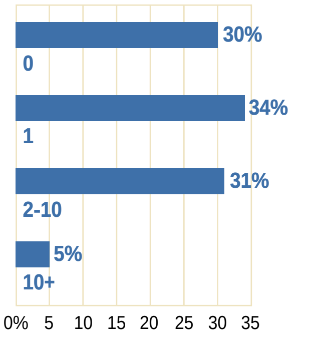
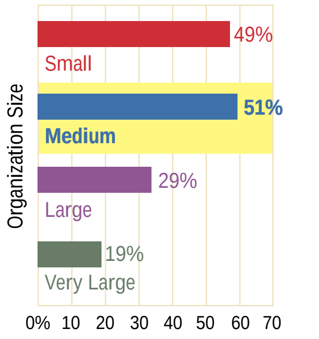


FIGURE 7

SECURITY TRAINING

Organizations without any employees with post-secondary IT security training.



Budgets and Expenditures

Pudi's challenges with IR mirror those of other medium-sized companies. "Some money was shoehorned into useful corners," says an admin at an educational institution. "[But] most was burnt locking barn doors after it was too late."

Throughout the 2002 ISM Survey, there are two central themes relative to intrusion prevention: (1) management and user awareness are critical to preventing security breaches; and (2) the ever-increasing complexity of the IT security environment is making prevention more and more difficult. The point is this: Awareness training and keeping up with technology require investments in professional security staff. Yet medium-sized organizations don't make that investment. In fact, 51 percent of them don't have *any* staff with post-secondary security training *(see Figure 7, above)*.

Education isn't the only investment they don't make. Security budgets don't scale with IT budgets for medium-sized organizations. While they do spend roughly 10 percent of IT budgets on security—nearly identical to the average for all companies—their IT budgets are 480 percent greater than small organizations' IT budgets, while their security budgets are only 261 percent greater—again, far below the average increase *(see Figure 9, p 52)*. ◗

VOICES **Security practitioners at medium organizations sound off.**

Nonprofit vs. For-profit…

"I've been all my life in the for-profit and switched to nonprofit a year ago. In for-profit, you can afford more from a product or service perspective, because it's directly reflected in the bottom line. Here, what are we protecting? Image. Bad publicity. Donor information. There is a certain scale of criticality or importance.

TERESA PUDI
VP of Information Systems for Habitat for Humanity International

On security culture…

"What is happening [is] security became part of everyone's job. It became part of a mainstream. It has been moved to many various groups—application, administration, network, infrastructure. I think it's a good thing, because awareness and work in the overriding structure, design and architecture can be synchronized."

From the Survey

"Though I am the sole person responsible for security measures (firewall, AV, logs, etc.), it's only about 15 percent of my job. I [also] do all Internet/intranet/Web server/database development and maintenance." *–Manager at law firm*

"I am the only person interested in security. If I don't push for something, it will probably not be implemented, controlled or audited.… We don't have a set true security section. I have to argue for any resources once a year, and will usually not get half of them. This past year, I was only able to spend about $20,000 on specific security items. That isn't even close to one-tenth of 1 percent of our profits." *–Engineer*

"Our current policy is, 'All employees will do their best to be secure.' We are working on a corporate policy, but it is dragging out—like waiting for Christmas." *–Senior scientist at energy company*

"No policies makes conducting security an exercise in frustration. If not futility.… It's not that we don't know what to do. It's not even that we don't have the money to do it. It's that we have no policy, so constructing effective security rules is impossible. We can't tell you authoritatively who should be allowed to do what, in what circumstances, and what penalties there are for noncompliance.… Finally giving up on user education and just fascistically stripping all non-plaintext elements from e-mail has been a huge boon." *–Administrator at educational institution*

"My users just have no concept of computer security…and it does not seem they have any desire to understand." *–Technology coordinator, high school*

"Last year, out of about 300 systems, only three (1 percent) had to be rebuilt. This is credited to good security, training and awareness, management involvement and strong measures taken at the e-mail server and firewalls." *–Telecom consultant*

FOR MORE SURVEY VOICES, SEE
www.infosecuritymag.com/2002/sep/2002survey/voices/medium.shtml

LARGE ORGANIZATIONS
(1,000-10,000 machines)

"Training Remains the Weakest Link"

–*Information systems security officer, National Defense Agency*

LARGE ORGANIZATIONS HAVE "PEOPLE PROBLEMS" AT ALL LEVELS.

BY ANDREW BRINEY AND FRANK PRINCE

What's life like for security staff in large organizations? Shortfalls in security budgets, management support, security staffing and end-user training conspire to create "people" problems at all levels. Making matters worse, large organizations have complex infrastructures and high exposure on the Internet, making them frequent hacker targets. Pressed by other concerns, non-security management doesn't pay much attention to security, leaving the full-time security staff—what there is of it—to deal with what one survey respondent calls "ordinary, unalert, uninterested, lax, ignorant, uncaring end users."

"Policy enforcement definitely becomes more difficult as the company grows," says Andrew Bagrin, director of business technologies for Tennessee-based Regal Entertainment. Following a series of mergers, the $2.5 billion film distribution conglomerate now runs one of the world's largest theater chains. "But actually, as you grow bigger, more people understand it, whereas before you'd have people arguing with you about 'Why can't I do this?' or 'What do you mean I can't get in?'"

Spending

Organizations of all sizes struggle with lack of security funding, but the 2002 ISM Survey shows that the problem is particularly acute at large companies. These organizations only spent 5 percent of their total IT budgets on security, less than any other sized organization and less than *half* of the average for our survey respondents *(see Snapshot C, p. 49)*.

Where large organizations appear to skimp most is in security head count. They employ fewer full-time security staff per user than any other organization. In 50 percent of surveyed large companies, there's only one full-time security employee per 1,000 users.

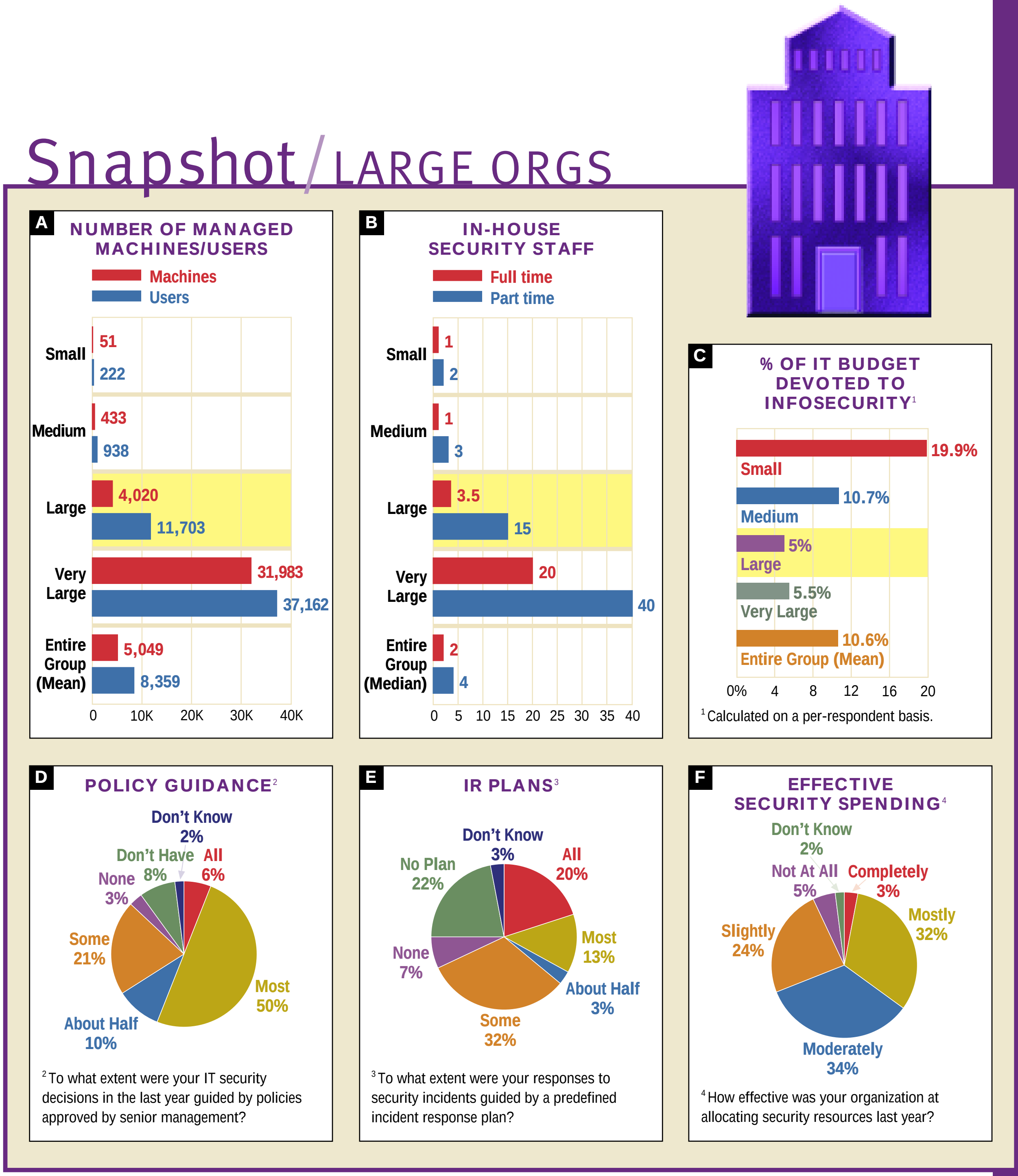
Moreover, large organizations are disproportionately reliant on part-time security staff—and that means trouble. "The problem," notes an auditor at a large financial institution, "is that employees with part-time security

Upshot

IT org. model	35% distributed; 31% hub/spoke
IT budget	$84.794 million
IT security budget	$1.339 million
# of incidents responded to (per year)[1]	11.5
Pct. suffering loss or damage due to incidents	84%
Biggest impact on security	29% – user awareness

[1] "Incidents" refers to a malicious disruption of normal operating procedures that requires human intervention (Mandia and Prosise).

Snapshot/LARGE ORGS



[1] Calculated on a per-respondent basis.

[2] To what extent were your IT security decisions in the last year guided by policies approved by senior management?

[3] To what extent were your responses to security incidents guided by a predefined incident response plan?

[4] How effective was your organization at allocating security resources last year?

responsibilities are usually ruled by the most demanding customer-service issues, not the most security-sensitive issues."

Given the lack of security funding, staffing and upper-management support, it's no surprise that that only about a third of large organizations said their security spending was completely or mostly effective, the lowest of any organizational size category *(see Figure 8, p. 50)*.

Large organizations throw a lot of money into IT—their average IT budget is roughly $85 million. Indeed, they are the only size category where general IT spending scales with the number of machines supported.

What *doesn't* scale, however, is security spending on a per-machine basis. Our survey shows they spend only

TABLE 2

SECURITY EXPENDITURES

Money spent per user and per machine

Company Size	$/User	$/Machine
Small	$3,360	$5,204
Medium	$1,158	$1,027
Large	$1,081	$328
Very Large	$315	$295

about $328 per machine—about one-third of medium-sized organizations and *one-fifteenth* of small organizations *(see Table 2, p. 49)*. The priority is on automation of operations—but not, correspondingly, on security. The result? Lots of pressure on security, bad decision making and a failure to tend to the basics.

"We were idiots," says a manager at a media programming company. "[We] pursued sexy NIDS crap when we should have focused on effective antivirus and backup strategies."

Policy and Incident Response

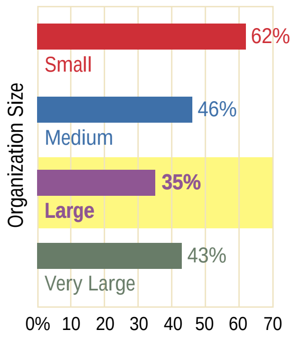
The good news is that, despite all the budgetary obstacles, large organizations believe they're mostly successful at implementing and following management-approved policies. Eight out of 10 survey respondents said at least some of their IT security decisions were driven by policy *(see Snapshot D)*.

The bad news is that two-thirds of large organizations still don't follow an IR plan when dealing with breaches *(see Snapshot E)*. Large organizations face twice as many incidents as small organizations, and 84 percent suffer operational losses or financial damage as a result *(see Upshot, p. 48)*.

FIGURE 8

EFFECTIVE SPENDING

Portion of respondents saying their security resource allocation was completely or mostly effective.



People

Getting management support for security is the never-ending battle. According to Bagrin, it's even harder to educate business-minded executives that traditional economic models don't always apply to IT security.

The "problem is trying to get the executives in your company to understand what's the ROI in security," he says. "That's a real tough one, because nobody feels the ROI until the first time you've been hacked…. That's one reason security's always a hard sell."

A survey respondent from a large medical/health care organization put it this way: "Many of our problems would have been much less severe if there had been uniform management and application of available security measures and training across the enterprise."

The survey numbers back him up. At half of the large organizations surveyed only one in 10 full-time security staffers had any advanced security training. Two-thirds reported that fully implementing existing security measures would have reduced their losses. And 60 percent said that keeping up with OS and application patches would have cut security losses. ◗

VOICES Security practitioners at large organizations sound off.

On growing up…

"Since we've gone through a merger and became a $2.5 billion company, we've gone to more formalization. We've stepped away from everybody wearing the same hat to more of a 'Andrew's in charge of security. All the stuff has to go through him.' We're not just going to make changes on the fly now…. I think we're trying to get more to that point of being a bigger company, since we are growing and learning to run a little more efficiently."

ANDREW BAGRIN
Director of Business Technologies, Regal Entertainment

On security brain drain…

"Good security people are hard to find. You've got to be able to trust them a lot, especially with technical people and technical knowledge."

From the Survey

"The single best thing we have done for security in our organization was to write and have [management] sign off on a security policy."
–IS security manager, energy company

"Security policies were always the driving point for designing and developing new controls. But dollars and cents make it happen, and numerous initiatives have been canceled due to budget constraints."
–Chief security officer, financial institution

"Typically, I have to write the security policy and market it to management. They never do anything proactively."
–Engineer, manufacturing/distribution

"One of our offices is four blocks from Ground Zero. We responded to 9/11 in accordance with our disaster recovery plan….The disaster closed down our New York operations, but [we] were able to pick up that work by allocating it to several of our other data centers. In fact, we were responsive in helping other companies quickly recover in their support to their customers."
–Security director, application service provider

"When your Web site is defaced, and more than 300 customers see it, that can be quite a loss of face."
–Analyst, state government agency

"We didn't have an incident response plan until after the first incident. In other words, it took an incident to get a plan."
–Chief security officer, government agency

"The most serious threat would be the loss of skilled personnel who keep us protected in spite of management's blissful ignorance of their effectiveness and dedication. The notion that we could just go out and hire another 'Larry' could be our downfall."
–Corporate officer, nonprofit

FOR MORE SURVEY VOICES, SEE
www.infosecuritymag.com/2002/sep/2002survey/voices/large.shtml

VERY LARGE ORGANIZATIONS

(10,000+ machines)

"Reputations Can Be Damaged by…Poor Security"

–Auditor, financial institution

SECURITY BUDGETS ARE GROWING THE FASTEST AT VERY LARGE ORGANIZATIONS, BUT THEY SPEND LESS ON USERS, MACHINES.

BY ANDREW BRINEY AND FRANK PRINCE

With IT budgets of nearly $300 million, security budgets approaching $6 million, and IT security staffs of around 60 (full-time and part-time), you might guess that very large organizations are feeling bullish about their IT security. Guess again.

Of all the company size categories in the 2002 ISM Survey, very large organizations have the broadest range of IT organizational models, evenly broken out into distributed, decentralized and hub-and-spoke architectures *(see Upshot, left)*. And they have to deal with all the problems that come with *just being big*—for instance, the average very large organization has more than 37,000 users and almost 32,000 machines. So, $6 million and 60 security staffers don't go as far as you might expect. Calculated on a per-respondent basis, very large organizations require each full-time security staff member to cover more than 8,000 users and nearly 3,000 machines—and that's a lot by any measure.

Upshot

IT org. model	33% distributed; 29% decentralized; 29% hub/spoke
IT budget	$294.2 million
IT security budget	$5.981 million
# of incidents responded to (per year)[1]	25.9
Pct. suffering loss or damage due to incidents	89%
Biggest impact on security	42% – user awareness; 32% – risk analysis

[1] "Incidents" refers to a malicious disruption of normal operating procedures that requires human intervention (Mandia and Prosise).

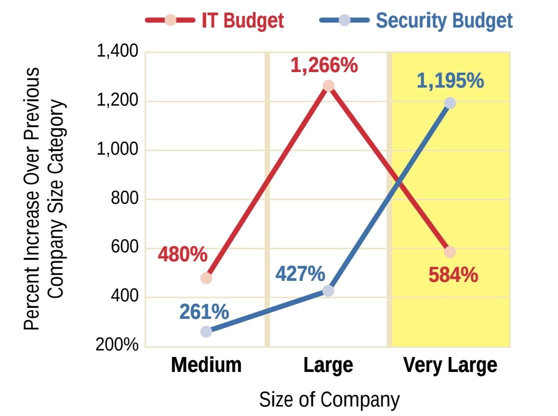
Budgets and Spending

The $6 million IT security budget of very large organizations represents a huge increase over the next-smallest category, large organizations. Where the IT security budget increases 261 percent from small to medium companies, and 427 percent from medium to large categories, it increases a whopping *1,195 percent* from large to very large categories *(see Figure 9, below)*.

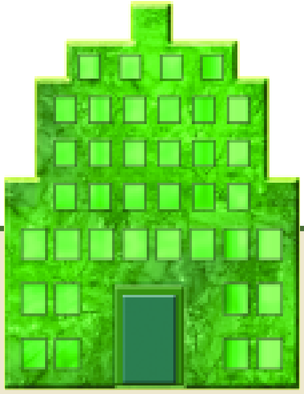
At the same time, the increase in IT budget from large to very large organizations (584 percent) is much *less* than

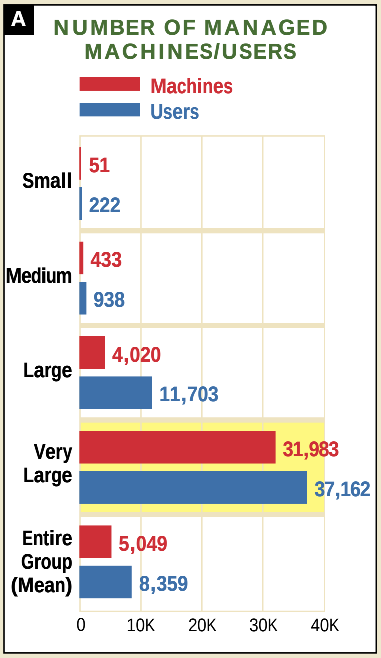
FIGURE 9

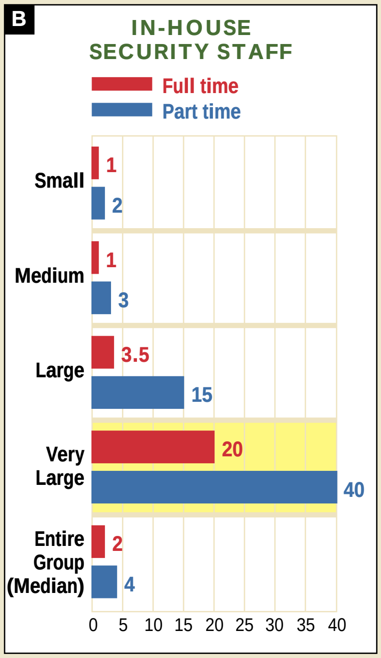
INCREASE IN % OF IT AND SECURITY BUDGETS BY COMPANY SIZE

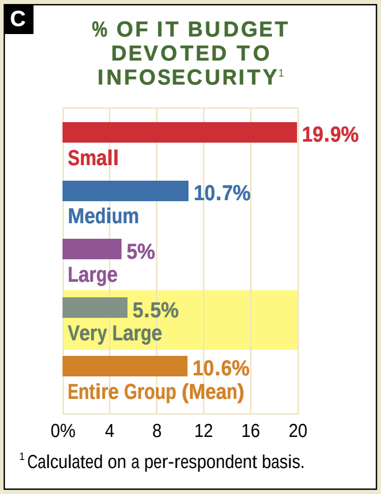


Snapshot/VERY LARGE ORGS

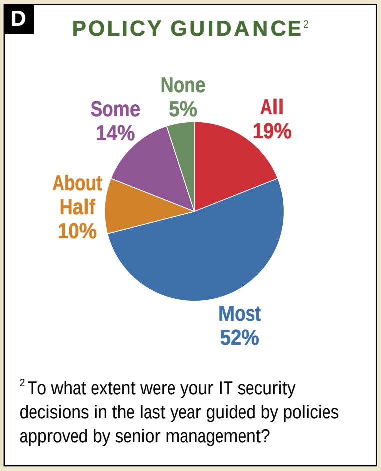



A NUMBER OF MANAGED MACHINES/USERS

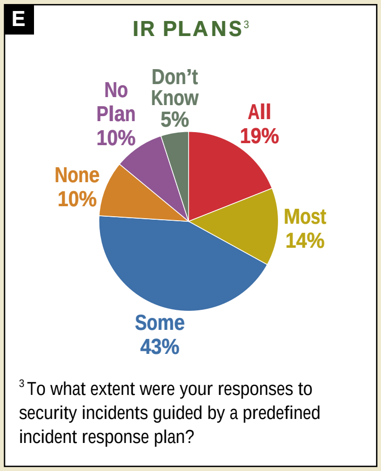

B IN-HOUSE SECURITY STAFF


C % OF IT BUDGET DEVOTED TO INFOSECURITY[1]

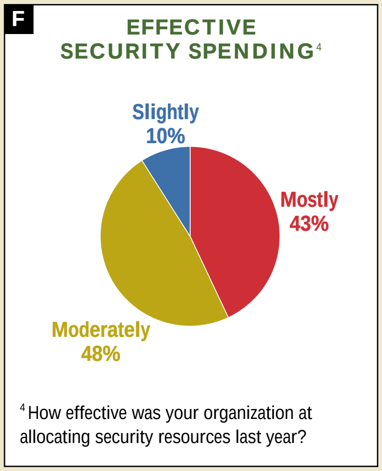
[1] Calculated on a per-respondent basis.


D POLICY GUIDANCE[2]

[2] To what extent were your IT security decisions in the last year guided by policies approved by senior management?


E IR PLANS[3]

[3] To what extent were your responses to security incidents guided by a predefined incident response plan?


F EFFECTIVE SECURITY SPENDING[4]

[4] How effective was your organization at allocating security resources last year?

that from medium to large organizations (1,266 percent). In this sense, very large organizations buck the trend of all other organizational size categories in the survey. As they mature into very large companies through acquisitions, mergers and operational build-out, their IT security budget actually grows faster than their IT budget.

But the growth rate of security budgets isn't the only barometer of security spending. Unlike small, medium and even some large companies, very large businesses have enormous scalability challenges. Even with their growing security budget, they spend only about $5.50 on security for every $100 spent on general IT. And dollars spent per user ($315) and per machine ($295) are the lowest of all size categories.

Policies and Procedures

The sheer size and complexity of global corporations means that, inevitably, standards, policies and procedures get applied unevenly across the company. About half of the organizations surveyed said their security spending was "mostly effective." But, as one university chief security officer points out, "Cultural changes [take] much longer than expected. Just throwing money at a project doesn't necessarily mean it will get finished faster."

Nevertheless, very large organizations are among the best at institutionalizing security policy. Seven out of 10 respondents said that all or most of their IT security decisions were guided by management-approved policies. But broad policy support belies a deeper challenge for IT security managers at these organizations, who are often in the position of serving two masters: corporate-level policy and division-level policy.

"Although there are always day-to-day decisions that will deviate from established [corporate] policy, all decisions based on group or unit direction were based on approved policies," says a division manager at a very large financial institution.

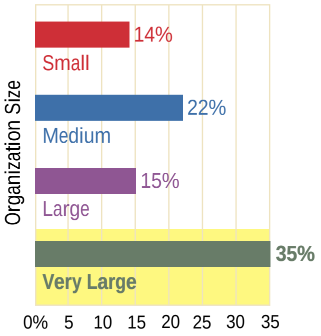
One reason for solid overall policy adoption in very large organizations may be increased government oversight in health care (via HIPAA) and financial services (via GLBA).

"Some policies have been put in place because of legislation related to the protection of confidential information and anti-terrorist laws," says a chief security architect at a financial institution.

FIGURE 10

IMPACT OF BREACHES, OPERATIONAL VS REPUTATIONAL

Portion of respondents saying breaches affect their reputation as much or more than they affect IT or business operations.



Incident Response

The bad news is that solid overall policy support doesn't usually carry over into effective incident response. Only about a third of respondents in this category said they use an IR plan to respond to all or most of their security incidents. Given their IT security budgets and amount of risk exposure, it's stunning that nearly one-fifth of very large organizations either don't have an incident-response plan or never use it *(see Snapshot E, p. 53)*.

The sheer size and organizational complexity of very large companies provides insight into the nature of the problem. "There is no completely effective security (yet) for everyone," says one security consultant. "The only thing you can do is to set yourself up as effectively as possible with incidents as they occur."

One explanation for the lack of IR policies is that very large organizations are much more concerned with reputational loss than operational loss. And for good reason: They are much more likely to have suffered damage to their reputation than any other size category *(see Figure 10, above)*.

"At some point, implementing the 'full/best' security measures will sharply reduce your operational throughput," says a server security team leader at a government agency. "[It] takes a while to determine the most appropriate settings relative to the business." ◗

VOICES **Security practitioners at very large organizations sound off.**

On security reporting...
"Since Sept. 11, state, local and federal authorities have tried to get their arms around the potential threats to the nation's infrastructure—including the telecommunications infrastructure. They have asked us questions like, 'What are your 100 most vulnerable places in the network?'"

BILL SMITH
CTO and President of Interconnection Services, BellSouth

"As much as we would like to help the government in its attempt to help us, we believe it would be counterproductive to share such information widely because if it were released, it would provide a terrorist with a roadmap to our key locations. Unless the government agrees that it can protect our information, we will continue to respectfully decline such blanket requests."

From the Survey

"Policies aren't necessarily 'approved'—just posted."
–Analyst, financial institution

"Senior management is more concerned with making everything easy for users than more secure for the company."
–Security engineer, national defense

"As viruses become easier to create with less programming knowledge, the threat to loss of productivity increases dramatically. Another key problem: When many IT people were laid off, the lack of corporate knowledge to be able to know what needed to be done to solve an incident/perform a task or grant access was diminished. Timeliness went way down for a while."
–Engineer, consumer electronics

"The recurring problem is a lack of competence of the technical teams in charge of configurations/security of the servers environments, and a lack of resources ($ and people). Too often, security (technology, process, means) is not a priority for the top management of a company."
–Project manager, telecommunications firm

"Wireless is becoming much more prevalent and difficult to control. Creating a DMZ segment to isolate the wireless traffic and control access points is going to prove to be something that the business will drive and the security field must react to."
–VP, information security, financial institution

[Our greatest risk is] the inherent complacency that you may get into once the standard security measures have been deployed, e.g., firewalls, IDS, VPNs, etc."
–Chief advisor, corporate security and architectures, financial institution

"One of our main roles is security policy creation; most of our security policies were completely rewritten within the past year."
–IT security consultant

FOR MORE SURVEY VOICES, SEE
www.infosecuritymag.com/2002/sep/2002survey/voices/verylarge.shtml