

The Global State of Information Security

BY SCOTT BERINATO

WITH RESEARCH EDITOR LORRAINE COSGROVE WARE

2005

A worldwide study by *CIO* and PricewaterhouseCoopers reveals a digital landscape ablaze, with thousands of security leaders fighting the flames. But amid the uncertainty and crisis management, there's an oasis of strategic thinking.

Every day it's something else.

Millions of personally identifiable records stolen.

Intellectual property left on a laptop that's gone missing.

Corporate espionage rings that stretch from the United Kingdom to the Middle East and use IT to infiltrate companies.

Phishing scams by the thousands: puddle phishing, Wi-phishing, pharming.

Then there's spam and spyware, zombie networks, DDoS (distributed denial-of-service) attacks and session hijacking. Online auction fraud. Online extortion. We haven't even mentioned good old viruses and worms, but those still work too.

To borrow from forestry parlance, information security is an escaped wildfire. And according to "The Global State of Information Security 2005," a worldwide study by *CIO* and PricewaterhouseCoopers (PWC), you are the firefighters, desperately trying to out-flank the fireline and prevent flare-ups and firestorms. It's a thankless, impossible business.

In this environment, just holding your ground is a victory, and that's what you're doing. This is the third annual edition of the survey—once again the largest of its kind with more than 8,200 IT and security executives responding from 63 countries on six continents. Each year the data has shown incremental improvement in the tactical battle to react to and fight off security incidents.

At the same time, and the data shows a notable lack of focus on actions and strategies that could prevent these incidents in the first place.

There's also a remarkable ambivalence among respondents about compliance with government regulations, a clear lack of risk management discipline, and a continuing inability to create actionable security intelligence out of mountains of security data.

Just 37 percent of respondents reported that they had an infor-

mation security strategy—and only 24 percent of the rest say that creating one is in the plans for next year. With increasingly serious, complex, targeted and damaging threats continuously emerging, that's not a good thing.

"When you spend all that time fighting fires, you don't even have time to come up with the new ways to build things so they don't burn down," says Mark Lobel, a security-focused partner with PricewaterhouseCoopers. "Right now, there's hardly a fire code." Lobel compares the global state of information security to Chicago right before the great fire. "Some folks were well-protected and others weren't," he says, but when the ones that weren't protected began to burn, the ones that were protected caught fire too.

Of course, with the survey's thousands of pages of data and tens of thousands of data points, the overall security picture is a little more complex than "Everyone's tactical; no one's strategic." Some respondents show signs of embracing a more holistic approach than others. So we'll delve into one industry sector—financial services—as a best practices group that, while still struggling to put out fires, has devoted more time, resources and strategic thinking to its information security posture than the average respondent. We'll also highlight some other encouraging numbers that suggest that more companies than ever are laying the groundwork for a more strategic information security department.

In all, we'll look at eight distinct cuts of the data from "The Global State of Information Security 2005," and post several more online (www.cio.com/091505). Use the data to benchmark yourself and to glean ways you can start to beat back the flames. Maybe even create a fire code so that if a cow does knock over a lantern, the whole city won't burn. *Results start on Page 64.* ▶▶▶

Inside the Study

"The Global State of Information Security 2005," a worldwide study by *CIO* and PricewaterhouseCoopers, was conducted online from March 14, 2005, through April 23, 2005. Readers of *CIO* and *CSO* (a *CIO* sister publication), and clients of PricewaterhouseCoopers were invited via e-mail to take the survey. The results shown here are based on the responses of more than 8,200 CEOs, CFOs, CIOs, CSOs, and vice presidents and directors of IT and information security from 63 countries. The study's margin of error is ±1%.

The study represents a broad range of industries including computer-related manufacturing and software (11%), consulting and professional services (11%), financial services/banking (9%), government (9%), education

(7%), health care (5%), telecommunications (5%) and transportation (2%).

Thirty-two percent of the executives surveyed reported total annual sales of less than \$100 million, while 17% reported sales between \$100 million and \$999.9 million. Twenty-one percent of the survey base said their organization's annual sales exceeded \$1 billion, while 17% were nonprofit organizations. (Twelve percent didn't answer the question.)

Fifty-four percent of the respondents held IT titles including CIO, CTO, vice president, director and manager while 10% were information security professionals. Twelve percent held CEO, CFO or non-IT director titles while 24% listed "other."

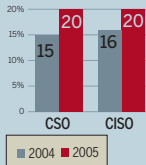
Sowing the Seeds of Strategic Security

As information security gains more status in the organization, security improves.

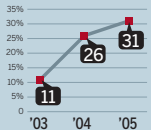
The Good News

More executive attention is being paid to the security function.

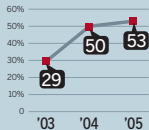
We employ a CSO or CISO.



IT and physical security report to the same executive leader.



We have some form of integration between physical and IT security.



Where/to whom does your CISO or equivalent information security executive report?



IT'S CLEAR FROM THE DATA that respondents spend most of their time in reactive mode: responding to incidents, deploying firewalls, and dealing with everyday nuisances like spam and spyware. Ironically, the most common proactive step respondents take is to develop business continuity and disaster recovery plans. So even their proactive steps are investments in reactive measures.

Having said that, a few numbers did pop out that suggest that the foundation is being laid for a time when information security may become more strategic. This year more companies employed security executives and focused on integration between physical and

information than in the two previous years.

"Security has gotten more visibility since I started watching this sector 11 years ago, no doubt," Lobel says. "Most encouraging is the combination of physical and information controls. All business eventually will have an e-business component, and as business evolves, security has to evolve with it and include physical and information security in equal proportions. Some of the data is starting to show that evolution, but we're clearly not there yet."

Security's rising profile is most encouraging when you cross-reference the governance numbers with effectiveness. Those companies where the function resides near the top have a far better security posture than the average respondent. Security's more strategic at those companies that have elevated the role. For example, only 37 percent of respondents said they have an overall security strategy. At companies with CSOs, that number leaps to 62 percent. Likewise, 80 percent of companies with CSOs also employed a CISO or equivalent, compared with about 20 percent overall.

Companies with an executive security function also reported that their spending and policies are more aligned with the business and that a higher percentage of their employees comply with internal information security policies. Companies with a security chief also measured and reviewed information security policies more than those without a security executive, and they were far more likely to prioritize information assets by risk level.

Resources are dialed up at companies with a security executive too. They averaged more full-time employees at their companies and higher budgets. They were almost twice as likely to have

a security budget separate from the IT budget and, while they were equally likely to get additional monies for security from the IT department, companies with executive infosec leaders reported getting more money more often from other lines of business, such as legal, risk, and compliance and regulatory groups.

Companies that haven't elevated the role outnumber those that have. But if companies that have elevated information security tend to act more strategically (and more companies are doing that), then it follows that information security is getting more strategic. It's early on in the trend, but it's a positive.

The Big Picture

You can read more results from "The Global State of Information Security 2005," including additional results about network breaches, and find links to past years' surveys at www.cio.com/091505.



Surveillance World

The bigger the company, the more it watches its employees.

THERE'S A SUDDEN AND DRAMATIC RISE in companies monitoring their employees. The upsurge, part of a trend toward more surveillance both in public and in private, can be attributed to several factors.

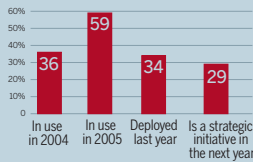
First, CISOs want to rein in instant messaging and other applications. Those apps not only sap employee productivity but they're easy vehicles for intellectual property theft and other information leaks. Second, security execs need to put down rampant spam and malware—feral creatures that often get into networks through unauthorized usage by employees and knock systems offline, slow down overall network performance, spread viruses and open up the network to further attacks. Third, they want to shield the company from liability when employees use peer-to-peer networks to download copyrighted material, such as movies and music. And finally, there's the evergreen insider threat. Thirty-three percent of all infosecurity attacks originated from employees, with another 28 percent coming from ex-employees and partners. In short, the only way security chiefs believe they can control the technologies that their employees use is to watch what they do with them. That's why 88 percent of respondents either have monitoring in place or plan to by year's end. It follows, too, that bigger companies have more to monitor and more resources to do it, and hence will monitor more.

Ironically, PWC's Lobel points out, it could be the unintended consequence of another, positive trend that's helping nurture the moni-

Eyes Wide Open

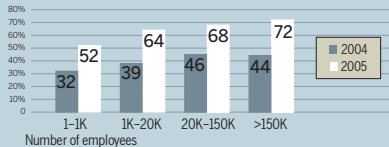
Tracking workers' information access is this year's hottest trend.

Monitoring of employee use of Internet/information assets



88% either monitor now or plan to in the coming year.

Percentage of companies monitoring workers



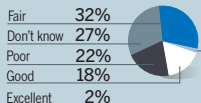
toring culture. "With more and more security organizations reporting outside of IT, they really don't integrate day in and day out with the folks rolling out the systems," he says. That is the trend. As we saw on Page 64, more companies have information security reporting to the CEO or other departments, and more are integrating it with the physical security function. Currently, the only way to combat that disconnect between who's deploying the applications and who's securing them is to monitor. "In fact," says Lobel, "the less security reports to IT, the more you'll need this watchdog function."

Respondents who profess some involvement with Homeland Security: **38%**

When the color-coded threat level changed, my information security activities changed

All respondents	9%
In aerospace	18%
In energy/utilities	29%
In government	22%
In transportation	21%

How would you rate DHS's effectiveness in handling information security activities?



DHS Gets Low Marks

Information security executives have a negative perception of the Department of Homeland Security. The color-coded alert system has proved useless.

CYBERSECURITY HAS BECOME something of a standing joke inside DHS, a buried priority that was even rumored to be moving to the Office of Management and Budget, of all places. It's also endured the departure of several appointees who left after only a few months, including Richard Clarke, Howard Schmidt and Amit Yoran. It seems DHS's attitude toward information security is reflected in our respondents' perception of how the agency has handled it. More respon-

dents rated DHS's handling of information security as "poor" than those who rated it "excellent" and "good" combined. DHS is also under pressure from Congress and other critics to either radically change or altogether scrap the color-coded alert system, and the numbers suggest that that's the right move in terms of infosec, since it hardly registered, even with critical infrastructure companies, when the feds declared Orange Alerts.

Compliance? What's That?

The majority of information security executives range from ambivalent (at best) to downright dismissive (at worst) about the intentions, effect and pertinence of security regulations.

ONE PWC ANALYST called these numbers scary, but which is scariest? Is it the comparatively low number of respondents who are in compliance? Or the shockingly high number of respondents who cop to not complying even though they know that they have to? Or could it be the startlingly low number who believe that the regulations apply to them? (The list of regulatory mandates in the survey was much longer, but other, lesser regulations showed a similar pattern.)

The third one may be the most telling. Just 11 percent of respondents said they needed to be in compliance with California's SB 1386 law, which mandates that companies report breaches of personal data to consumers. In fact, any company that has even

one customer in California must comply with the law, and surely more than 11 percent of U.S. respondents' companies do business in our most populous state. Similarly, more than half said they didn't need to comply with Sarbanes-Oxley, and four out of 10 respondents in the health-care industry said that the Health Insurance Portability and Accountability Act (HIPAA) didn't apply to them, which seems impossible on the face of it.

But what do the numbers mean? Here are two theories, both of which probably play some role: One, the regs are confusing and difficult to comply with. This would explain the low numbers of respondents who believe they needed to comply with HIPAA

or Gramm-Leach-Bliley regulations. They simply don't understand how the rules apply to them. Another theory is that the regulations have, in respondents' minds anyway, few if any teeth. Companies don't fear any serious repercussions for not complying with the regulations, either because the mandates are too vague to really be enforced, or the regulatory agencies aren't devoting resources to enforcement.

Supporting the "lack of teeth" theory is the fact that only a third of respondents reported having compliance testing in place, and only a quarter link their security organization to the compliance group.

Lobel offers a third factor: "There's just a lot of regs for these guys to deal with."

Safe Deposits

The financial services industry takes care of security business better than the rest of us. Learn from their best practices.

	Overall	Financial services
Security budget as % of IT budget	13%	12%
Budget <\$50,000	42%	21%
Budget >\$1 million	10%	21%
Budget will increase next year	47%	58%
Employ a chief privacy officer	17%	26%
Employ a CISO or CSO	34%	51%
Have an overall infosec strategy	37%	57%
Less than 50% employee compliance w/ policy	30%	17%
Policies not aligned w/ business	21%	7%

Full-time security employees (mean number)

For all respondents: **30**

For financial services: **46**

FOR THE PAST TWO YEARS we've highlighted a best practices group, culled from those respondents who professed that they were "very confident" in their information security. This year, our best practices group is not sorted by confidence, but rather pulled directly from one industry—financial services.

The financial services sector has long been presumed to practice superior information security, largely because of the preciousness of its assets (money) and the fact that its business is carried out almost entirely on IT systems. The stakes are higher, the risks are higher, so the information security protection must be higher too.

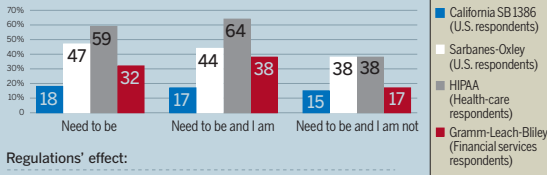
To an extent, the data supports the idea that companies in the money business tend to be more strategic and more secure than the rest of us, and, it turns out, even more confident. Another factor that helps financial companies excel is that they tend to be bigger, and bigger companies usually have more resources. (Then again, bigger companies often have a harder time with governance, and financial services companies, by this data, show strong organization.)

But we also chose the financial services sector as a best practices group for several other reasons. The stakes are fiercely high in a business shooting huge sums of money around IT networks. Also, financial services companies already use risk models, returns on investment and other strategic tools in other parts of the business and have begun to apply those same tools

No-Compliance Zone

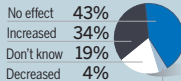
Fewer companies than expected are following new government rules.

What is your compliance with the following U.S. regulations?

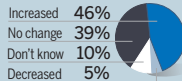


Regulations' effect:

On spending



On effectiveness of information security



Indeed, security mandates so far have targeted specific threats, industries or niches without a single overarching standard for companies to aim for. In this survey, we listed 43 regulations, all of which some respondents said they needed to comply with, and some respondents even added ones we didn't put on the list. Inevitably, companies will prioritize their limited resources to comply with those they consider most pressing and let others go.

But the point remains: The negative attitude toward regulation (only half of respondents believe it has increased the effectiveness of information security) indicates that they haven't had the intended effect, at least on information security.

to information security. Finally, the financial community knows regulations and has for a long time. When it comes to information security, the financial services industry is in a position where everyone else is headed.

The differences between that place and the place most people are today is pronounced. Start with money. Financial services companies have bigger security budgets, but not necessarily bigger vis-à-vis the overall IT budget. To whatever extent these companies are more secure than the average company, that superiority can be attributed to more efficient spending, and spending on strategic planning, not technology. One simple example of this is investment in network firewalls. It was the fifth most cited strategic priority for next year with all respondents, but it doesn't even make the top 10 with financial services companies. Same for data backup, which is number three overall but not on financial services companies' radar. These companies have these important technologies in place but also seem to have shifted priorities, perhaps understanding that more technology doesn't mean more security. (The one type of technology financial services companies do seem to be investing in is identity management—not surprising as a reaction to the ID theft epidemic.)

On the other hand, the banks were far more likely to have listed compliance testing as a priority for next year compared with the overall respondent base. You should anticipate this happening to

your company, and start preparing sooner rather than later, as regs—including the big ones such as Sarbanes-Oxley, but also local ones such as California's 1386 law and whatever new regs come out of the current identity theft pandemic—start to take hold and you have no choice but to do compliance testing.

And just because the financial companies seem to be more strategic doesn't mean they shy away from using threats to justify investments. While financial companies are slightly more likely to use ROI and contribution to business objectives as justifications for security investments, they are still far more likely to rely on legal and regulatory requirements, liability and revenue impact to justify their investments. Interestingly, half of all financial services respondents said "common industry practice" was one justification for security investments—suggesting either some level of information sharing amongst companies in the industry, or at least a copycat culture where many security executives try to keep up with the good security Joneses.

One area in which the financial services sector doesn't seem to outperform the rest of the respondents is integration with physical security practices. Watching the year-over-year numbers next year in this area will be important given the number of high-profile data thefts that used physical security weaknesses—or at least the disconnect between the information security practices and physical security practices—to gain access to personal records.

So Many Breaches, So Few Insights

When it comes to malicious activity on their network, information security executives have more information than ever, but that doesn't mean they know what to do with it.

THE NUMBERS ON INCIDENTS, downtime and damages have remained steady, but some other numbers in this year's breach data are unsettling. First, the sharply rising number of respondents who report damages as "unknown," up to 47 percent this year from 40 percent two years ago, suggests that respondents have neither the time nor the means to truly calculate losses from a breach, or if they considered the attacks

minor, they didn't bother. The increased sophistication of attacks during the past year could also contribute to the rising "unknown" group.

The more complex attacks hit more complex targets. Take the hypothetical identity theft of 1,000 customer records. Many experts are concerned about "deferred loss identity theft," wherein thieves sit on stolen identities for months or years until victims

believe the danger has passed. It's hard to put figures on potential outcomes like that.

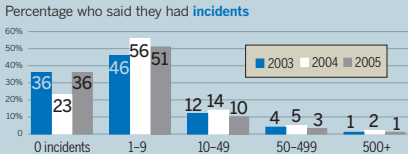
Other "unknown" responses get one's attention too: "Unknown" showed up in survey responses as the second most prevalent attack type, the fourth most common attack method and the third highest attack source. Plus, data or material damages trail only firewall and IDS logs as the means of dis-

Continued on Page 72

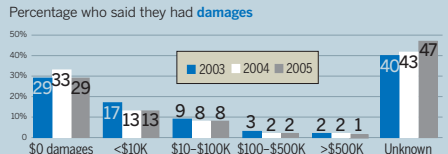
The Great Unknown

Security executives still have trouble identifying who is attacking them, where the attack is coming from and how it's being done.

After billions have been spent on security defenses, the number of reported incidents remains steady...

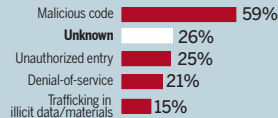


...and information security executives know less than ever about the damage the incidents cause...



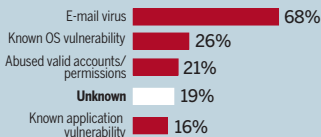
Executives often don't know how they have been attacked...

Top five attack types



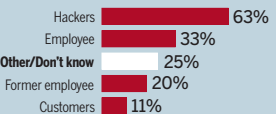
...or where they've been attacked from...

Top five attack vectors



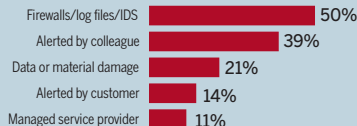
...or who's attacking them.

Top five attack sources



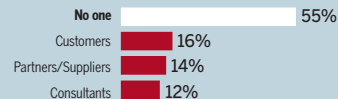
Top five bearers of bad news

How did your organization learn of the attacks?



Who do you tell?

Contacted as a result of attack:



Continued from Page 70

covering attacks. In other words, information security professionals most often react. They learn of attacks after the damage is done. And often once the events happened, they couldn't figure out what it was, where it came from or who did it.

CIOs, CISOs and CSOs have gotten quite good at collecting and logging events on their networks—organizing their haystacks—but haven't been able to reliably turn all that data into intelligence—efficiently finding the needles before they are pricked by them. A long-term strategic goal of all information security departments should be to reorganize so that they work as an intelligence unit rather than just a data collection unit.

Next Year's To-Do List

Respondents identified their top strategic priorities for the next year. Here are the 10 most common answers.

1. Disaster recovery/business continuity
2. Employee awareness programs
3. Data backup
4. Overall information security strategy
5. Network firewalls
6. Centralized security information management system
7. Periodic security audits
8. Monitoring employees
9. Monitoring security reports (log files, vulnerability reports and so on)
10. Spending on intellectual property protection

This list further reinforces the reactive nature of information security. Awareness programs often score high as a strategic priority because they're relatively low-cost. One should expect number 10 on this list will shoot up in priority next year, given the steady stream of identity thefts and other major information crimes.

Follow the Money...Please!

Information security is getting more money, but exactly how much and from where isn't always clear. It's more evidence of a lack of strategic direction.

IN PREVIOUS YEARS when we asked what your information security budget was, we didn't include "don't know" as an option. This year, we did, and Bang! A full one-fifth (22 percent) of the information executives responding said they didn't know how much money their companies budget for infosecurity. More signs of a lack of proactive, strategic focus. Not good.

Good news: The information security function can shake some money out of other departments' pockets to supplement its own appropriations.

The larger companies are most guilty of not tracking their spending well. About 40 percent of the 1,700 companies with \$5 billion in revenue or more said they didn't know their information security budget.

Bigger companies, with more divisions and probably a more distributed world view, might have a harder time pinning down all the monies devoted to information security. In fact, the bigger companies reported much higher usage of money from other departments for security than smaller companies did. Many bigger companies also have integrated information and physical security, making their information security budget a less distinct entity.

We didn't report the spending trends here—whether budgets were increasing, decreasing or staying the same because for the third straight year those numbers stayed relatively constant. Except for one telling tidbit. We added "don't know" to the question of whether or not budgets will increase, stay the same or decrease, and 16 percent said they weren't sure which way their budgets were headed. **CIO**

Where the Money Comes From

One-fifth of respondents have no idea.

Where, besides the information security budget, does money for information security come from?



Information security budget as a percentage of IT budget:



Is your information security budget part of your IT budget or separate?

