THE GLOBAL STATE OF
INFORMATION
SECURITY

Our annual global survey,
with PricewaterhouseCoopers,
of more than 7,000 senior
executives finds you're
spending more on security.
**But technology doesn't buy
peace of mind.**

A Joint Research
Project of *CIO* and *CSO*
in partnership with

PRICEWATERHOUSECOOPERS 🄿

THE **GOOD** NEWS 👍

You've beefed up your IT security arsenal, and you're focused on compliance. But you're still vulnerable. Here's why.

BY KIM S. NASH

👎 THE **BAD** NEWS

Not to be alarmist, but WAKE UP, PEOPLE! Our information security is, in many ways, failing.

Ask the 11 alleged hackers charged in August with breaking into TJX and other retailers by way of insecure Wi-Fi. Forty million credit and debit card numbers were stolen. Ask the Medicaid claims processor at the outsourcer EDS. In February she pleaded guilty to stealing Social Security numbers and dates of birth, and selling them for use on fake tax returns. Ask the courier hired by the University of Utah Hospital to take backup tapes to offsite storage. One day in June, he used his own car instead of his company's secured van. The tapes, containing billing data for 2.2 million patients, were stolen from his front seat.

Or you could, as we did, ask 7,097 business and technology executives worldwide about their security troubles. In this, our sixth year of conducting the "Global State of Information Security" survey with PricewaterhouseCoopers, we got an earful about the challenges, worries and wins in security technology, process and personnel.

Reader ROI

:: Why IT tools alone don't provide security

:: Why regulatory compliance doesn't protect you

:: Why you need to focus more on your employees and your data

44% plan to **increase**

security spending in the next year.

Quantifying returns on information security projects can be a struggle, often because it's hard to put a dollar value on a crisis averted. This year, a bad economy forces decision makers to squint even harder at proposals. Even so, survey results show companies are buying and applying technology tools, including software for intrusion detection, encryption and identity management, at record levels. That's pretty good news.

However—and this is serious, folks—too many organizations still lack coherent, enforced and forward-thinking security processes, our survey shows. While 59 percent of respondents said they have an "overall information security strategy," that's up just two points from last year and it's not enough, says Mark Lobel, advisory services principal at PricewaterhouseCoopers. Two elements, Lobel says, correlate with lower numbers of security incidents: having a C-level security executive and developing the aforementioned security strategy. But disappointing numbers piled up this year. (For additional stats see "The Global State of Information Security," Page 57.)

For instance, 56 percent of respondents employ a security executive at the C level, down 4 percent from last year. You comb network logs for fishy activity, but just 43 percent of you audit or monitor user compliance with your security policies (if you have them). This is up 6 percent from 2007, but still "not where we need to be," Lobel says.

As a result, security is still largely reactive, not proactive. More-sophisticated organizations will funnel data from network logs and other monitoring tools into business-intelligence systems to predict and stop security breaches. So along with encryption fanatics and identity management experts, an infosec team needs statisticians and risk analysts to stay ahead of trouble and keep the company name off police blotters.

Still, while our survey illuminates continuing problems, in discovering the problems, we also see a path to safer data for companies that, yes, apply technology but also develop processes and make them part of everyone's everyday work. So it's not all grim. What we have to do now is examine our failings, then act.

The Big Picture: Technology Reigns

Money really is power, isn't it? When asked to indicate any sources of funding for information security, 57 percent of survey respondents named the IT group and 60 percent cited functional areas such as marketing, human resources and legal as major providers. Just 24 percent indicated a dedicated security department budget.

With the IT group a strong force, technology becomes the answer to many security questions. To someone with a hammer, everything looks like a nail, according to the old saw. Divert potential phishing attacks with spam filters. Stymie laptop thieves by encrypting corporate data.

If there's a security tool out there, our survey pool uses it.

Companies have realized they must do a better job disposing of outdated computer hardware, for example, wiping disks of data and applications. Sixty-five percent of respondents now have tools to do that, up from 58 percent last year. More organizations than ever are encrypting databases (55 percent), laptops (50 percent), backup tapes (47 percent) and other media. Use of intrusion-detection software also is up: 63 percent this year compared with 59 percent last year. And installing firewalls to protect individual applications, not just servers and networks, increased to 67 percent from last year's 62 percent.

That's good stuff.

Despite these technology-oriented gains, though, disturbing trends continue in the areas of security processes and personnel—some negate any protection an IT budget can buy. For example, encrypting sensitive data makes good sense, but such technology can't stop an employee from flouting policies concerning how that data should be handled.

If the goal is to secure information, to make it truly safe, you'd better develop processes and procedures for putting your nails in the right place before whacking anything with a technology hammer. Technology must be part of a larger plan to secure information, says Dennis Devlin, chief information security officer at Brandeis University. Devlin reports to Brandeis's vice president and provost for libraries and information technology.

59%

have an **information security** strategy.

Criminal activity becomes the focus of a lot of what we do in information security. Lock down the Wi-Fi to keep out the bad guy. (Got that, TJX?) But well-meaning people who make bad decisions inflict untold numbers of security incidents upon us, Devlin says. He's seen it at Brandeis, since joining last year, and at Thomson Corp., now called Thomson Reuters, where he was chief security officer for seven years.

For example, employees sometimes fall for e-mail scams and open attachments that unleash malicious software such as key-stroke loggers that record passwords and rootkits that take control of operating systems. Devlin says the job of security managers is to teach self-defense. Rather than warn employees to watch out for the latest e-mail scam bearing a specific subject line, for example, the idea is to teach people broader lessons about the risks of clicking on unfamiliar URLs, opening attachments or handing over Social Security numbers to anyone online, he says.

"It's not possible with technology to protect every individual from every possible security risk," he says. "Our job is to teach people to think the way we think."

Like Brandeis, more organizations seem to be trying that. This year, 54 percent of survey respondents said they provide employees with security awareness training, up from 42 percent last year.

But there's plenty of work to do. Just 41 percent of those surveyed require employees to undergo training on the corporate privacy policy and practices, up incrementally from last year's 37 percent. Forty-three percent of organizations—slightly higher than last year—don't take the simple step of posting their privacy policies on their internal websites.

Furthermore, what's taught at many organizations provides only a veneer of security, namely, compliance with government or industry regulations.

Checklist Security

Regulations such as the Health Insurance Portability and Accountability Act for medical data, Sarbanes-Oxley for financial data and the Payment Card Industry standard for credit card data continue to move executives to action. The threats of fines and jail time tend to do that. For example, 44 percent of respondents say they test their organization for compliance with whatever laws and industry regulations apply, up from 40 percent last year; 43 percent say they monitor user compliance with security policy, a healthy increase from last year's 37 percent. Assessing internal risks to compliance is something 55 percent are doing, up from 49 percent.

But let's not pass around attaboys too quickly. Note that even with such positive steps, those numbers are far from 100 percent. Many organizations aren't doing much beyond checking off the items spelled out in regulations—and basic safeguards are being ignored, says Karen Worstell, a managing principal at the consulting firm W Risk Group, former chief information security officer at Microsoft, and former CISO and VP of IT risk management at AT&T.

Adhering to regulations and standards doesn't amount to thorough security policy, Worstell says, for many reasons. For one, organizations can sometimes pass compliance audits simply by writing up policies, without demonstrating how they adhere to them. Other times, the standard or regulation may have holes.

PCI, for example, mandates that a firewall be installed to protect cardholder data. But Worstell says the standard doesn't address whether a company has processes to ensure that once a piece of technology is installed, it's regularly upgraded or monitored to see how effective it is. "If security stops at PCI, that's not enough," she says. Hannaford Supermarkets experienced the theft of customer credit and debit card data from December 2007 to last March, a period when the grocery chain was certified compliant with PCI, "the highest security standards required by the credit card industry," the company says.

Neither is it enough if security monitoring stops within your own four walls. But that's exactly what's happening. A dirty secret uncovered in this year's poll reveals that companies don't know, and apparently don't care to know, what happens to their data once they hand it to another company. Get ready to be disturbed.

Outsourced Out of Sight, Security Out of Mind

Here's one of the most worrisome of our findings this year: A skimpy 22 percent of respondents keep an inventory of all the outside companies that use their data.

If that isn't enough to make you wince, we've got more. Just 37 percent of our survey respondents require third parties handling the personal data of customers or employees to comply with their privacy policies. Even fewer—28 percent—perform due diligence of those third parties to understand how or whether they safeguard information. Yet 75 percent of respondents profess at least some level of confidence in the effectiveness of their partners' security. Isn't that rosy?

Yet due diligence on any outsiders that handle your data is more important than ever as companies parcel out corporate work of all sorts to third parties, says Tom Bowers, managing director of Security Constructs, an industry analysis firm specializing in trade-secret protection technologies. In that respect, pharmaceutical companies can teach other industry verticals a great deal, he says.

Bowers was senior manager of global information security operations at Wyeth Pharmaceuticals for seven years before starting Security Constructs. Bowers's security group subjected potential Wyeth business partners to detailed scrutiny of their security practices. He had to. "We were responsible for protecting intellectual property no matter where it sat. Here or with an outsourced clinical trials company in Dublin. Wherever."

Ken Harris, CIO at Shaklee, says every company should make sure its outsourcers have the same security as its own—or better. "You vet the security and disaster recovery of your outsource providers in the same way you would vet your own operation," he says, adding, "It does take time and resources."

Companies skip this security check, though, because it's expensive and time-consuming, says PwC's Lobel. Checking out a partner's security and privacy practices would take at least one full-time employee at least two days for the smallest company, he estimates. "A large company may have literally thousands of partners," he says.

4 Ways to Maximize Your Security Budget

Businesses are investing more in security. But what if yours isn't one of them? You can get more from the budget you have.

1. Keep on training.
Security consultant John Bambenek notes that there are plenty of open-source tools available for security shops that can't afford the latest and greatest defenses. Existing commercial tools can also be better-maintained or tweaked with the right scripts. But to make these things work, employees need constant training. "Trained staff know how to make the most of their abilities to get the job done, even without commercial tools," he says.

2. Increase security awareness.
An aware workforce can be enough to make the difference when you can't spend more money, says Ernie Hayden, a principal at 443 Consulting and former CISO of the Port of Seattle. Through training, education and continuous "rifle-shot guerrilla marketing techniques," a company can condition employees to be paranoid of e-mail attachments and URLs sent by strangers, or to be more cognizant of any trouble fellow employees may be up to.

3. Pay attention to morale.
Cut the red tape. Employees will be happier if it's easier to get their work done, notes Joseph Guarino, CEO and senior consultant for Evolutionary IT. And watch what you cut from your budget. When the money supply runs dry, employees understand if the free snacks in the office kitchen have to go away. But slice too deeply into discretionary expenditures like professional development programs, and employee morale will tank, says Richard Parry, head of global security for Novartis Institutes for BioMedical Research. In-house cross-functional training helps, too, by providing "interesting variations in their daily duties."

4. Simplify IT.
Cutting down on IT complexities and embracing security compliance controls will lessen the chances of a mistake-fueled catastrophe, says Atlanta-based strategic architect James DeLuccia. One common requirement of regulatory compliance is to reduce network complexities and redundancies so data can be better tracked and protected. Fewer complexities also mean fewer opportunities for a security failure, especially in an organization where staffing and tech savvy are in short supply.

Bill Brenner is a senior editor with *CSO* magazine. To read a longer version or comment on this story, go to *www.csoonline.com/article/403713*.

Only **24%** classify the **business value of data** as part of security policies.

Protect Information, Not Just Systems

Where data is and where it's going constantly worries information security managers. Thirty-eight percent of the managers we surveyed said they experienced one to 49 security events in the past year, and another 35 percent say they don't know whether they have been hit. Those figures are close to last year's results.

Among those in our survey who experienced incidents, 39 percent found out about them via server or firewall logs and 37 percent used intrusion detection or prevention systems. But a significant number—36 percent—say a colleague clued them in. These figures reflect an unchanging trend showing that the human element is just as important as any technological one when it comes to good security. More evidence of the need for diligent and repeated employee training.

Investing employees with responsibility for keeping data correct and protected is the best way for a company to guard against security threats, says Tim Stanley, CISO at Continental Airlines.

Stanley wants to categorize every file in the enterprise by three variables: owner, business value and risk level. The government has "top secret," "secret" and "confidential" ratings, but Continental's designations will be more granular and dynamic, using tiers and subsets of tiers. Thinking this way vaults Continental ahead of most companies. Just 24 percent report that classifying the business value of data is part of their security policies. While 68 percent classify their data according to risk level, at least periodically, 30 percent don't ever do it.

The complexity of such a project explains the low numbers, Lobel says. "Doing this project is a lot of effort, and unless there's a regulatory need for it, many don't do it."

Stanley expects the project to take three or four years. "Anything that keeps planes in the air and money coming through is Tier 1," Stanley explains. That would include information about

crew scheduling, and cargo and fuel needs, as well as credit card processing information. Tier 2 or 3 is still important to protect, but not critical to keeping planes aloft, for example, providing employees access to their 401(k) accounts.

Security technology and procedures will correspond to the risk and tier level in which a given piece of data falls, as defined by the data owner. Tier 1 might mandate twice-a-day backups and two-factor user authentication, he says. "I can expend my resources more appropriately to our data's value and therefore save the company money," he says. "Stop spending $10 to protect $5 worth of data." Music to an airline CEO's ears, no doubt.

Which Brings Us Back to Money

With security budgets averaging $1.7 million, an optimistic 44 percent of those surveyed said their information security spending would increase this year, while 4 percent expected a decrease. Where will the money go? We see glimmers of hope.

Top priorities in the coming year include hiring information security consultants and hiring a chief information security officer. Respondents also plan to develop security procedures for handheld devices and create an identity management strategy. They expect to invest in technologies, including biometrics, to tighten access to sensitive data, as well as in data-leakage prevention and security event correlation tools to start analyzing what works and what doesn't on which kinds of security problems.

These steps, Lobel says, will get companies closer to a comprehensive security strategy. Already, he notes, 40 percent of organizations use security as a marketing point, usually soliciting business on the grounds that they protect customer data better than their rivals. "But it's only a competitive advantage if it works, if it's *good* security." **CIO**

Something Else to Worry About

Read what blogger Mike Kavis has to say about the security challenges of SOA in **ARE YOU INSECURE ABOUT SOA SECURITY?** at **www.cio.com/article/447129**.

CIO.com

Senior Editor Kim S. Nash can be reached at *knash@cio.com*. To comment on this article, go to *www.cio.com/article/451092*.

How do you leverage your information security investment? How can a well-integrated plan help you mitigate risk while maximizing your business objectives? These are the questions we help our clients answer—working together while sharing our knowledge of how information security can help improve your business.

To learn more about how we can help you turn a compliance enabler into a business enabler, visit www.pwc.com/security

security is good business.

THE GLOBAL SECURITY LANDSCAPE

BY CAROLYN JOHNSON

Who Pays for Security?

Few companies have dedicated security budgets. IT is still a common source of security money, but funding from business functions is on the rise.

Funding source	2007	2008
Functional budgets	47%	60%
I.T. budget	65%	57%
Security budget	24%	24%

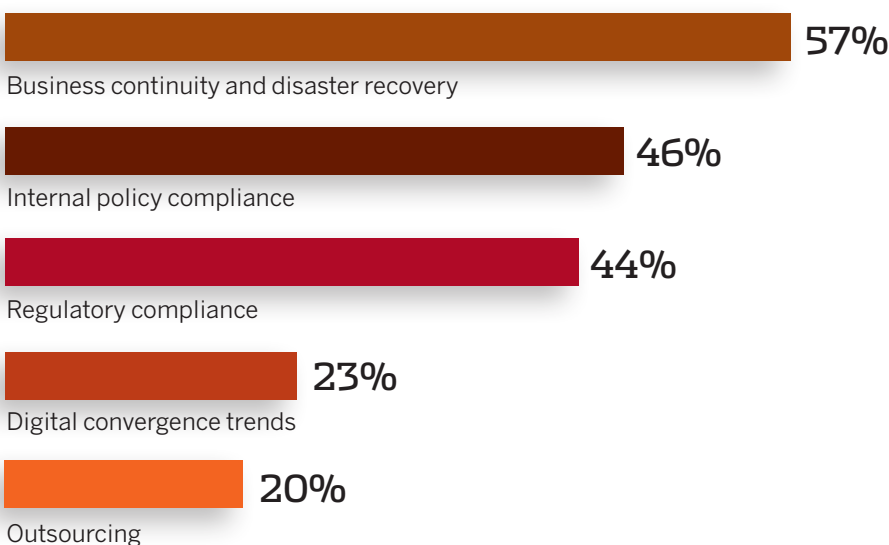Respondents chose all that apply.

SECURE THOSE BLACKBERRYS!

14%

of security incidents in the past year **involved devices**.

WHY COMPANIES CARE

Business continuity and **compliance** lead the reasons for investing in security

57%
Business continuity and disaster recovery

46%
Internal policy compliance

44%
Regulatory compliance

23%
Digital convergence trends

20%
Outsourcing

Respondents chose all that apply.

WHO'S IN CHARGE OF INFORMATION SECURITY?

CISOs often report to **more than one executive**. At large companies, one of them is most likely the **CIO**

Among big companies with CISOs, **44%** report to the CIO, compared to **36%** at mid-market companies.

WE'VE BEEN Hit!

How organizations learn of security incidents:

Server or firewall files and logs **39%**

Intrusion detection/prevention system **37%**

Colleague **36%**

Respondents chose all that apply.

Leader and Laggard

Financial services companies have adopted security best practices most widely. The consumer-products and retail industries lag the rest.

Practice	Consumer products/Retail	Financial services
Employs a CSO or CISO	43%	83%
Has an information-security strategy	52%	75%
Runs personnel background checks	47%	69%
Involves business and IT decision makers with information security issues	47%	67%
Dedicates staff for employee awareness programs	41%	60%
Provides security baselines for external partners	40%	59%
Has an information security budget	18%	37%

Respondents chose all that apply.

28%
of **consumer products and retail executives** said their company's security spending is **poorly aligned or not aligned with business objectives,** compared with
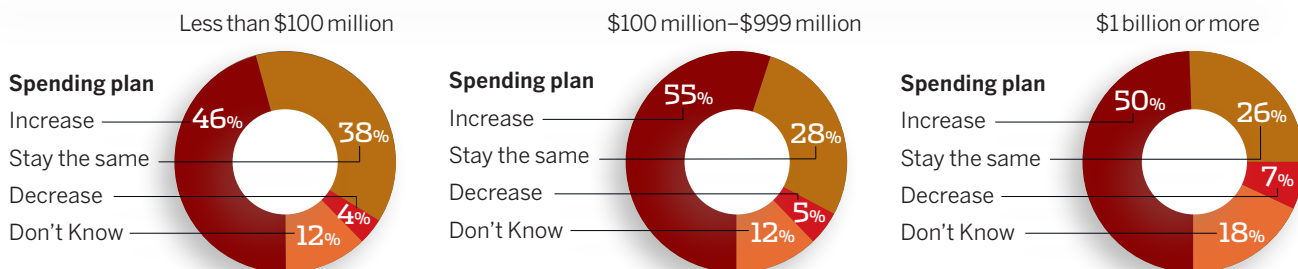
14%
of **financial services executives**.

SPENDING MORE

Investment in security is going up, especially in the mid-market. Few are making cuts.

COMPANY REVENUE

Less than $100 million

Spending plan
Increase
Stay the same
Decrease
Don't Know

46% 38% 4% 12%

$100 million–$999 million

Spending plan
Increase
Stay the same
Decrease
Don't Know

55% 28% 5% 12%

$1 billion or more

Spending plan
Increase
Stay the same
Decrease
Don't Know

50% 26% 7% 18%

Numbers may not add up to 100% due to rounding.
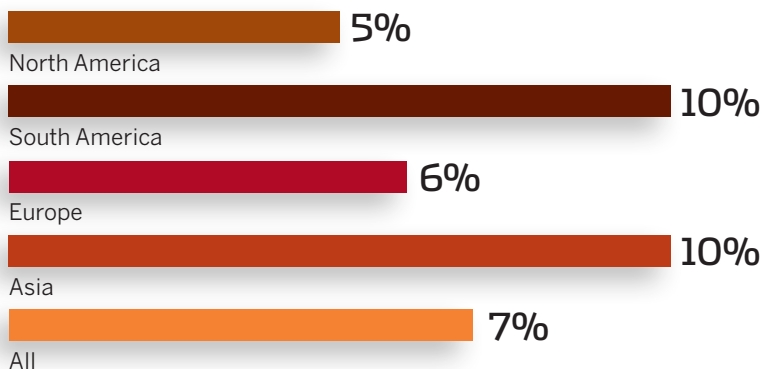
What's in Your Toolbox?

With the IT group as a major source of funding for information security projects, technology has become the answer to many security questions. More respondents now have a comprehensive set of IT security tools.

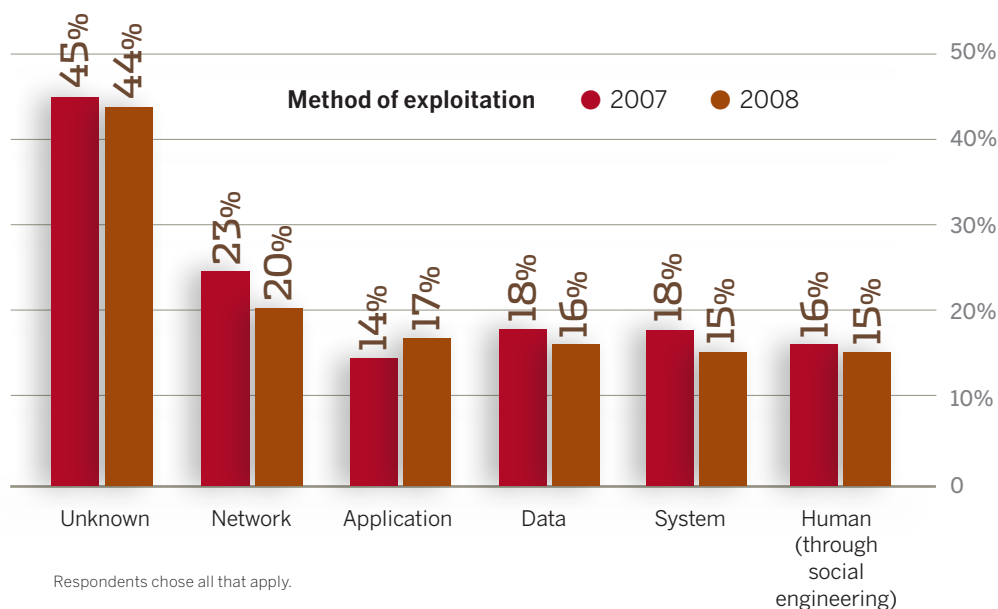| Technology	2007	2008
Malicious-code detection tools	80%	84%
Application-level firewalls	62%	67%
Intrusion detection	59%	63%
Intrusion prevention	52%	62%
Encryption		
Database	45%	55%
Laptop	40%	50%
Backup tape	37%	47%
Automated password reset	40%	45%
Wireless handheld device security	33%	42%

Respondents chose all that apply.

On average, companies in North America plan the smallest increases to their security budgets

AVERAGE INCREASE

- North America — 5%
- South America — 10%
- Europe — 6%
- Asia — 10%
- All — 7%

Ignorance Isn't Bliss, Part 1

Nearly half of respondents can't identify vulnerabilities
that led to security incidents

Method of exploitation ● 2007 ● 2008

Category	2007	2008
Unknown	45%	44%
Network	23%	20%
Application	14%	17%
Data	18%	16%
System	18%	15%
Human (through social engineering)	16%	15%

Respondents chose all that apply.

Ignorance Isn't Bliss, Part 2

Employees and former employees together remain
the biggest threat. But the source of nearly half
of security incidents is unknown.

Source of incident	2007	2008
Unknown	*	42%
Employees	48%	34%
Hackers	41%	28%
Former employees	21%	16%
Business partner	19%	15%
Customer	9%	8%
Other	20%	8%
Terrorist/Foreign government	6%	4%

Respondents chose all that apply.   * Not a choice in 2007

Know Your Weakness

Find out **WHO KNOWS THE MOST ABOUT YOUR SYSTEM VULNERABILI-TIES** at **www.cio.com/ article/449694**.

CIO.com