Advisory Services
Security

Safeguarding the new currency of business*

Findings from the 2008 Global State of Information Security Study®

*connectedthinking

PRICEWATERHOUSECOOPERS

October 2008

The heart of the matter

Information is the new currency of business—a critical corporate asset whose value rises and falls at different times, and in different ways, depending on when, how, where and by whom it is placed into circulation as a medium of exchange.

Therein lie the risks. And the opportunities.

It’s a different world.

Information has become the new currency of business—and its portability, accessibility and mobility back and forth across international, corporate and organizational boundaries are crucial components of a collaborative, globally connected business world.

At the same time, however, protecting corporate information assets is equally critical—especially as mobile devices proliferate, open use of the Internet surges, new business models shake out, and strategic sourcing initiatives stretch “long reach” supply chains further and across more countries and companies than ever before.

Just how well are companies across global markets, sectors and regions addressing these challenges this year?

We wanted to know. So we asked more than 7,000 CEOs, CFOs, CIOs, CSOs, vice presidents and directors of IT and information security from 119 countries.

One of the most striking survey results from the 2008 Global State of Information Security study is that—across industries and sectors, countries and regions, business models and company sizes—most respondents are reporting strong, often double-digit advances in implementing new security technologies, across virtually every security domain, from prevention to detection.

Yet other results indicate that, in spite of the rapidly evolving maturity of security capabilities for so many companies, more than three out of every ten survey respondents cannot answer basic questions about the risks to their company’s key information.

Moreover, these trends are playing out differently across regions of the world. Asian companies—led principally by India—continue to overtake North American ones in establishing leading global practices in security. And South American security and privacy practices are advancing so quickly, they are likely to surpass Europe’s within two years.

What are the implications of these trends on your business strategies? Where does your organization sit in this spectrum? What actions can you take to improve its position?

Here’s a brief overview of the critical areas we believe deserve your attention—and why we believe that, from this point forward—quarter-by-quarter, the companies that do the best job at safeguarding their business currency and preventing data and identity theft will be those that take a risk-based, integrated and proactive approach.

An in-depth discussion

Companies across the world are confronting real, growing, and strategic risks to their information assets.

I. As the drivers of security spending evolve—executive perceptions about what's most important are not necessarily fully aligned

Finding #1

Change almost rivals compliance as a leading driver of spending.

Finding #2

Compliance is still a priority, of course. Yet few companies have a well-rounded view of their compliance activities.

Finding #3

Executive misalignment can undermine value from investments.

Finding #1. Change almost rivals compliance as a leading driver of spending

The shift is subtle. But it’s impossible to ignore.

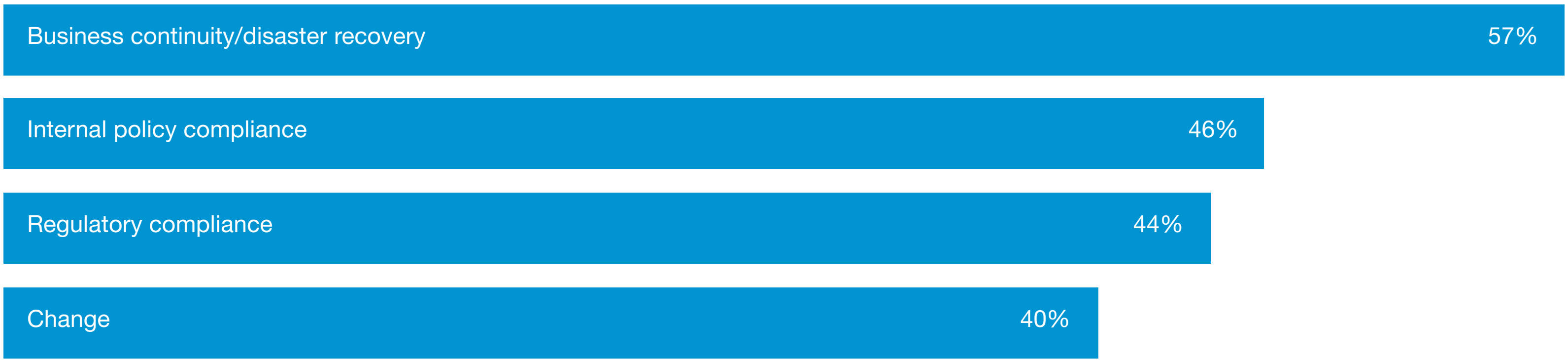
Over the last decade or more, one of the most consistent and enduring characteristics of executive decision-making on information security and privacy issues has been the emphasis on preventing harm. And this focus, of course, will continue. After all, isn’t security, by nature, principally about protection?

Not anymore.

Not, at least, according to the executives accountable for information security’s performance in a world where scrutiny over information security’s alignment with business objectives is becoming more and more rigorous.

Asked to identify the most critical business issues or factors driving information security spending, survey respondents still point first to “business continuity and disaster recovery” (57%). But they also now cite “change” (40%) almost as often as they do “compliance with regulations or internal policies” (44% and 46%). (Figure 1)

Figure 1: Percentage of respondents who identify the following business issues or factors as the most important drivers of information security spending in their organization[1]



[1] Does not add up to 100%. Respondents were allowed to indicate multiple factors.

Source: The Global State of Information Security Survey®, 2008

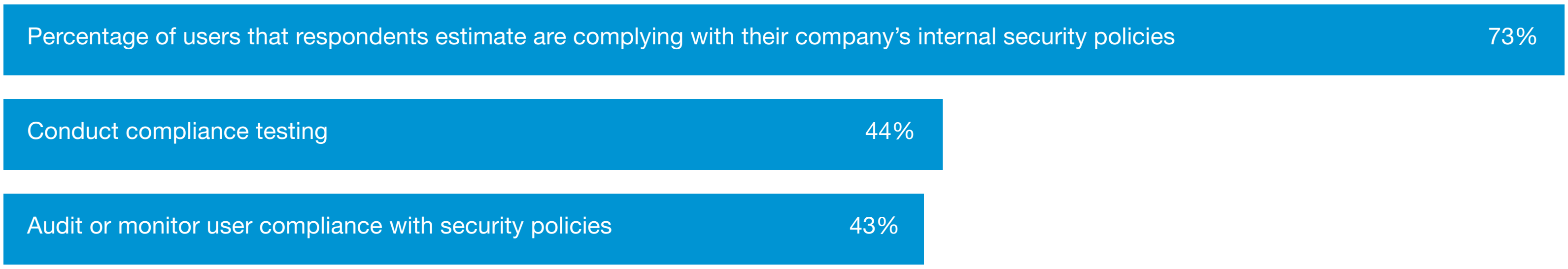
Finding #2. Compliance is still a priority, of course. Yet few companies have a well-rounded view of their compliance activities.

Regulations keep mounting. Just consider the epidemic of credit card fraud—and the widespread worldwide rush across many sectors with retail operations to comply with the new payment card industry data security standards (PCI DSS). Regulatory enforcement is rising too—particularly, for example, of payer violations of the U.S. Health Insurance Portability and Accountability Act (HIPAA).

Are companies experiencing compliance fatigue? Or is a “culture of compliance” taking root? It’s hard to tell. Maybe the fact that regulatory compliance is cited less often this year (44% vs. 54% in 2007) as a driver of security spending is another sign that compliance is now more deeply embedded within organizations.

Other survey results, though, suggest that business and IT executives may not have a full picture of compliance lapses. Although confidence that users are complying with internal security policies still runs optimistically high at 73%, most companies aren’t checking. Fewer than half of all respondents say their organization audits and monitors user compliance with security policies (43%). And only 44% conduct compliance testing. (Figure 2)

Figure 2: Percentage of respondents who report compliance-related capabilities



Source: The Global State of Information Security Survey®, 2008

Finding #3. Executive misalignment can undermine value from investments

There are many places to spend limited security budget funds. Not all, however, are equally aligned with the business's strategic direction. This year, Chief Information Security Officers (CISOs) are more likely than any other executives on the senior management team to perceive a significant gap between security policy alignment with business objectives and security spending alignment with business objectives. In fact, CISOs believe that spending alignment trails policy alignment by a full 16 points—compared to CEOs, for example, who perceive no gap whatsoever. (Figure 3)

This makes sense—at least, partly. Aren't CISOs on the frontlines of security, closer to how investments are being spent and, therefore, in the best position to identify a spending alignment gap?

Maybe so. But CISOs are also—or should be—among the executives best positioned to direct or influence security spending towards the most strategic, business-aligned priorities.

There's a more likely explanation of this perception gap—and a crucially important one: CISOs don't see eye-to-eye with the rest of the executive suite on what single business issue is principally driving information security spending. They are far more likely to cite regulatory compliance than CEOs, CFOs, and even—quite surprisingly—Chief Compliance Officers (75% vs. 27%, 37% and 24%, respectively). And all of these executives—in addition to the CIO, who is the only other business leader who sits on the IT side of the table—unanimously disagree: they cite a completely different principal driver for security investments: business continuity and disaster recovery. (Figure 4)

Who's right? It's tempting to say: "That depends on the company". After all, some CISOs are more aware than their executive counterparts of security-related deficiencies in regulatory compliance-related capabilities. And other CISOs are dangerously out-of-synch with the support that the most critical business objectives require of security—from both a "protection" and an "enablement" perspective.

The real question shouldn't be: "Who is right?" Instead, it should be: "Are we aligned, as a leadership team, on what we expect security to contribute to the business?" If the answer is "no", follow up quickly with the game-changing question: "Why not?" And if your team isn't sure, ask the CISOs. It looks like, instead of being part of the management process, they are the whistle-blowers.

Figure 3: Percentage of senior business and IT executives who report that security policies and security spending are completely aligned with business objectives

	CEO	CFO	CIO	CISO
Security policies are completely aligned with business objectives	34%	28%	31%	38%
Security spending is completely aligned with business objectives	34%	30%	21%	22%
Alignment gap	0	-2	10	16

Source: The Global State of Information Security Survey®, 2008

Figure 4: Differences among senior business and IT executives on what constitutes the primary business issue or factor driving information security spending[2]

	CEO	CFO	CIO	CISO
Business continuity / Disaster recovery	√	√	√	
Regulatory compliance				√

[2] Respondents were asked to select from the following list: change, business continuity/disaster recovery, outsourcing, digital convergence trends, company reputation, terrorism, M&A activity, regulatory compliance, and internal policy compliance.

Source: The Global State of Information Security Survey®, 2008

II. This year, respondents trumpet a headlong rush into technology. But these investments don’t necessarily mean better security.

Finding #4

It’s dramatically clear: one of the highest priorities for companies over the past year has been technology.

Finding #5

Many companies, however—if not most—do not know exactly where important data is located.

Finding #6

Companies need to focus more acutely on advancing critical processes—and supporting the people that run them.

Finding #4. It’s dramatically clear: one of the highest priorities for companies over the past year has been technology.

A big strategic step forward took place last year—when respondents reported, 17-to-20 point gains in appointing a senior information security executive and establishing an overall information security strategy.

With new leadership and a plan in place—exactly where was the investment emphasis was placed in 2008?

The answer is in technology.

Across industries, regions and business models, survey respondents report huge, double-digit gains in implementing new security-related technologies. In ten-point leaps, companies are much more likely, for example, to encrypt sensitive information not just in laptops but also in databases, file shares, backup tapes and removable media. They have also taken significant strides in advancing Web/Internet capabilities—such as content filters, website certification/accreditation, secure browsers, and web services security. And they have made similar leaps ahead in technologies that help protect wireless devices and secure remote access via VPN as well as tools to prevent intrusions or discover unauthorized devices. (Figure 5)

Here’s the hitch: capturing the business benefits of technologies intended to advance objectives related to security, privacy, compliance and business continuity also requires knowing as much as possible about where the greatest risks to sensitive information are coming from. And that, as we discuss next, appears to be a critical challenge.

Figure 5: Respondents report strong, double-digit advances in implementing technologies across most critical security and privacy domains

	2008	2007
Encryption, Laptops	50%	40%
Encryption, Databases	55%	45%
Encryption, File shares	48%	37%
Encryption, Backup tapes	47%	37%
Encryption, Removable media	40%	28%
Web/Internet, Content filters	69%	51%
Web/Internet, Website certification/accreditation	58%	48%
Web/Internet, Secure browsers	66%	55%
Web/Internet, Web services security	58%	48%
Detection, Tools to discover unauthorized devices	51%	40%
Prevention, Tools to prevent intrusions	62%	52%
Prevention, Secure remote access via VPN	68%	59%
Prevention, Wireless handheld device security technologies	42%	33%

Source: The Global State of Information Security Survey®, 2008

Finding #5. Many companies, however—if not most—do not know exactly where important data is located.

Progress always advances unevenly. Sector responses this year reveal that, in spite of the support provided by a much broader and stronger portfolio of technologies, a surprisingly large percentage of survey respondents “don’t know what they don’t know”. In fact, more than three out of every ten respondents cannot answer basic questions about the risks to their company’s most sensitive information.

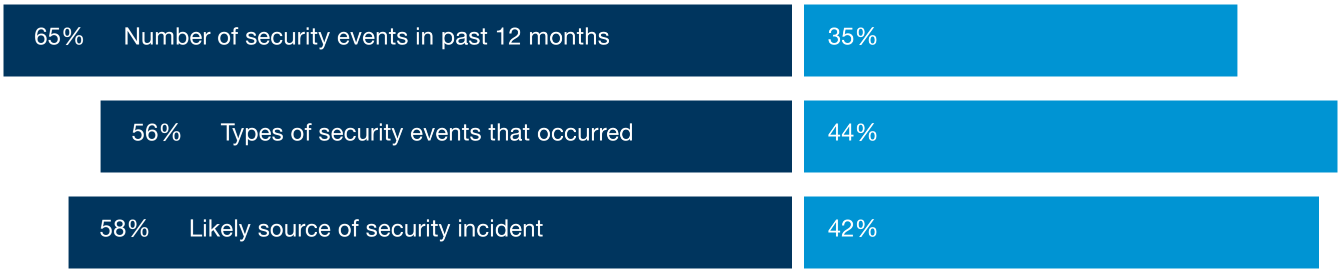
How many security incidents occurred this year? Thirty-five percent (35%) of respondents aren’t sure. What types of security incidents presented the greatest threats to the company’s most sensitive information, assets and operations? Forty-four percent (44%) of respondents couldn’t say. What about the source of incidents—whether the attack was most likely to have originated from employees (either current or former), customers, partners or suppliers, hackers or others? Forty-two percent (42%) don’t know. (Figure 6)

Internal stakeholders looking to defend these numbers won’t find it hard. Any large survey—of either thousands of companies or one—will find many respondents who don’t have a front-row view of the attack or other form of first-hand knowledge.

That’s true. But it also misses the point. What matters, of course, is improving an organization’s ability to defend and prevent attacks on an ongoing basis—without distracting people from the every-day operational needs of the business or incurring the exorbitantly high price tags associated with a reactive response to an unexpected (but foreseeable) crisis.

And that requires getting key information about the risks to an organization’s data and systems very quickly from the front row to everyone else in the house. Expanding security awareness at every level of the enterprise is essential.

Figure 6: Percentage of respondents who don't know basic information about the risks to their company's information assets



Source: The Global State of Information Security Survey®, 2008

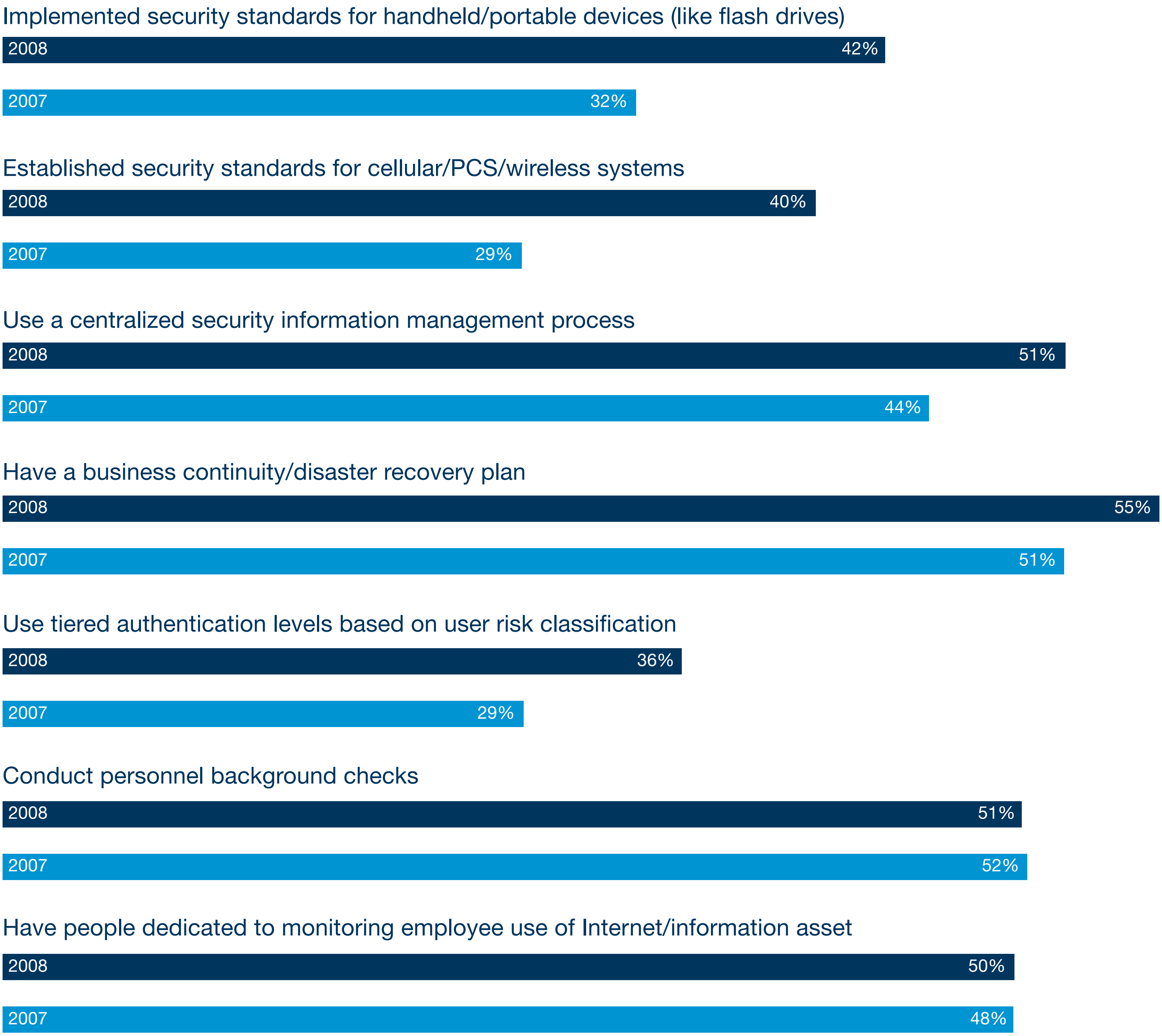
Finding #6. Companies need to focus more acutely on advancing critical processes—and supporting the people that run them.

One of the best ways of improving enterprise-wide visibility into the crucial details of actual security incidents is to match technology investments with an equally robust commitment to the other principal drivers of security's value: the critical business and security processes that support technology, and the people that administer them.

This year, respondents report noteworthy advances in implementing a few critical processes—such as establishing security standards for handheld/portable devices like flash drives or external drives (42% vs. 32% in 2007) and cellular/PCS/wireless systems (40% vs. 29%). Yet gains tend to be more muted (i.e., in the single digits) for most other important security processes—such as establishing a centralized security information management process (51% vs. 44%), implementing a business continuity/disaster recovery plan (55% vs. 51%) and using tiered authentication levels based on user risk classification (36% vs. 29%).

Addressing the people side of effective security also remains a challenge. For example, only about half of all companies conduct personnel background checks (51%) or have people dedicated to monitoring employee use of Internet/information assets (50%). (Figure 7)

Figure 7: Percentage of respondents reporting gains in key processes and people-related capabilities



Source: The Global State of Information Security Survey®, 2008

III. From protecting privacy to preventing data loss: opportunities to improve safeguards abound.

Finding #7

Privacy: Few companies are well prepared to protect it.

Finding #8

Access control: Progress is clear, but more work lies ahead.

Finding #9

Sourcing, alliances and other collaborative networks: Risks linger.

Finding #10

Data loss prevention: A critical tool—if implemented correctly.

Finding #7. Privacy: Few companies are well prepared to protect it.

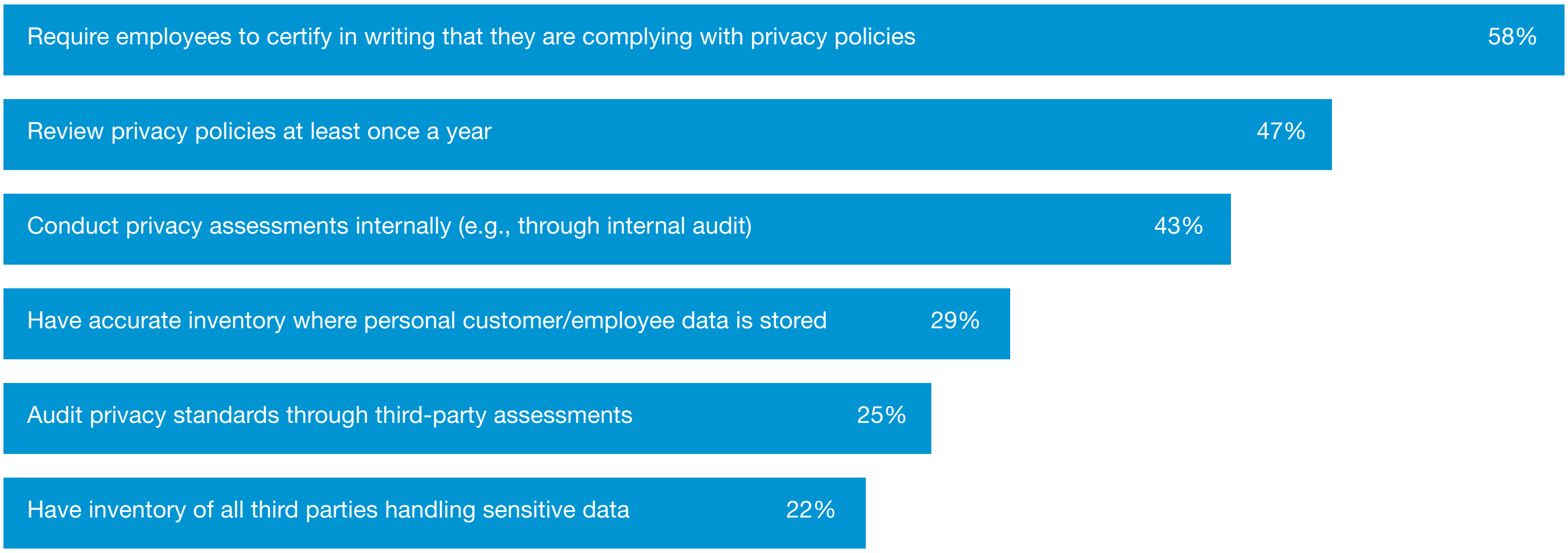
Gains in privacy protections have slowed—in spite of a slew of high-profile headlines this year announcing breaches of consumer information, information subject to protection under regulations such as the U.S. Health Insurance Portability and Accountability Act (HIPAA) and the E.U.'s Data Protection Directive.

Companies worldwide are somewhat more likely this year to review their privacy policies at least once a year (47% vs. 44%) and require employees to certify in writing that they are complying with them (58% vs. 53%).

But while proactive measures such as these are important, so is knowing exactly where this information resides within the organization and who has been granted access to it. Yet 71% of respondents say their organization does not have an accurate inventory of where personal data for employees and customers is stored.

Other privacy-related opportunities also beckon. Many companies could benefit by joining the ranks of organizations that audit privacy standards through third-party assessments (25%) and conduct privacy assessments internally through governance mechanisms such as internal audit reviews (43%). (Figure 8)

Figure 8: Percentage of organizations with privacy-related capabilities



Source: The Global State of Information Security Survey®, 2008

Finding #8. Access control: Progress is clear, but more work lies ahead.

Among the greatest risks to sensitive corporate information is that a user with either legitimate or unauthorized access to systems will compromise data—intentionally or accidentally.

This year, survey respondents were much less likely to view their own staff as the likely source of a security incident (34% vs. 48% in 2007).

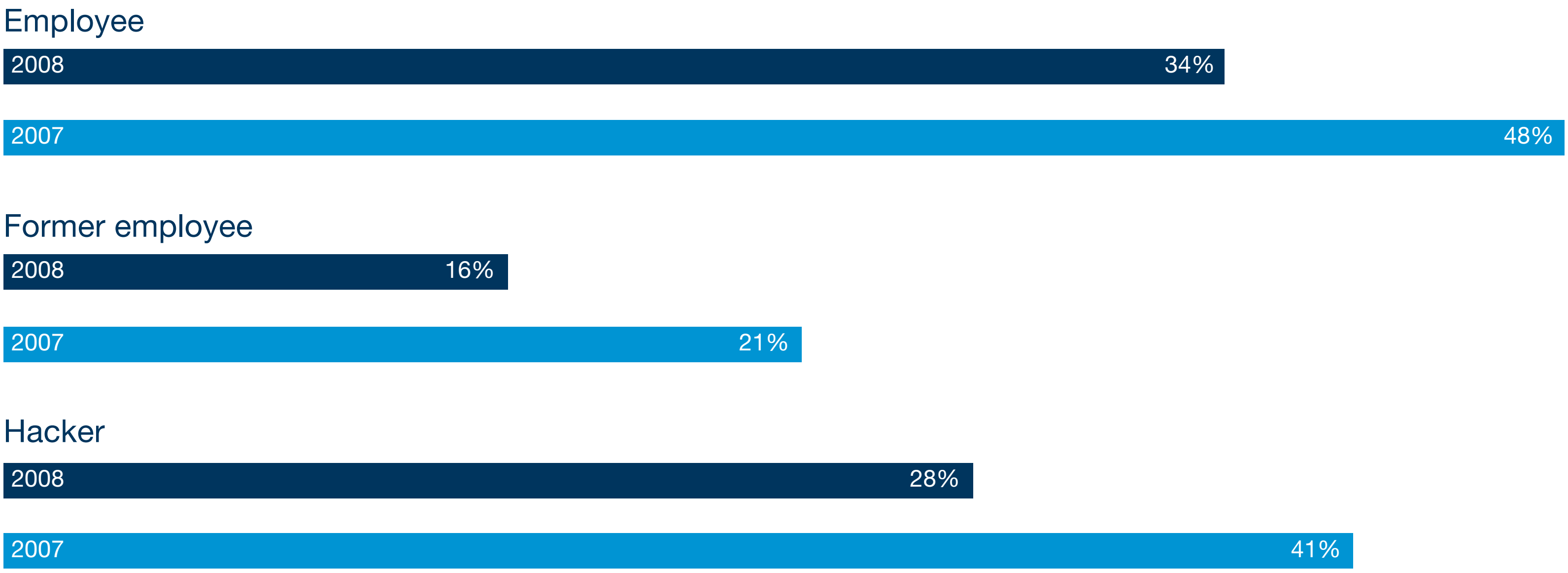
And small wonder—given that more now report using tools such as a centralized user data store (55% vs. 47%) and reduced/single sign-on software (35% vs. 28%).

Yet other responses reveal that, while the dangers are tangible, they can also be mitigated. Asked about what primary methods were used to exploit corporate systems, almost half—46%—cited the abuse of valid user accounts and permissions.

Survey results also indicated that a strategic approach to access-related risks benefits only a minority of companies worldwide. Only 41% have an identity management strategy in place.

More than half could better mitigate the risks of data and identity theft by implementing user activity monitoring tools (52%) and deploying automated account de-provisioning (73%). (Figures 9 and 10)

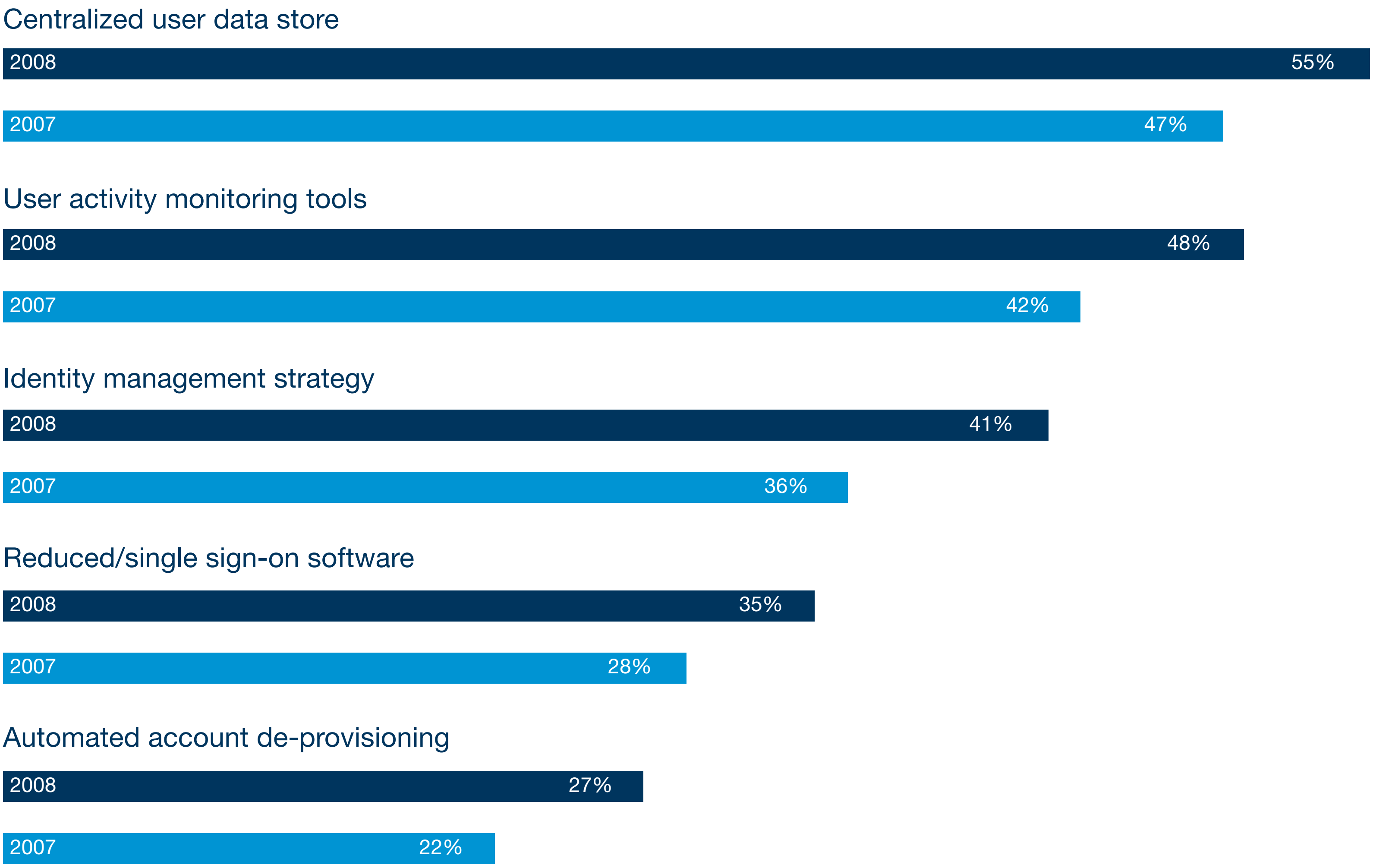
Figure 9: Estimated likely source of security incidents over the last 12 months[3]



[3] Other likely sources of security incidents cited in 2008 included customers (8%), service providers/contractors (8%), partners/suppliers (7%), terrorists (2%) and foreign governments (2%). Forty two percent (42%) of respondents didn't know. Data does not add up to 100%. Respondents were allowed to indicate multiple factors.

Source: The Global State of Information Security Survey®, 2008

Figure 10: Percentage of organizations with access control-related security and privacy protection capabilities



Source: The Global State of Information Security Survey®, 2008

Finding #9. Sourcing, alliances and other collaborative networks: Risks linger

As companies seek sourcing benefits, faster innovation, lower-cost manufacturing, and entry into emerging markets, partnering arrangements such as strategic alliances and joint ventures are on the rise.

Yet fewer than half of all survey respondents say their organization has established security baselines for external partners, customers, suppliers and vendors (43%) or requires third parties to comply with internal privacy policies (37%). And less than 3 out of 10 have an inventory of third parties handling the personal data of customers and suppliers (22%) or conduct due diligence of these third parties (28%). (Figure 11)

Are executives aware of the risks to their information as it passes back and forth between parties? They are. Asked how confident they were in their partners' or suppliers' information security practices, 78% of the respondents—an overwhelming majority—said they were only "somewhat" confident (53%), "not at all" confident (10%), or "didn't know" (15%). (Figure 12)

Figure 11: Percentage of organizations with security capabilities that safeguard sensitive information shared with third-party organizations

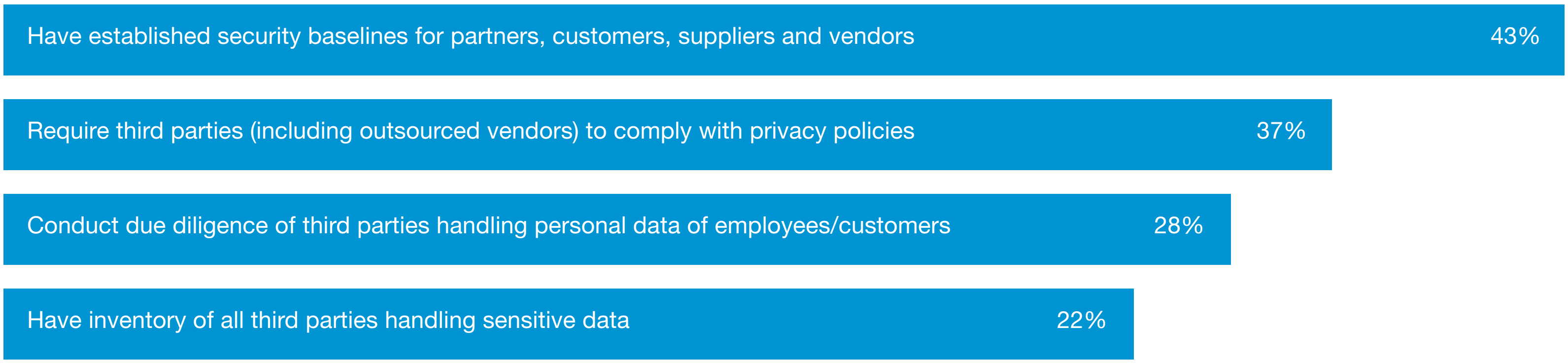
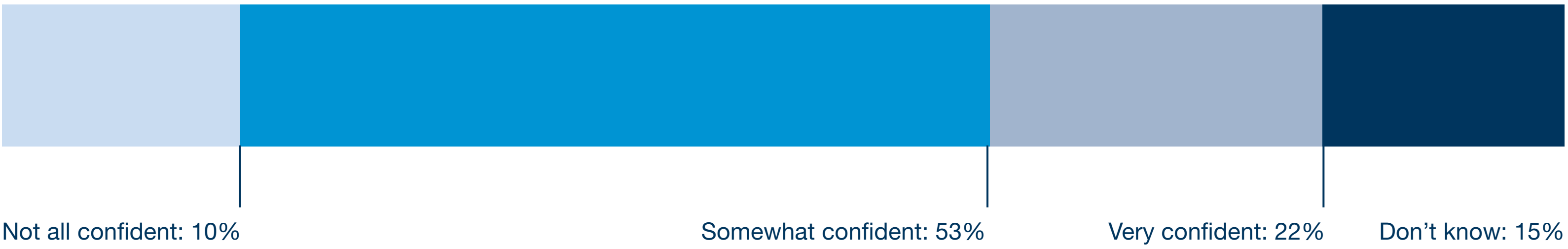


Figure 12: Few respondents are very confident in their partners' or suppliers' information security practices



Source: The Global State of Information Security Survey®, 2008

Finding #10. Data loss prevention: A critical tool—if implemented correctly

When data breaches occur, they hurt. This year, a significant percentage of respondents who cite negative business impacts from security breaches point to financial losses (39%), theft of intellectual property (30%), compromise to brands or corporate reputation (27%), and fraud (21%), among other damages. (Figure 13)

In addition to citing advances in encrypting data at rest, in motion and at end-points, 3 out of 10 respondents (29%) say their organization now has a data loss prevention (DLP) capability in place. And another 10% say that implementing DLP is a "hot priority" over the next 12 months. (Figure 14)

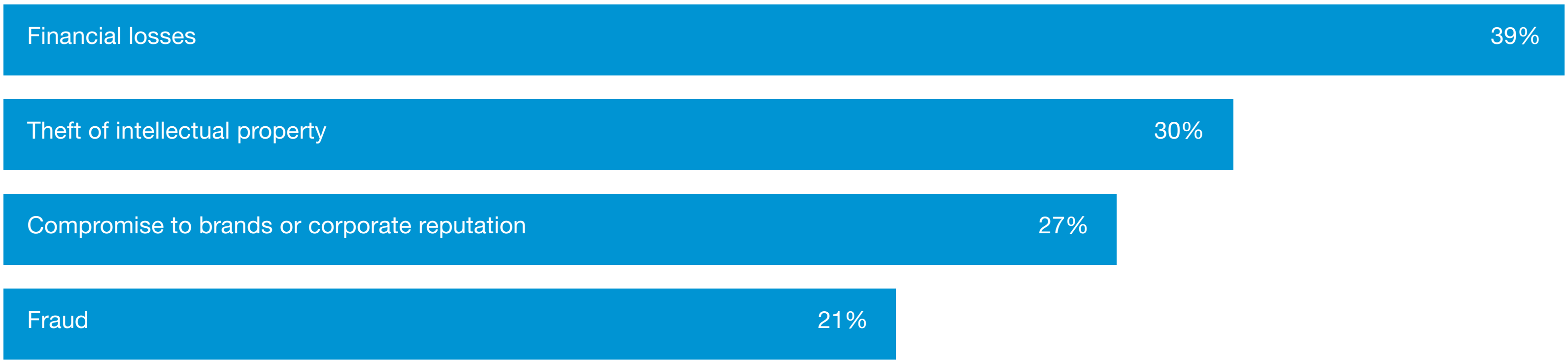
But point solutions aren't enough.

For capabilities like DLP to be effective, companies must decide on the right strategy, engage the right people, target the right data, and employ the right technology.

By aligning a well-designed data loss prevention program with an overall data protection strategy, companies can gain control over sensitive data, reduce the cost of data breaches and achieve greater visibility into how data is used throughout the organization.[4]

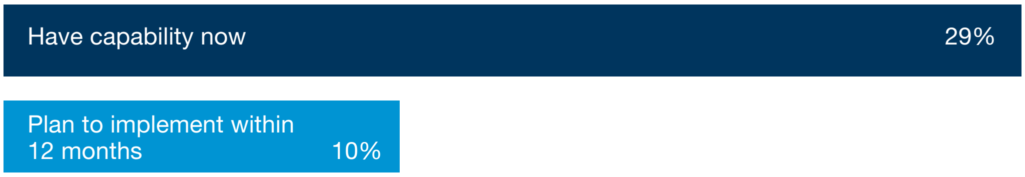
[4] For additional information on data loss prevention, see PricewaterhouseCoopers's Data Loss Prevention: Keeping sensitive data out of the wrong hands

Figure 13: Percentage of respondents reporting the following business impacts of a security breach



Source: The Global State of Information Security Survey®, 2008

Figure 14: Percentage of respondents citing current and intended use of data loss prevention technologies



Source: The Global State of Information Security Survey®, 2008

IV. Companies in some regions of the world—though not all—are expanding their security capabilities at a tremendous pace.

Finding #11

India now leads other countries—while China posts big gains.

Finding #12

Asia's security practices now on a par with those in North America.

Finding #13

Europe stalls—just as South America moves into the passing lane.

Finding #11. India now leads other countries—while China posts big gains

Perhaps the most dramatic and compelling highlights of this year's survey are the breadth and depth of India's advances across almost every security domain. Last year, 65% of Indian respondents reported that their organization planned to increase security spending in 2008—compared to 44%, the global average—and clearly they have.

This year, Indian respondents say their organizations are much more likely to conduct employee security awareness training (68% vs. 51%), use malicious code detection tools (85% vs. 57%) and have security standards in place for handheld/portable devices (56% vs. 36%). In fact, over the 24 months since the survey was taken in 2006—and across most of the metrics it tracks—Indian companies have advanced many of their security capabilities by more than 100%.

As a result of this investment blitz, India's security capabilities now surpass those in almost every country in the world. Indian respondents are more likely than those in the U.S., the U.K, and Australia, for example, to report that their company has a information security strategy in place (72% vs. 65%, 61%, and 51%, respectively), employs either a CSO or a CISO (77% vs. 52%, 48% and 28%), and conducts an enterprise risk assessment at least yearly (78% vs. 60%, 58%, and 57%).

And we expect India's lead to widen by 2009. A clear majority of Indian respondents (72%) say security spending will increase over the next 12 months—a significantly higher level of commitment than reported, for example, by respondents in the US (39%) or indicated by the global average (44%).

China also continues to make advances in security—though not as briskly or as strategically as India. The majority of Chinese respondents report now having an overall security strategy in place (54% vs. 41% in 2007) as well as making strides in implementing technologies—such as content filters (62% vs. 35%), secure browsers (59% vs. 48%), and laptop encryption (53% vs. 42%). Chinese gains in people- and process-related areas, however, remain modest. (Figures 14, 15 and 16)

Figure 14: Indian respondents report significant advances in security capabilities over the past three years

	2008	2007	2006	Three Yr. Gain
Have an overall information security strategy	72%	62%	34%	112%
Deploy malicious code detection tools	85%	57%	27%	215%
Integrate privacy and compliance plans	44%	31%	23%	91%
Engage periodic threat and vulnerability assessments	60%	40%	33%	82%
Use tiered authentication based on user risk classifications	47%	31%	21%	124%
Has security standards for handheld/portable devices	56%	36%	25%	124%
Ensure the secure disposal of technology hardware	69%	51%	26%	165%
Will increase security spending over next 12 months	72%	65%	69%	—

Source: The Global State of Information Security Survey®, 2008

Figure 15: Chinese respondents also report progress—particularly in security-related technologies[5]

	2008	2007
Have an overall information security strategy	54%	41%
Deploy content filters	62%	35%
Use secure browsers	59%	48%
Encrypt laptops	53%	42%
Leverage user activity monitoring tools	31%	25%
Conduct personnel background checks	41%	37%
Have security standards for handheld/portable devices	36%	33%
Have established security baselines for suppliers and vendors	31%	30%

[5] 2006 survey data for China is not available.

Source: The Global State of Information Security Survey®, 2008

Figure 16: India’s information security capabilities typically exceed those in other countries

	India	U.S.	U.K.	Germany	Brazil	Australia	China
Have an overall information security strategy	72%	65%	61%	52%	46%	51%	54%
Conduct enterprise risk assessment at least once a year	78%	60%	58%	58%	63%	57%	74%
Use security in marketing as a competitive advantage	58%	37%	40%	45%	59%	35%	68%
Employ a CISO or CSO	77%	52%	54%	36%	54%	28%	68%
Will increase security spending over next 12 months	72%	39%	38%	35%	54%	36%	61%
Have a business continuity and/or disaster recovery plan	63%	62%	60%	43%	43%	50%	33%
Use centralized security information management process	63%	53%	50%	46%	53%	39%	44%
Conduct active monitoring/analysis of security intelligence	69%	56%	55%	55%	54%	45%	41%
Continuously prioritize data assets according to risk level	27%	26%	28%	25%	25%	20%	28%
Have an employee security awareness program	68%	61%	51%	44%	45%	54%	52%
Have intrusion prevention tools	69%	63%	59%	65%	64%	55%	57%
Have intrusion detection tools	68%	65%	62%	60%	67%	57%	46%
Have accurate inventory of where sensitive data stored	40%	41%	42%	38%	28%	28%	38%
Have implemented a data loss prevention capability	34%	30%	27%	56%	30%	18%	36%
Don’t know what types of security incidents occurred	28%	49%	52%	52%	39%	46%	16%

Source: The Global State of Information Security Survey®, 2008

Finding #12. Asia's security practices now on a par with those in North America

Asian companies no longer trail North American organizations in establishing leading practices in information security. Boosted by the widespread advances made principally by India and, to a lesser extent, China, Singapore and Hong Kong, Asian security capabilities are now on a par with those in North America—and in some cases exceed them.

While Asian respondents are just as likely as North American ones to say their organization has an information security strategy (64%), they are more likely to employ either a CISO or CSO (63% vs. 52%) and rely upon a centralized security information management process (55% vs. 53%), among other security benchmarks.

In protecting privacy, however, Asian companies lag behind those in North America. They're less likely, for example, to employ a Chief Privacy Officer (18% vs. 21%), require employees to complete training in privacy practices (41% vs. 54%), and conduct due diligence of third parties handling sensitive data (30% vs. 33%).

Survey results, however, strongly suggest that information security will remain a high priority for Asian organizations—at least over the near-term: almost 6 out of 10 Asian respondents expect their company will increase security spending over the next 12 months. (Figure 17)

Finding #13. Europe stalls—just as South America moves into the passing lane

Last year, Europe vied with North America in setting most of the high-water marks in security and privacy practices. This year, its relative position has slipped—nudged back less by North America's moderate capability gains in 2008 than by an apparent stall in Europe's progress.

European companies, for example, are barely more likely this year than they were in 2007 to conduct compliance testing (37% vs. 34%) and ensure the secure disposal of technology hardware (61% vs. 59%).

Some of these findings are partly due to lower survey participation this year by countries such as France and the United Kingdom and greater participation by countries such as Finland and Spain—whose companies' security capabilities, in general, are not as developed.

But in spite of these disparities in year-to-year trending comparisons, it's clear that while Europe now trails Asia and North America in many areas, South America is making great strides across many security domains—and catching up quickly.

For example, the percentage of South American respondents who say their company has an identity management strategy leapt 13 points from 25% in 2007 to match Europe's 38% this year—during which time European respondents reported only a two-point gain. (Figure 17)

Figure 17: Other responses reveal significant differences in security and privacy capabilities by region

	Asia	North America	South America	Europe
Have an overall information security strategy	64%	64%	43%	54%
Conduct enterprise risk assessment at least once a year	71%	59%	64%	57%
Will increase security spending over next 12 months	57%	39%	52%	36%
Employ a CISO or CSO	63%	52%	56%	58%
Engage both business and IT executives in addressing security	55%	62%	33%	44%
Have established security baselines for third parties	46%	45%	41%	39%
Have an identity management strategy	44%	43%	38%	38%
Conduct compliance testing	51%	48%	40%	37%
Security policies address data protection, disclosure and destruction	57%	56%	40%	44%
Have a centralized information security management capability	55%	53%	49%	46%
Encrypt databases	60%	56%	60%	47%
Use vulnerability scanning tools	58%	59%	51%	47%
Employ a CPO	18%	21%	21%	25%
Require employees to complete training in privacy practices	41%	54%	30%	28%
Conduct due diligence of third parties handling sensitive data	30%	33%	20%	22%

Source: The Global State of Information Security Survey®, 2008

What this means for your business

Insist on a risk-based, integrated, and proactive approach to safeguarding information.

Then execute it.

A risk-based, integrated approach is the best way to create a more secure and efficient (as well as compliant) organization. And for many companies, adopting one represents a clear opportunity. Survey data supports this:

- Thirty-six percent (36%) of respondents say their organization integrates security and privacy compliance plans;

- Twenty-four (24%) ensure that their security policies address classifying the business value of data;

- And while 24% report that their organization continuously—not just periodically—prioritizes data and information assets according to their risk level, 30% report that they don't classify data and information assets at all.

When undertaken correctly, a risk-based, integrated approach can help you (1) better understand the risks to your information across functions, assets, technologies and networks as well as the impacts to your business when breaches occur; (2) know which information assets are most important and where they are located; (3) allocate resources to the areas of opportunity and vulnerability that will deliver the greatest strategic business return to the organization, and (4) accelerate the transition of your organization's security, privacy and compliance functions from a reactive, "fire-fighting" posture to a proactive, enablement-savvy one.

Methodology

The Global State of Information Security 2008 is a worldwide security survey by PricewaterhouseCoopers, *CIO Magazine* and *CSO Magazine*. It was conducted online from March 25 to June 26, 2008. Readers of *CIO* and *CSO Magazines* and clients of PricewaterhouseCoopers from around the globe were invited via email to take the survey. The results discussed in this report are based on the responses of more than 7,000 CEOs, CFOs, CIOs, CSOs, vice presidents and directors of IT and information security from 119 countries. Thirty-nine percent (39%) of respondents were from North America, 27% from Europe, 17% from Asia, 15% from South America, and 2% from the Middle East and South Africa. The margin of error is ±1%.

pwc.com/giss2008

For more information, please contact:

Gary Loveland
Principal, National Security Leader
949.437.5380
gary.loveland@us.pwc.com

Mark Lobel
Principal
646.471.5731
mark.a.lobel@us.pwc.com

This publication is printed on Mohawk Options PC. It is a Forest Stewardship Council (FSC) certified stock using 100% post-consumer waste (PCW) fiber and manufactured with renewable, non-polluting, wind-generated electricity.

Recycled paper

The information contained in this document is for general guidance on matters of interest only. The application and impact of laws can vary widely based on the specific facts involved. Given the changing nature of laws, rules and regulations, there may be omissions or inaccuracies in information contained in this document. This document is provided with the understanding that the authors and publishers are not herein engaged in rendering legal, accounting, tax, or other professional advice and services. It should not be used as a substitute for consultation with professional accounting, tax, legal or other competent advisers. Before making any decision or taking any action, you should consult a PricewaterhouseCoopers professional.