Advisory Services
Security

Trial by fire*

What global executives expect of information security—in the middle of the world's worst economic downturn in thirty years.

*connectedthinking

PRICEWATERHOUSECOOPERS

Table of contents

The heart of the matter

Today, in the middle of the worst economic downturn in thirty years, information security has an enormously important role to play.

For many years, information technology—and, by extension, information security—was among the most likely cost centers to encounter cutbacks in funding when companies fell upon difficult economic times.

Why?

One reason – a lingering one, unfortunately—is that business leaders responsible for controlling "the purse strings" haven't always found it easy to link multi-year investments in security with concrete, tangible, strategy-aligned business outcomes.

A second reason, among many others, is that it's often seductively tempting for corporate decision-makers—executives under pressure to spread less funding across the same number of priorities—to find false comfort in applying cutbacks equally and indiscriminately across functions and business units until economic strength returns.

So it stands to reason—in the middle of the most significant economic downturn in decades—that the information security function might well be subject to the same waves of layoffs, project cancellations, and budget cuts that are affecting nearly every other corporate function and many different cost centers in companies, industries and regions across the world.

Is that true? To find out, we asked more than 7,200 CEOs, CFOs, CIOs, CISOs, CSOs and other executives responsible for their organization's IT and security investments in 130 countries.

We think you'll be intrigued by the results.

Two findings, in particular, stand out. On the one hand, there's compelling evidence that, in some respects, the security function appears to be "under protection"—as if the efforts of technology and security executives to better align security with the business are, in fact, beginning to show results.

On the other hand, the economic downturn has clearly "raised the bar" on security. In addition to helping the business mitigate risks associated with factors such as globalization, outsourcing and third-party compliance with the company's policies, the information security function is now also charged with new challenges—and for some companies, with more urgency than ever before. The function and its leaders are now also tasked with helping the company address an acute set of crisis-related risks and opportunities such as those associated with new business models, M&A transactions, successive waves of layoffs, a shifting regulatory landscape, cost-cutting drives in other parts of the enterprise, and major shifts in a key competitor's strategy.

What are the implications of these trends on how your business is addressing the challenges of the economic downturn? What expectations should you be placing on your information security function at this time? Which areas of focus offer the best opportunities for security to provide concrete business value—not just over the long run but right now, during an unusual economic period?

Global leaders appear to be “protecting” the information function from budget cuts—but also placing it under intensive pressure to “perform”.

I. Spending: A decline in growth rate—but a manifestly reluctant one

Finding #1
The economic downturn has shaken up the normal roster of leading drivers of information security spending—and very nearly jumped to the top of the list.

Finding #2
Not surprisingly, security spending is under pressure. Most executives are eyeing strategies to cancel, defer or downsize security-related initiatives.

Finding #3
Yet far fewer executives are actually "cutting security back". And among the half or less that are taking action, most are taking the least dramatic response.

Finding #1. The economic downturn has shaken up the normal roster of leading drivers of information security spending—and very nearly jumped to the top of the list.

The shift in pattern isn't even subtle.

Year after year, the leading drivers of information security spending remain remarkably stable. The enduring favorite among business and IT respondents to this survey—planning for business continuity and disaster recovery—tops the list every year. And so it does again this year.

The next two drivers most commonly cited are regulatory compliance and compliance with internal policies.

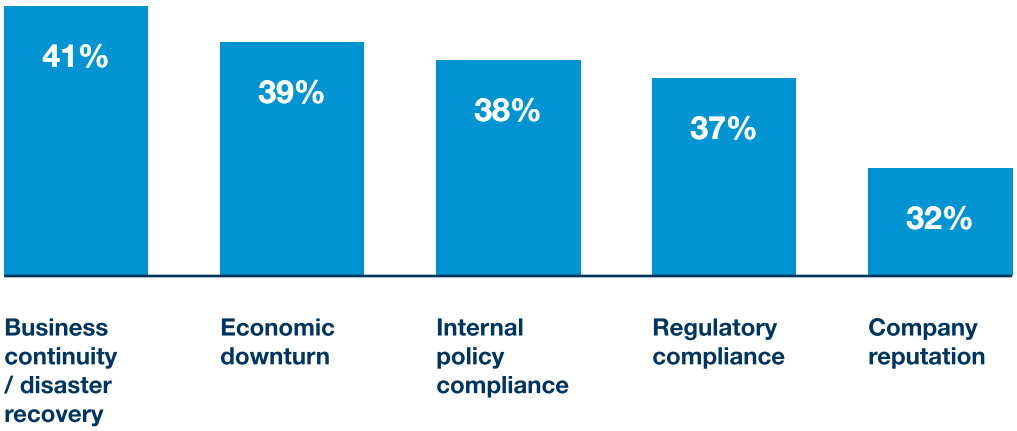
Other spending drivers—such as a wave of outsourcing activity in a given year, intensifying trends towards digital convergence, or major changes associated with mergers and acquisitions—clamber onto the executive agenda for a year or two but never really displace the priority status that business, IT and security executives ascribe to rigorously ensuring business continuity and compliance.

This year is different.

The economic downturn, as a major driver of information security spending has slammed onto the executive agenda.

The global economic crisis hasn't just elbowed its way nearly to the top of the list (it's the second leading driver this year) but it's actually considered, on average, by the more than 7,200 respondents to this survey, to be a more compelling driver of investment in information security than company reputation. (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, 2010

Finding #2. Not surprisingly, security spending is under pressure. Most executives are eyeing strategies to cancel, defer or downsize security-related initiatives.

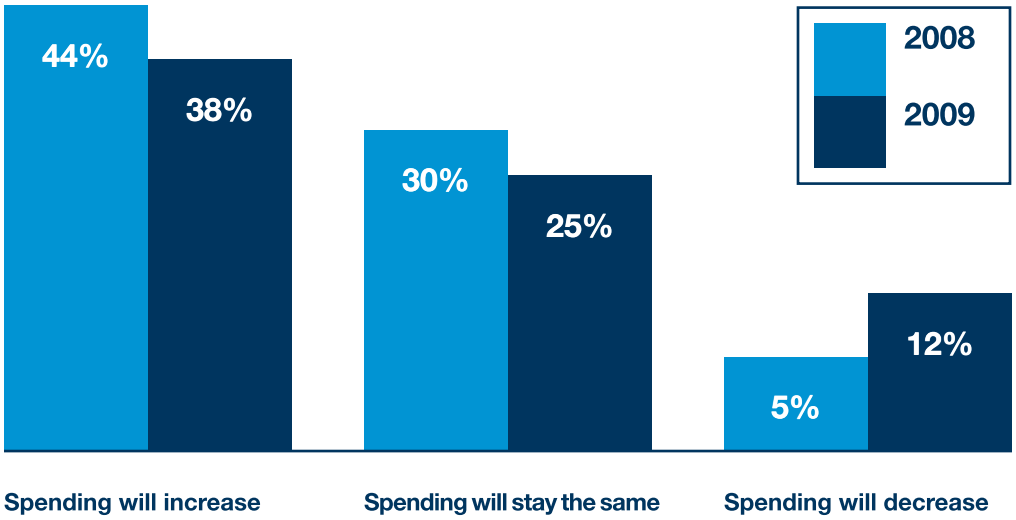
When the global economic floor drops suddenly, it's natural for executives to flinch. And so they have this year.

For the last three years—2006, 2007, and 2008—the percentage of survey respondents reporting that they expected security spending to increase has barely wavered beyond the survey's one-percent margin of error (46%, 44% and 44%, respectively). This year's responses, however, reveal a sudden and rare 6-point decline to 38% for this bellwether benchmark.

Yet what we find most interesting is that nearly two out of every three respondents (63%) expect spending to either increase or stay the same—in spite of the worst economic downturn in decades. (Figure 2)

Or, perhaps because of it.

Figure 2: Percentage of respondents reporting their expectations of their organization's security spending over the next 12 months compared to last year (2)



(2) Not all responses shown.

Source: The Global State of Information Security Survey, 2010

Finding #3. Yet far fewer executives are actually “cutting security back”. And among the half or less that are taking action, most are taking the least dramatic response.

It’s one thing to consider a strategy. It’s another to put it into action.

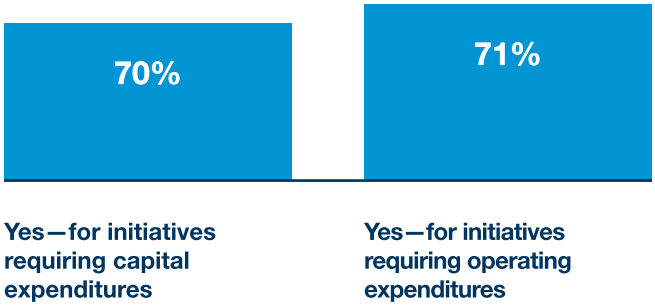
Not unpredictably, most respondents agree that to continue meeting their security objectives in the context of the current harsh economic realities, cancelling, deferring, or downsizing security-related initiatives is “important”—for initiatives requiring either capital (70%) or operating (71%) expenditures. (Figure 3)

Yet far fewer respondents report that their organizations are taking these actions—and actually reducing budgets for security initiatives requiring capital (47%) or operating (46%) expenditures. And even fewer are deferring these capital or operating outlays (43% and 40%, respectively). (Figure 4)

In fact, the half or fewer that are taking action are taking the least dramatic response—either by reducing spending by less than 10% or deferring initiatives by fewer than 6 months.

In short, it appears that some executives are reluctant to cut too deeply into security’s funding and may, to some extent, be “protecting” the security function.

Figure 3. Percentage of survey respondents who consider cancelling, deferring, or downsizing security-related initiatives to be "important"



Source: The Global State of Information Security Survey, 2010

Figure 4. Percentage of survey respondents who report that their organization is reducing budgets for security initiatives or deferring them

Has your company reduced budgets for security initiatives?	Yes	By under 10%	By 10% to 19%	By 20% or more
• For capital expenditures	47%	19%	16%	12%
• For operating expenditures	46%	19%	15%	12%

Has your company reduced budgets for security initiatives?	Yes	By less than 6 months	By 6 to 12 months	By 1 year or more
• For capital expenditures	43%	21%	14%	8%
• For operating expenditures	40%	22%	12%	6%

Source: The Global State of Information Security Survey, 2010

II. Impacts of the economic downturn: Rising pressure amid evidence of gains

Finding #4
Although given a reprieve, of sorts, from the budget knife, the information security function is under pressure to “perform”.

Finding #5
After years of “thinking differently”, business and IT leaders may be starting to think like each other.

Finding #6
Companies have made strong advances in several critical arenas over the last 12 months including strategy, assessment and compliance as well as people and organization.

Finding #4. Although given a reprieve, of sorts, from the budget knife, the information security function is under pressure to “perform”.

So what exactly has been the impact of the economic downturn on the information security function?

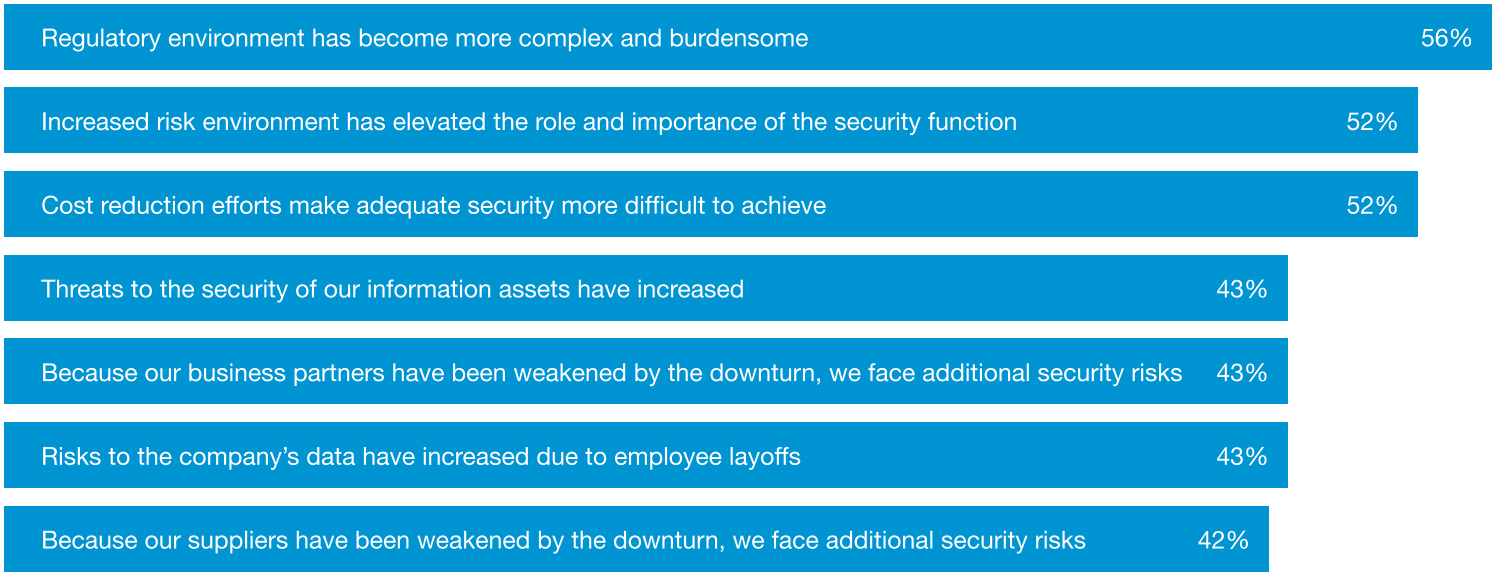
Not surprisingly, this year’s pool of survey respondents are most concerned about the regulatory environment—and the fact that it has become more complex and burdensome. (Figure 5)

They’re also concerned about cost reduction efforts that make adequate security more difficult to achieve. They believe that the threats to the security of their business assets have increased—due to employee layoffs and risks associated with business partners and suppliers weakened by the downturn.

Taken either individually or in combination, these factors—and addressing them—represents challenges that sit squarely on the security leader’s desk.

In fact, respondents report that the second greatest impact of the economic downturn is an increase in the role and importance of the information security function.

Figure 5: Percentage of survey respondents reporting impacts that the current economic downturn has had on their company's security function (3)



(3) Respondents who selected either "agree" or "strongly agree". Not all responses shown.

Source: The Global State of Information Security Survey, 2010

Finding #5. After years of “thinking differently”, business and IT leaders may be starting to think like each other.

Let’s step back a year.

Remember that last year’s survey revealed significant misalignment among business and IT decision-makers—highlighted, for example, by the difference in perspective between CISOs, who perceived a 16-point gap between security policy alignment with business objectives and security spending alignment with business objectives, and CEOs, who perceived no gap whatsoever.

What a difference a year—and a global crisis, perhaps—can make. Asked to identify the economic downturn’s impact on the security function, the security function’s leading champions, CISOs and CIOs, identified the same three leading impacts as CEOs and CFOs: (1) a more complex and burdensome regulatory environment, (2) security challenges that are harder to address in light of cost reduction initiatives, and (3) increased role and importance of the security function. That’s pretty strong evidence of a rapid convergence in perspective.

And there’s more. Asked to select from a list of seventeen possible strategies for meeting security objectives in the context of the economic downturn, the leading answer among CEOs wasn’t what one would normally expect given the list of challenges crowding CEO agendas—challenges such as risk management, governance, strategy or cost reduction. Instead, CEOs pointed to a priority often overlooked by the business in years past and frequently championed by CIOs and CISOs: increasing the focus on data protection. (Figure 6)

It was gratifying to see CISOs return the nod. What did they consider the leading strategy for addressing security objectives during the economic crisis? Their answer could have been pulled right off a memorandum from the desk of the CEO, CFO, or COO: prioritizing security investments based on risk.

It’s hard not to conclude that right now—right when the floor of the economic ship is pitching in different directions—business and IT leaders are starting to think like each other.

Figure 6: The most important strategy for meeting security objectives in the context of the current economic realities—according to senior business and IT executives (4)

	CEO	CFO	CIO	CISO
Increasing the focus on data protection	■	■		
Prioritizing security investments based on risk			■	■

(4) Respondents who selected either "agree" or "strongly agree". Not all responses shown.

Source: The Global State of Information Security Survey, 2010

Finding #6. Companies have made strong advances in several critical arenas over the last 12 months, including strategy, assessment and compliance as well as people and organization.

In spite of the economic decline, security departments have been busy advancing their capabilities over the past year—particularly in specific areas.

One of the clearest improvements has been an expansion in leadership positions—such as for Chief Information Security Officers (from 29% in 2008 to 44% this year), for Chief Security Officers (from 27% to 41%), and for Chief Privacy Officers (from 21% to 30%).

With more robust leadership also comes an improvement in planning. Nearly two out of every three respondents (65%) now report that their organization has an overall information security strategy—and nearly half (48%) point to having an identity management strategy in place.

Consistent with a steady evolution toward a more mature, well-championed, strategy-led approach to information security is evidence of gains in areas such as compliance testing (from 44% to 51%), risk assessments conducted by third parties (from 26% to 36%), integration of privacy and compliance plans (from 36% to 44%), and incident response coordination with third parties handling company data (from 27% to 35%).

Gains were revealed even in the technology arena—where last year's drumbeat of double-digit advances across virtually every key area of security technology made it unlikely that a comparable surge would occur again this year. Yet improvements in a few key technical areas are worth noting—such as automated account de-provisioning (from 27% to 38%), security event correlation software (from 35% to 43%) and even biometrics (from 19% to 30%).

Figure 7: Respondents report notable gains in areas such as strategy, assessment and compliance as well as people and organization.

	2008	2009
Employ Chief Information Security Officer	29%	44%
Employ Chief Security Officer	27%	41%
Employ Chief Privacy Officer	21%	30%
Have an overall information security strategy	59%	65%
Have an identity management strategy	41%	48%
Link security to privacy and/or regulatory compliance	44%	53%
Conduct compliance testing	44%	51%
Conduct personnel background checks	51%	60%
Conduct risk assessments via third parties	26%	36%
Use tiered authentication levels based on user risk classification	36%	42%
Integrate privacy and compliance plans	36%	44%
Have incident response process to alert third parties handling data	27%	35%
Automated account de-provisioning	27%	38%
Security event correlation software	35%	43%
Biometrics	19%	30%

Source: The Global State of Information Security Survey, 2010

III. New trends: What this year's decision-makers are thinking about

Finding #7
After years in the limelight, protecting data elements is now a top priority—arguably—at the most critical time.

Finding #8
Companies are beginning to focus acutely on the risks associated with social networking.

Finding #9
While IT asset virtualization is a growing priority, only one out of every two respondents believes that it improves information security.

Finding #7. After years in the limelight, protecting data elements is now a top priority at—arguably—the most critical time.

If improving data protection is attracting the CEO's attention as a key strategy during the downturn, isn't it likely that IT and security leaders are also addressing it as a critical priority?

They are—at least in some respects. The number of respondents, for example, who say that their organization has a data loss prevention (DLP) capability in place has leapt this year—from 29% in 2008 to 44% in 2009. And more now report that their organization continuously prioritizes data and information security assets according to their risk level. (Figure 8)

To protect data elements, however, you also have to have a clear set of guidelines about how data should be managed and safeguarded over the course of day-to-day operations. Yet fewer than half of this year's respondents (45%) report that their organization's security policies address the protection, disclosure and destruction of data. And it isn't clear, from this year's responses, whether companies have the customizable, element-specific internal controls required to protect specific classification levels of data without, in effect, having to "boil the ocean".

You also have to know where the most critical data elements lie. Yet six out of ten respondents report that their organization still does not have an accurate inventory of locations or jurisdictions where personal data for employees and customers is collected, transmitted and stored.

Figure 8: Response levels for two data protection-related capabilities

Source: The Global State of Information Security Survey, 2010

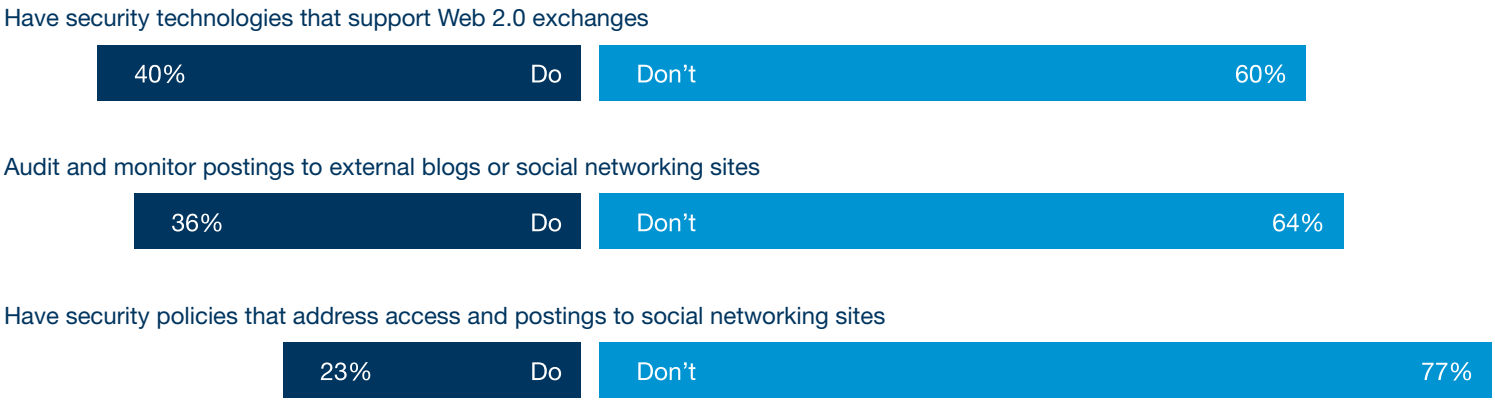
Finding #8. Companies are beginning to focus acutely on the risks associated with social networking.

Today a new generation of employees worldwide is accessing social networks from work in great numbers, often without the knowledge of the IT department—and in circumvention of the traditional countermeasures employed by many.

Some companies have moved quickly to close this gap—but most need to do more.

Four out of every ten respondents (40%) report that their organization has security technologies that support Web 2.0 exchanges, such as social networks, blogs, and wikis. In addition, approximately a third (36%) audit and monitor postings to external blogs or social networking sites and even fewer (23%) have security policies that address access and postings to social networking sites. (Figure 9)

Figure 9: Percentage of respondents who report their organization is engaging in the following security-related capabilities and practices to counter the risks associated with social networking



Source: The Global State of Information Security Survey, 2010

Finding #9. While IT asset virtualization is a growing priority, only one out of every two respondents believes that it improves information security.

IT asset virtualization may lower the costs that an IT department incurs on everything from electricity, hardware and staff support time to disaster-related expenses.

But does it improve information security?

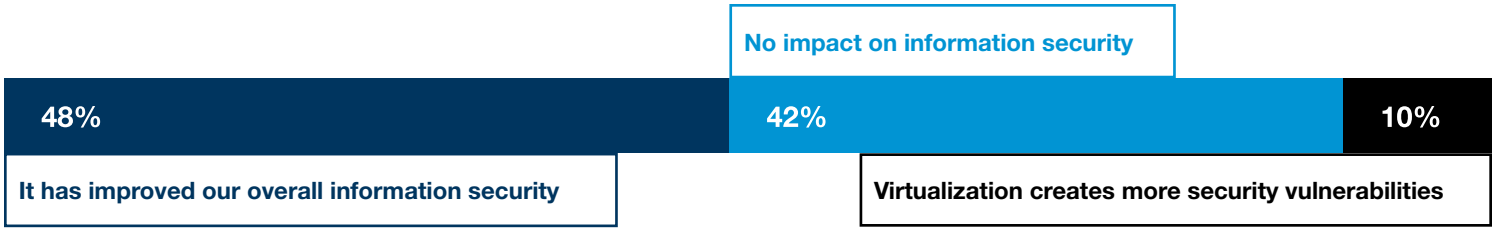
It depends who you ask. Nearly half of this year's survey respondents (48%) say that it does. But almost as many (42%) say it has no effect—and 10% insist that IT asset virtualization actually increases risk. (Figure 10)

We pressed further—and asked about the greatest security risks to a cloud computing strategy. The two most common reasons represent about half the risk: i.e., an uncertain ability to enforce security policies at a provider (23%) and inadequate training and IT auditing (22%). But the rest of the list can undermine a cloud computing initiative almost as easily. (Figure 11)

These other factors include questionable privileged access control at the provider site (14%), the uncertain ability to recover data (12%), the proximity of the company's data to that of others (11%), and the uncertain ability to audit the provider (10%).

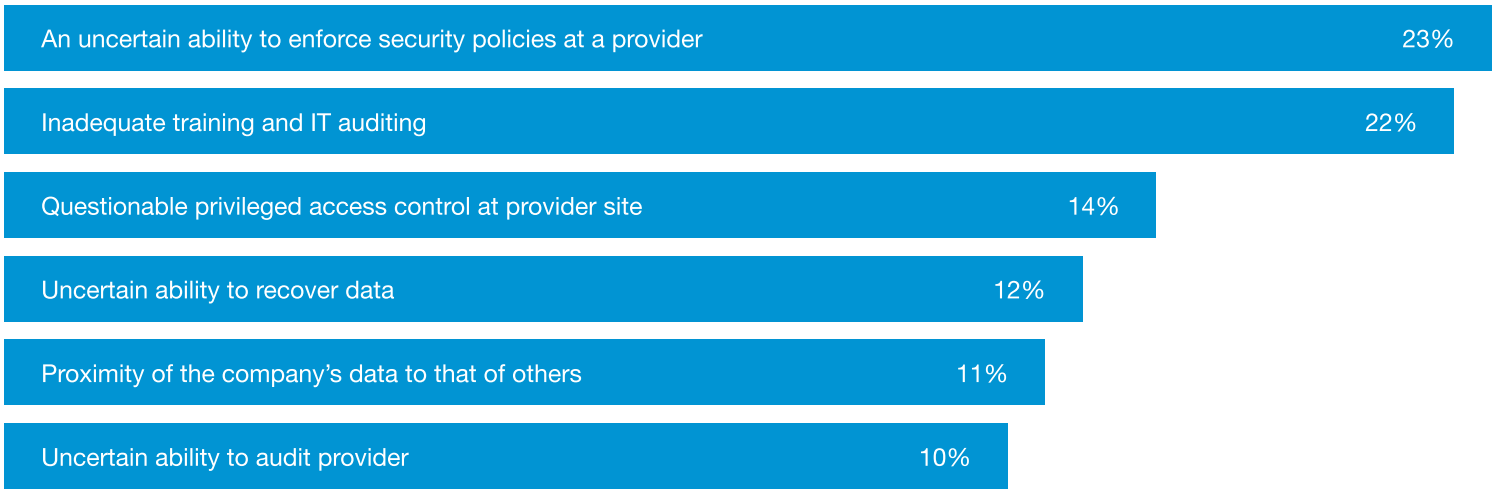
If you're at the threshold of an IT asset virtualization initiative, take a second look. Make sure you understand the risks—and are adequately prepared to mitigate, transfer or accept them.

Figure 10: Percentage of respondents responding to a survey question on the net impact virtualization has had on their organization's information security



Source: The Global State of Information Security Survey, 2010

Figure 11: Percentage of respondents responding to a survey question on the greatest risk to their organization's cloud computing strategy



Source: The Global State of Information Security Survey, 2010

IV. Global shifts South America steps out—while China takes the lead

Finding #10
With more mature security practices than any other regions of the world, North America eases up on investment—unlike Asia, which relentlessly presses ahead.

Finding #11
South America achieves major, double-digit advances in security practices—bypassing Europe at a breathless clip.

Finding #12
As China muscles its way through the economic downturn, its security capabilities have stepped nimbly ahead of India's—in a dramatic shift from last year's trend—and, in the same one-year sweep, ahead of those in the US and most of the world.

Finding #10 With more mature security practices than other regions of the world, North America eases up on investment—unlike Asia, which relentlessly presses ahead.

North American and Asian security practices are no longer on a spending par with one another, as survey responses last year indicated. On the one hand, gains in Asia—across every major security domain, from strategy and assessment to technology—have advanced very significantly over the past 12 months. On the other hand, gains in North America have advanced even further. (Figure 12)

That may change this year. Why? Because both regions are approaching security investment in the midst of the global downturn quite differently.

Take spending, for example. Asian respondents are far more likely than their North American colleagues to estimate that spending on security over the next year will either increase or stay the same (73% vs. 60%). And while decision-makers in both regions began 2009 by planning deferrals and cancellations of some security-related initiatives, those in Asia are much more likely to view these as short-term impacts over a 6-month period than their North American counterparts who believe the project and funding impacts will last for a longer period of time.

Why the difference in spending outlook? It's hard to know.

One tantalizing clue is that Asian organizations have a deeper understanding about where the threats to their assets are coming from than do North American ones. They're much more likely, for example, to know the number of security incidents occurring in the past 12 months as well as the likely source and type of the attack.

What has this better "visibility" revealed to Asian decision-makers? That attacks are more numerous than expected. And that the incidents have actually been much more successful in exploiting data and networks—rather than devices, applications and users—than Asian companies estimated last year.

This "knowledge advantage" will make it easier for some Asian organizations to take a more effective risk-based approach to security investment in the coming year—and, by extension, realize a better return on the investment for the business. On the other hand, while spending can shift, it takes years to change culture—so how the "knowledge advantage" or "disadvantage" impacts different organizations in North America and Asia needs to be taken on a company-by-company basis.

Finding #11. South America achieves major, double-digit advances in security practices – bypassing Europe at a breathless clip.

For years, South American security capabilities lagged behind those in other global regions. Last year, while Asia and North America vied for leadership, South America nudged up just behind Europe—and moved into the passing lane. This year, notwithstanding the downturn, South America has continued to post double-digit gains in many key areas—such as compliance testing (from 40% in 2008 to 53% in 2009), account deprovisioning (from 27% to 43%) and establishing security baselines for partners and customers (from 41% to 56%).

In the process, South America hasn't just left Europe behind; it has also established the global leadership position for a few capabilities that security experts consider important benchmarks of a mature security program. Two examples include conducting an enterprise risk assessment at least twice a year (43%) and prioritizing information assets according to their risk level—on a continuous basis (43%). (Figure 12)

Meanwhile, Europe trails—making gains in a few important areas, such as leadership and people-related capabilities, but "treading water" in most others.

What's behind South America's surge? Three possible reasons. First, South American respondents, like their Asian colleagues, simply know more about the number, type and source of attacks. Second—and perhaps as a result of this insight—South American respondents are far more likely than European ones to view the economic downturn as elevating the role and importance of information security (62% vs. 38%). Third, South American respondents point to "client requirement" as the leading factor used to justify security spending, an answer that contrasts with that of European respondents whose leading response was "legal or regulatory requirement".

Is the momentum behind South America's rapid advances in security likely to continue? Yes. An overwhelming number of South American respondents (80%) expect security spending to increase or stay the same over the next 12 months—a higher percentage than any other global region, and 30 points more than reported by European respondents (50%).

Figure 12: Differences in regional information security practices

	Asia	North America	South America	Europe
Security spending will increase or stay the same	73%	60%	80%	50%
Deferred security-related capital investments by less than 6 months	26%	16%	30%	18%
Deferred security-related operating expenditures by less than 6 months	26%	18%	29%	19%
Have an identity management strategy	53%	55%	42%	40%
Have established security baselines for partners and customers	46%	56%	56%	42%
Have implemented account deprovisioning	42%	39%	43%	28%
Conduct compliance testing	52%	57%	53%	39%
Conduct threat and vulnerability assessments	50%	55%	46%	39%
Encrypt laptops	57%	58%	54%	45%
Use vulnerability scanning tools	55%	59%	49%	44%
Use intrusion prevention tools	59%	62%	62%	48%
Use secure browsers	63%	68%	62%	52%
Number of security incidents in the past 12 months: Unknown	21%	41%	15%	45%
Type of security incidents: Unknown	30%	47%	21%	50%
Likely source of incidents: Unknown	32%	45%	25%	47%
Number of security incidents in past 12 months: 1-49	53%	34%	69%	31%
Type of security incidents: Data exploited	31%	17%	31%	16%
Type of security incidents: Network exploited	31%	15%	28%	15%
Conduct enterprise risk assessment at least twice a year	37%	30%	43%	28%
Continuously prioritize information assets according to their risk level	33%	31%	43%	26%
Have a centralized security information management process	55%	60%	50%	43%

Source: The Global State of Information Security Survey, 2010

Finding #12. As China muscles its way through the economic downturn, its security capabilities have stepped nimbly ahead of India's—in a dramatic shift from last year's trend—and, in the same one-year sweep, ahead of those in the US and most of the world.

Last year, one of the most dramatic and compelling highlights of this survey was the depth of India's advance across almost every security domain—many steps ahead, for example, of China's.

This year, as India pauses to catch its breath, China has raced by—with very strong double-digit gains in security-related capabilities in spite of the economic headwinds affecting so many global markets.

In fact, this year's survey results reveal that many of China's security practices, processes and technologies today represent among the world's most advanced "high water" marks in security—in areas such as employing a Chief Information Security Officer, having an identity management strategy, establishing security standards for handheld or portable devices and using security technologies to support Web 2.0 exchanges. (Figure 13)

Clearly, information security is a priority for Chinese organizations. More than eight out of every ten Chinese respondents expect information security spending to either increase or stay the same over the next 12 months—a higher score than nearly every other country in the world. Chinese respondents are also more likely than their counterparts in most other countries to view the economic downturn as having a major impact on the role and importance of the information security function (74% vs. 65% in India and 50% in the US). (Figure 14)

Why the comparatively higher emphasis in China on information security? The first answer might surprise anyone not intimately familiar with business in China: Chinese respondents are actually more concerned about the increasing complexity and burdensome challenges associated with regulation than decision-makers in other regulation-sensitive markets (72% vs. 58% in the US and 49% in Germany). And the second answer? Chinese respondents are also more concerned than those in other countries that they face "additional risks" because business partners and suppliers have been weakened by the global economic crisis.

Figure 13: This year, China has emerged as a leader in global information security practices

	India	U.S.	U.K.	Germany	Brazil	Australia	China
Employ a CISO	51%	42%	37%	28%	48%	29%	55%
Have an overall information security strategy	73%	73%	62%	50%	58%	73%	67%
Security spending will increase or stay same over next 12 months	80%	59%	49%	43%	82%	77%	86%
Conduct enterprise risk assessment at least twice a year	38%	31%	28%	26%	43%	31%	49%
Conduct active monitoring/analysis of security intelligence	70%	63%	50%	41%	55%	71%	66%
Continuously prioritize data assets according to risk level	36%	31%	31%	27%	42%	24%	41%
Have a business continuity and/or disaster recovery plan	57%	65%	47%	41%	44%	82%	50%
Have security standards for handheld/portable devices	58%	54%	44%	34%	42%	56%	61%
Have established security baselines for partners and suppliers	49%	56%	44%	39%	57%	52%	47%
Use centralized security information management process	58%	60%	45%	40%	53%	65%	60%
Use security technologies supporting Web 2.0 exchanges	49%	40%	32%	27%	49%	30%	58%
Use server, storage or other IT asset virtualization	73%	63%	52%	49%	78%	73%	83%
Have an identity management strategy	55%	55%	44%	35%	44%	50%	62%
Have an identity management solution	52%	47%	39%	30%	46%	38%	62%
Have an employee security awareness program	59%	64%	48%	36%	48%	59%	61%
Use tools to monitor user activity	57%	54%	46%	28%	48%	59%	56%
Use tools to detect intrusion	57%	67%	54%	43%	59%	71%	60%
Use tools to discover unauthorized devices	57%	58%	56%	33%	58%	55%	64%
Use biometrics	37%	26%	22%	12%	37%	16%	69%
Have accurate inventory of where sensitive data stored	42%	48%	37%	34%	29%	46%	50%
Have implemented a data loss prevention (DLP) capability	51%	50%	47%	46%	39%	34%	52%
Don't know how many incidents occurred in past 12 months	18%	41%	49%	61%	15%	27%	7%
Don't know type of security incident	29%	47%	58%	68%	18%	42%	13%
Don't know likely source of security incident	32%	45%	52%	66%	23%	39%	19%

Source: The Global State of Information Security Survey, 2010

Figure 14: Differences among country-specific perceptions of the impacts of the economic downturn on the information security function (5)

	India	U.S.	U.K.	Germany	Brazil	Australia	China
Increased risk environment has elevated the role and importance of the information security function.	65%	50%	33%	34%	62%	42%	74%
The regulatory environment has become more complex and burdensome.	57%	58%	43%	49%	59%	57%	72%
Cost reduction efforts make adequate security more difficult to achieve.	56%	53%	37%	36%	60%	53%	52%
Because our business partners have been weakened by the downturn, we face additional security risks.	46%	42%	30%	29%	53%	27%	64%
Because our suppliers have been weakened by the downturn, we face additional security risks.	44%	39%	30%	27%	52%	29%	63%
Risks to the company's data have increased due to employee layoffs.	51%	42%	30%	25%	54%	25%	53%
Threats to the security of our information assets have increased.	46%	46%	30%	28%	46%	42%	48%

(5) Respondents who answered either "agree" or "strongly agree".

Source: The Global State of Information Security Survey, 2010

What this means for your business

Take a strategic, risk-based approach. This year, the message isn’t new or different. It’s just more urgent.

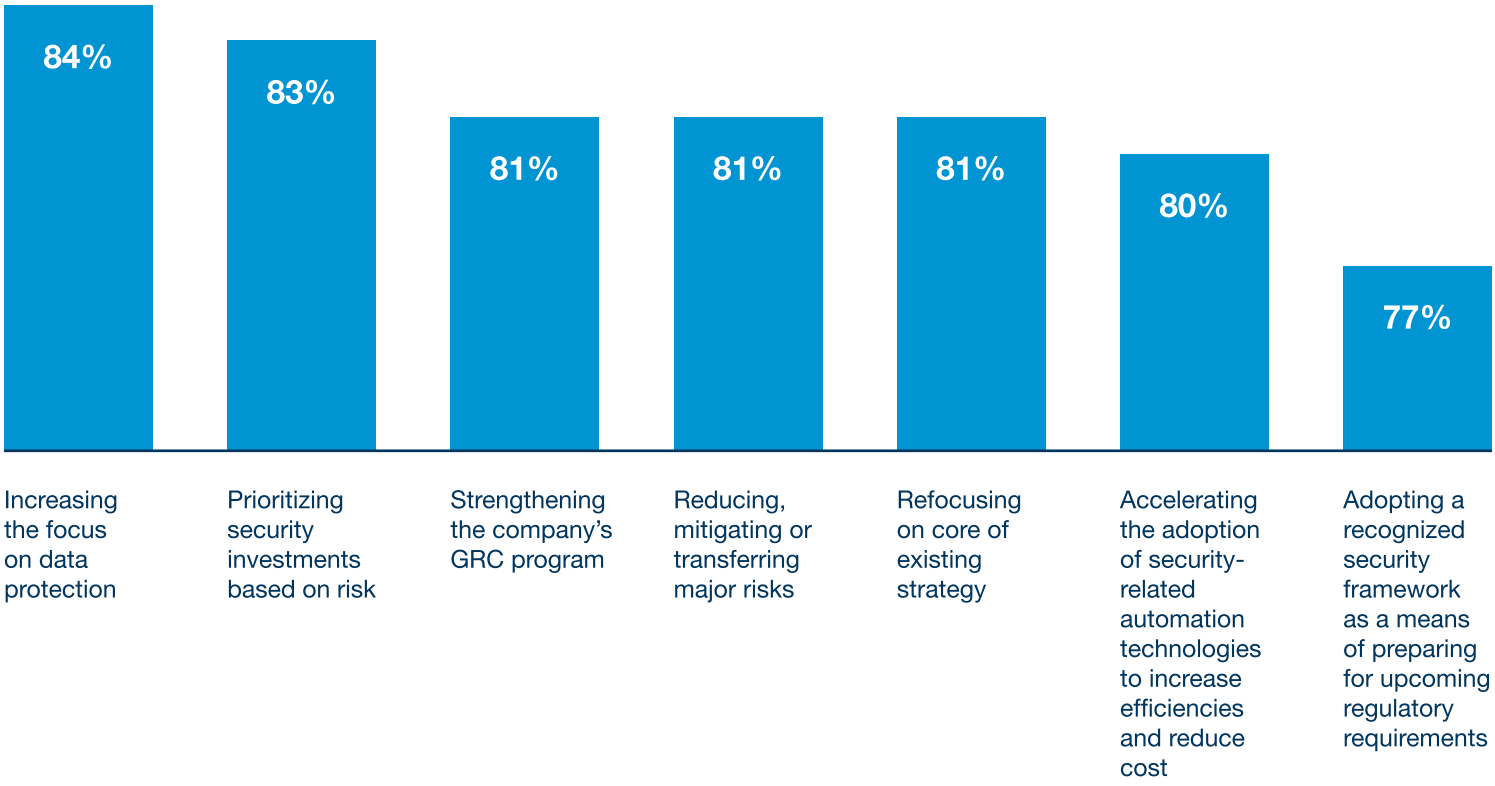
Survey results reveal that companies are looking hardest—and placing their highest expectations on – initiatives that:

- Address the “big risks” first;
- Improve data protection;
- Invest in disciplined alignment with the security strategy; and
- Increase efficiency and reduce cost.

Many companies are also considering adopting a recognized security framework as a means of preparing for an expected wave of upcoming regulatory requirements.

If this year, moving from 2009 to 2010, proves to be a trial by fire, these strategies will be enormously valuable—not just in limiting damages to assets and reputations and mitigating risks but also in positioning companies for the recovery period and stronger business performance in the years ahead.

Figure 15: Percentage of survey respondents who answered the following question: "To continue meeting your security objectives in the context of these harsher economic realities, how important are the following strategies?" (6)



[6] Respondents who answered "somewhat important", "important", "very important", or "top priority". Total does not add up to 100%.

Source The Global State of Information Security Survey, 2010

Methodology

The Global State of Information Security 2010 is a worldwide security survey by PricewaterhouseCoopers, CIO Magazine and CSO Magazine. It was conducted online from April 22 to June 15, 2009. 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 7,200 CEOs, CFOs, CIOs, CSOs, vice presidents and directors of IT and information security from 130 countries. Thirty-one percent (31%) of respondents were from North America, 27% from Asia, 26% from Europe, 14% from South America, and 2% from the Middle East and South Africa. The margin of error is ±1%.

pwc.com/giss2010

To have a deeper conversation on the topic mentioned, 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 Finch Fine Recycled. It is a Forest Stewardship Council (FSC) certified stock using 30% post-consumer waste (PCW) fiber and manufactured with renewable, non-polluting wind-generated electricity.

Recycled paper