

Retail & Consumer Insights



Respected - but still restrained

The 2011 Global State of Information Security Survey®

53%: Percentage of R&C executives surveyed who think the increased risk environment has elevated the role and importance of the information security function.

67%: Percentage who are attempting to reduce economy-related risks by focusing on data protection.

51%: Percentage of R&C executives surveyed who expect security spending to increase over the next 12 months.

46%: Percentage whose company has purchased an insurance policy that protects against theft or misuse of assets, including electronic data or customer records.

Even though they recognize the growing and continued importance of information security to their organizations and customers, retail and consumer (R&C) executives have been holding back on increasing information security investments, according to the 2011 Global State of Information Security Survey®.

With global economic conditions still in flux, these executives are walking a fine line between preserving cash and protecting the business. Restraining information security spending brings its own risks. Without continued investment, companies could see their core information security system capabilities decline at a time when the business impact of any breach is growing.

Information security has reached a critical fork in the road. Thanks to management support, many information security systems and processes continued to become fully integrated into business operations. But new risks are still emerging and information security must keep evolving to provide the necessary level of protection to the business. The survey findings provide a roadmap to next stage of information security priorities and risks.

Spending drivers: A subtle but enormously meaningful shift

The top spending drivers for security change from year to year as needs are met and as efforts are taken by organizations to stay in step with the continuously evolving threat and compliance landscape. Because information security sits in the heart of the business, the drivers of security spending often reflect the business and economic trends at a given point in time. Not surprisingly, the economic downturn is currently the leading driver of decreasing security spending, reported by 53% of companies.

It is important to note that the top four spending drivers identified in this year's survey—the economic downturn, business continuity/disaster recovery, company reputation and internal policy compliance—are all trending at four-year lows. Although these drivers have become no less important, companies tend to invest heavily to meet the most pressing needs. Then, once the resulting security becomes embedded into the

organization and core business operating processes— through newly automated systems, updated job descriptions and better internal controls—spending is often reduced. For example, business continuity and disaster recovery was a leading driver of this spending until it peaked in 2007 when 70% of companies reported it as a leading driver for security spend. Today, just 39% of R&C companies list business continuity and disaster recovery as a driver of security spending. Similarly, regulatory and industry compliance peaked as a driver at 51% of companies in 2007 following the passage of the Sarbanes Oxley Act of 2002 and the release of the PCI Data Security Standards in 2004. This year, just 36% of companies consider regulatory or industry compliance a key driver of security spending.

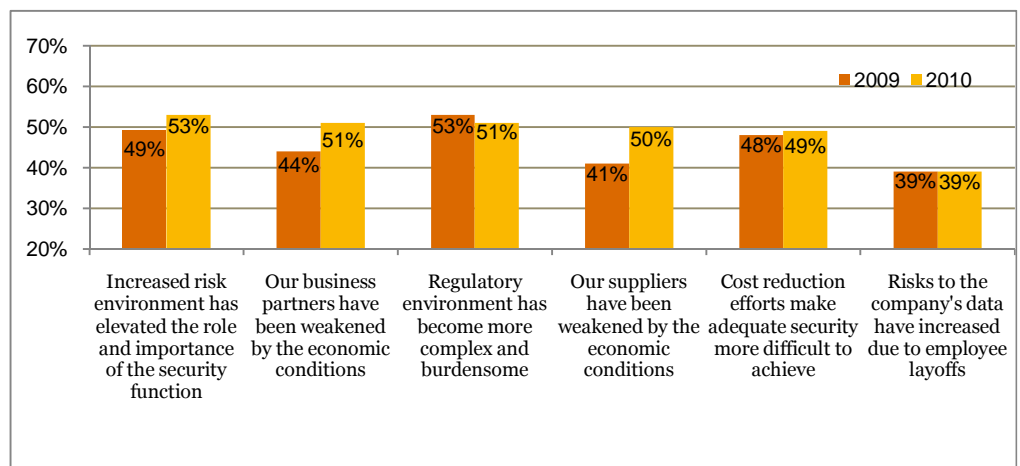
As this year's top spending drivers wane, a new spending driver—meeting client requirements—continues to emerge. Since 2007, the GISS survey has shown a steady increase in client requirements as a driver of security spending—from 20% in 2007 to 37% in 2010—as clients demand reassurance that their data will be protected. Meeting client requirements includes any specific security service or assurance that an internal or external client could require or expect before doing business with, or buying a product or service from an organization.

As client requirements take on greater importance, R&C companies are leveraging new technologies, including cloud computing, social networking, and e-commerce, to meet client needs. Companies must be prepared to integrate information security and privacy controls into these emerging technologies in order to meet internal and external compliance requirements. If this continues to grow in importance as a driver, the information security function will have an important opportunity to take on a more customer-facing, business-supporting, strategic value-building role.

Economic context: The leading impacts and strategies

The recession may be officially over but its impact continues to linger. As a result, half of the survey respondents reported that the largest increases in information security risk stem not from their own internal operations but from weaker partners and suppliers (Fig. 1). What makes this finding so significant is the fact that the respondents are functional middle managers who work closely with these partners and suppliers. These individuals are in the best position to evaluate the current state supplier and partner operations and associated risk.

Figure 1. Question: What impacts have the current economic conditions had on your company's security function?



Although R&C companies continue to make data protection one of their highest priorities, they are also trying to create efficiencies, for example, by relying on the outsourcing of security functions in the form of managed security services instead of full-time security personnel and shifting security-related responsibilities to non-security personnel. However, if these efforts are not carefully managed, this quest for efficiency and cost reduction could simply leave these companies vulnerable to new areas of risk.

Funding and budgets: A balance between caution and optimism

R&C companies must balance the need for caution in an uncertain economic climate with the need to ensure that information security controls, systems and procedures remain robust and effective. Concerned about increasing security spending, these companies are interested in funding a higher portion of security-related operating and capital expenditures from revenue streams.

The survey results point to good news in two areas. First, more companies have deferred information security spending for capital expenditures by less than six months. Second, even as companies reduce budgets, more of the companies are keeping these reductions in security spending below 10% (Fig. 2).

Figure 2.

Has your company deferred security initiatives	2009	2010	Has your company reduced budgets for security initiatives?	2009	2010
Yes, for capital expenditures	41%	43%	Yes, for capital expenditures	47%	43%
-By less than 6 months	19%	26%	- By under 10%	19%	22%
-By more than 6 months	22%	17%	- By more than 10%	28%	21%
Yes, for operating expenditures	37%	40%	Yes, for operating expenditures	44%	44%
-By less than 6 months	21%	24%	- By under 10%	20%	24%
-By more than 6 months	16%	16%	- By more than 10%	24%	20%

Overall, 51% of responding companies expect security spending to grow over the next 12 months, a significant jump compared to the 35% reporting increases in last year's survey. Indeed, absent another global economic downturn, this pent-up demand is likely to lead to an increase in security-related CAPEX and OPEX spending later this year.

Capabilities: Advances in people, decline in processes and technologies

New investments in information security could not come at a better time. After reporting consistent improvements in information security processes for several years, with funding tight, the investment in process security was either flat or declined this year (Fig. 3 & 4). However, as a counterpoint to this decline, there was a strong improvement in the number of R&C respondents who reported they have a written privacy policy in place (69% vs 54% in 2009). Furthermore, R&C respondents were also significantly more likely this year to employ dedicated security personnel and an increasing number also report employing a Chief Privacy Officer.

Figures 3 and 4. Question: What privacy and security safeguards does your organization currently have in place?

Examples of declines in process-related capabilities	2007	2008	2009	2010	One-year change
Conduct business continuity / disaster recovery planning	49%	50%	53%	41%	- 12 pts
Review privacy policy at least once a year	42%	44%	51%	42%	- 9 pts
Require third parties to comply with our privacy policies	42%	29%	46%	33%	- 9 pts
Conduct threat and vulnerability assessments	38%	44%	49%	41%	- 8 pts
Due diligence of third parties that handle personal data	n/a	22%	35%	29%	- 6 pts
Conduct penetration tests	38%	39%	39%	35%	- 4 pts

Examples of declines in technology capabilities	2007	2008	2009	2010	One-year change
Vulnerability scanning tools	42%	53%	54%	49%	- 5 pts
Network firewalls	90%	88%	76%	72%	- 4 pts
Website certification / accreditation	48%	61%	57%	53%	- 4 pts
Intrusion detection tools	54%	59%	57%	54%	- 3 pts
Personal / end user firewalls	56%	65%	63%	60%	- 3 pts

Further on the positive side, information security continues to grow in prominence in many R&C companies with more Chief Information Security Officers now reporting to the Board of Directors, Chief Financial Officer, Chief Operations Officer or legal counsel rather than reporting only to the Chief Information Officer or Chief Technology Officer. In addition, more companies are shoring up information security by adopting enterprise security management (ESM) software, having a written privacy policy in place, and using encryption for databases, file shares, laptops, backup tapes and removable media.

R&C companies need to ensure the sustainability of their information security and privacy activities. Any continued lack of focus on and investment in the long-term viability and sustainability of comprehensive information security and privacy programs could put overall security and customer confidence at risk.

Breaches: Business impacts are now too large to ignore

These efforts to enhance information security are paying off—but there is still work to be done. Although the number of companies reporting no information security breaches increased significantly from 24% last year to 31% this year, the severity and cost of the incidents that do occur has increased significantly over the past two years (Fig. 5).

The percentage of firms reporting financial losses, intellectual property theft and/or an incident with resulting brand damage have nearly doubled or more. It is this fact more than any other that is likely to increase pressure for additional information security funding as R&C companies look for ways to better protect and support the business. The fact that R&C companies continue to be targets for security breaches and compromises is another reason to maintain attention, focus and investment in information security improvements.

Figure 5. Question: What were the business impacts to your organization as a result of the incident?

Business impacts	2008	2009	2010	Two-year % change
Financial losses	11%	13%	21%	+ 91%
Intellectual property theft	6%	8%	15%	+ 150%
Brand / reputation compromised	6%	8%	13%	+ 117%

As security teams scrutinize breaches to identify the sources and impact of each incident, they are finding higher levels of exploitation in nearly every category. The percentage of incidents from insiders—current and former employees—has increased from 25% to 30% for current employees and from 18% to 24% for former employees. At least part of this increase could be attributed to dissatisfaction caused by layoffs, salary freezes and other measures taken during the recession.

The road ahead: What this means for your business

As R&C companies adapt to the current global economic environment and look for opportunities to innovate, the need for information security will only continue to increase. To deal with current and emerging innovations, such as mobile commerce, multi-channel operations and increasing enterprise mobility, R&C companies should focus on these four actions:

- **Continue to monitor expanding technologies.** Social networking by employees presents new types of risk. The growing prevalence of cloud computing services such as software-as-a-service, platform-as-a-service, or infrastructure, require R&C companies to get a strong handle on the vulnerabilities and risks associated with these technologies.
- **Prepare for multiple demands.** All of these developments have implications for information security and its place in business operations. R&C companies need to minimize the impact of information security processes and procedures on the customer experience, manage distributed devices, and keep watch on the ongoing 'data explosion' flowing among the company, its suppliers and customers—and the associated risks.
- **Focus on sustainable activities.** As business impacts rise, the pressure on CFOs to dedicate more funding to the information security function will rise as well -- not just to maintain security capabilities at their current level but also to advance security's ability to protect and support the business. As such, companies need to focus on the long-term viability and sustainability of their information security and privacy programs to ensure the effectiveness and efficiency of these programs and to make certain they protect the business, its overall security, and customer confidence.
- **Respond quickly.** No matter what, R&C companies must be prepared to respond quickly to any hint of an information security breach. However, only about one-third (35%) of responding organizations have an effective incident response plan to deal with security incidents. The other 65% either have no contingency plan or have a disaster recovery or business continuity plan that is not effective. Respondents reported that the principal reasons for these inadequacies were lack of training, incomplete plan, delay in implementation, lack of management support, and lack of partner cooperation.
- **Explore the insurance option.** Not surprisingly, nearly half of R&C companies have sought protection from these risks by purchasing insurance coverage for theft or

misuse of assets, such as electronic data or customer records. Insurance coverage is one of the fastest emerging mechanisms of defense in this area - a trend we expect will continue to rise in the coming years.

Methodology

- The 2011 Global State of Information Security Survey®, a worldwide study by PwC, CIO Magazine and CSO Magazine, was conducted online from February 19 - March 4, 2010.
- This is PwC's 13th year conducting the online survey, 8th with CIO and CSO Magazines.
- Respondents included readers of CIO and CSO Magazines and clients of PwC member firms in 135 countries.
- The survey includes more than 12,840 responses from CEOs, CFOs, CIOs, CSOs, VPs and directors of IT and security on more than 40 questions on topics related to privacy and information security safeguards and their alignment with the business.
- Thirty percent of respondents are from companies with \$500 million or more in revenue.
- R&C respondents total 1,062.

For more information on the information contained in this survey and how our professionals can assist you, please contact:

Gary Loveland, Principal and US Advisory Security Leader, gary.loveland@us.pwc.com

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

Lisa Feigen Dugal, Principal and Americas R&C Advisory Leader, lisa.feigen.dugal@us.pwc.com

Ron Kinghorn, Principal and US R&C Advisory-IT Leader, ron.kinghorn@us.pwc.com

Gerard Verweij, Principal, gerard.verweij@us.pwc.com

Pieter Penning, Director, pieter.penning@us.pwc.com

Paul Ritters, Director, paul.j.ritters@us.pwc.com

© 2010 PricewaterhouseCoopers LLP. All rights reserved. In this document, "PwC" refers to PricewaterhouseCoopers (a Delaware limited liability partnership), which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity.