

Retail & Consumer Insights



Confidence and progress

As the global economy stalls and information security threats such as cyber crime and advanced persistent threats cloud the horizon, many retail and consumer (R&C) industry executives see sunshine and clear skies overhead.

Global State of Information Security Survey® 2012

While the economic uncertainties of 2008 have largely subsided, clouds still loom over revenue, growth and margin performance. Information security challenges also remain as visibility into the next information cyber threat is poor, at best. An effective information security program is paramount; two of the most crucial drivers of information security effectiveness are having an effective strategy in place and proactively executing it. So how does the R&C industry measure up?

Despite the uncertain forecast, PwC's 2012 Global State of Information Security Survey® revealed that the vast majority of R&C executives are confident in the effectiveness of their information security practices. Overall, respondents believe they have an effective strategy in place and that their organizations are proactively executing it. This perception is likely because, in the past year, the business impacts of security incidents have declined — nearly across the board.

However, companies should be cautious not to develop an overinflated sense of safety. Security event frequency is on the rise. Strategic security processes are beginning to degrade. And companies are more likely than they were at any time in 2008 to defer or cancel the capital and operating expenditures crucial to early prevention and agile response. Combined, these conditions could develop into the perfect storm.

If 2008 was any indication, industry organizations need to ramp up their readiness efforts and give credence not just to the cyber threats of the past, but to their present vulnerabilities and potential future threats as well. Certainly, the growing incidents of cyber crime should give reason to do so quickly and strategically.

Methodology

- The 2012 Global State of Information Security Survey®, a worldwide study by PwC, CIO Magazine and CSO Magazine, was conducted online from February 10 - April 18, 2011. This is PwC's 14th year conducting the survey, and the 9th with CIO and CSO Magazines
- Respondents include readers of CIO and CSO Magazines and clients of PwC from 138 countries
- This survey includes more than 9,600 responses from COs, CFOs, 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-one percent of respondents are from companies with revenue of \$500 million or more
- R&C respondents total 996
- The margin of error is less than 1%

Confidence and progress

Organizations are taking heed to make information security an integral part of their planning, which was not as prominent in the past. In our survey of almost 1,000 industry executives, 63% reported they had information security strategies in place within their organizations. Forty percent of those would classify themselves as front-runners in information security, having both a strategy in place and taking proactive steps to execute on it, while the other 23% just have strategies in place. The remaining 37% focus more on tactics than strategy (16%) or react to issues as they arise (21%), as shown in Figure 1.

Fig. 1: "Which statement best characterizes your organization's approach to protecting information security?"



As more organizations adopt information security practices, they become more confident in their organization's security. Nearly three quarters (72%) of respondents said they are either very confident (35%) or somewhat confident (37%) that their information security practices are effective. This surge in confidence can be attributed to a new-found ability to monitor security activity. Insights into the frequency, type, and source of security breaches have leaped dramatically over the past 12 months. At least 75% of respondents could provide these details in this year's survey. Comparatively, less than half of respondents could do so in past years.

Contributing to confidence is the reduced business impact companies experience when security breaches do occur, as compared to last year. This year, survey participants indicated a decrease in financial losses, intellectual property theft, reputational or brand damage, fraud, and legal exposure.

After three years of cutting information security budgets and deferring security-related initiatives, R&C respondents are hoping for an increased focus on security. Nearly half (48%) of respondents were confident that security spending would increase anywhere from 10%–30% or more within the next year. Considering that the many vulnerabilities that emerged last year are still prevalent, companies would be wise to invest in updating their security strategies and defenses to protect themselves against new and current threats.

Signs of vulnerability and exposure

The most sophisticated, adaptive, and persistent types of cyber threats are no longer rare events. Advanced persistent threats (APT) are not just threats to the public and defense sector, they are an increasingly urgent issue for the private sector too. Nearly half (43%)

of R&C respondents said that APT concerns drive their organization's security spending. But what is most alarming is that in spite of this concern, 86% of participants revealed that their organization's security policy does not address APT, nor do they have the capabilities and tools to combat it (e.g., penetration testing, advanced network traffic analysis, and centralized security information management processes). By not taking the proper measures against APT, companies risk intellectual property and trade secret theft, and the exposure of their client's sensitive data. Figure 2 illustrates the percentage of respondents who reported the types of APT-related capabilities their organizations have in place.

Fig. 2: "What technology information security safeguards does your organization currently have in place?"

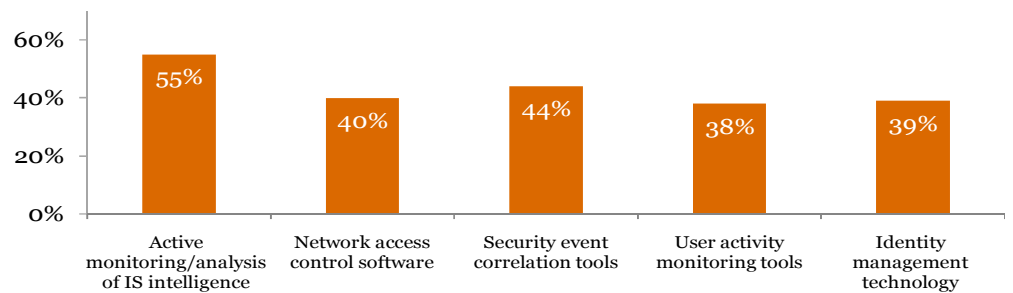


Fig. 3: Number of security incidents in the past 12 months

	'07	'08	'09	'10	'11
No incidents	25%	34%	24%	31%	33%
1 to 9 incidents	34%	28%	33%	37%	43%
10 to 49 incidents	7%	9%	6%	6%	8%
50 or more incidents	3%	2%	4%	3%	8%

Meanwhile, organizations must also contend with rising security incidents. Even though one-third of survey participants reported that they did not experience security events in the past year, reported incidents have increased across the board, as illustrated in Figure 3.

In the face of such a contentious security environment, information security leaders should have easy access to executive leadership to discuss security strategies and threats. However, survey findings reveal backtracking in this area. One-quarter of industry respondents are now saying that their chief information security officer (CISO) or equivalent executive now reports to the chief information officer. In the past, the CISO was more likely to report to the board of directors, chief executive officer, or chief financial officer. Perhaps this change in direction can be attributed to an increased confidence in current strategy resulting from the improved ability to detect and prevent security threats. However, companies need to be wary of these moves as an indicator of complacency, which is most apparent as it relates to security spending. Security spending deferrals and cutbacks, which were already high, have increased even further for both capital and operating expenditures. This year's reluctance to spend on security priorities increased or remained constant for all categories. In fact, spending appears even more restrained than it was in 2009 and 2010.

These trends are alarming, considering the growing number of security incidents and threats. As such, it is no wonder that survey respondent confidence is waning – while confidence remains high, it has declined 13 points since 2007. These numbers are telling. R&C business and IT personnel across the world are less sure that their organization is prepared to address the threats that confront their critical information.

The greatest opportunities for improvement

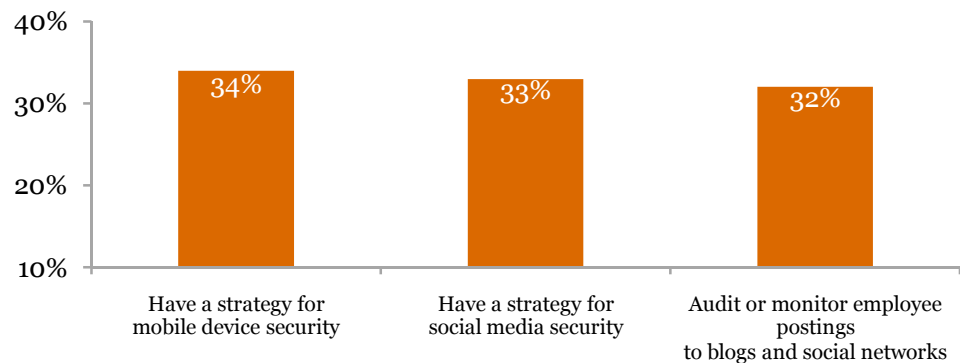
Fig. 5: What are the greatest obstacles to improving overall strategic effectiveness of your organization's information security function?

	2011
1. Insufficient capital expenditures	29%
2. Insufficient operating expenditures	24%
3. Lack of an actionable vision or understanding	24%
4. Leadership - CEO, president, board or equivalent	23%
5. Lack of an effective information security strategy	23%
6. Absence or shortage of in-house technical expertise	21%
7. Poorly integrated or overly complex information/IT systems	16%
8. Leadership - CISO, CSO, or equivalent	16%
9. Leadership - CIO or equivalent	15%

Given the austere spending environment — not just this year, but since 2008 — and a steady regression in security readiness capabilities, it's not surprising that R&C respondents consider insufficient capital and operating expenditures the leading obstacles to the effectiveness of their organization's information security function. However, what is surprising is that industry respondents point to leadership and a lack of an actionable vision for the security function as the next greatest obstacles to effectiveness (Figure 5). The latter obstacles could be overcome if the information security function and leadership worked more closely together, giving leadership a clear view of the real, menacing, and consistent threats their organizations face every day. A collaborative relationship between leadership and the CISO could catapult information security to a higher organizational priority, and in turn gain support for an actionable strategy and increased funding.

Organizations are also starting to consider the security impacts of new technologies and taking steps to protect themselves. Many R&C companies are implementing strategies to keep pace with employee use of personal electronic devices and social networking tools (Figure 6). They are also implementing controls to govern how employees can use personal technology within the enterprise. However, more than half of the industry has not yet started to put these capabilities in place.

Fig. 6: What process information security safeguards does your organization currently have in place?



Cloud computing is also gaining popularity. Thirty-five percent of R&C respondents said their organization uses cloud services. And while more than half (54%) of those respondents say that cloud computing has improved their information security, they also reveal that its leading security risk is the uncertainty surrounding their ability to enforce provider security policies. Another crucial issue challenging many R&C clients: monitoring and confirming that service providers are adhering to the client's policies and standards. These are all vital issues companies should consider and address when entering into vendor agreements.

What this means for your business

R&C companies need to regain their focus on security. It is promising that so many already have strategies in place, but it is also important to revisit and update those strategies regularly to account for new vulnerabilities and threats. As technology advances, so does the sophistication of cyber threats. Leadership must remain aware of the real and virulent attempts to penetrate their organizations, which threatens not just critical company information, but also sensitive customer data. Without this insight, leadership could develop a false sense of safety over a situation that could have serious business impacts.

Although negative business impacts resulting from security incidents are at a low, attempts to infiltrate organizations has not abated. As technology evolves, organizations must consider the implications of adopting new technologies and take precautionary steps to maintain security while advancing with the times.

Is your information security strategy up-to-date? Do you have an actionable plan to enforce your strategy? What are your organization's main threats? Do you have the proper technologies and processes in place to monitor and safeguard against those threats?

While we still face tough economic times, and budgets are tight, companies must continue to invest in security to protect valuable company assets. An investment now not only helps thwart security incidents, but also the costs and consequences that accompany them.

For full survey results,
please visit:
www.pwc.com/giss2012

To have a deeper conversation about the issues in this paper or to discuss information security and your business, please contact:

Gary Loveland, Principal, National Security Leader
(949) 437-5380
gary.loveland@us.pwc.com

Gerard Verweij, Principal
(617) 530-7015
gerard.verweij@us.pwc.com

Lisa Feigen Dugal, Principal, National R&C Industry Advisory Leader
(646) 471-6919
lisa.feigen.dugal@us.pwc.com

Ron Kinghorn, Partner, National R&C Industry Advisory-IT Leader
(617) 530-5938
ron.kinghorn@us.pwc.com

Pieter Penning, Director
(678) 419-1094
peter.penning@us.pwc.com

Paul Ritters, Director
(612) 963-6596
paul.j.ritters@us.pwc.com