Weathering the Storm

Key findings from PricewaterhouseCooper's 2012 Global State of Information Security Survey®.

When economic downturns hit, operations and IT budgets are quite often some of the first casualties, asked to fall on their swords for areas of the business perceived to be more important.

Withholding investment can impact on an organisation's capabilities to protect itself. Sacrificing IT is like sending your cavalry home at the start of a battle because hay is expensive. After all, information security threats often increase in times of economic uncertainty. So how are companies worldwide addressing information security issues now?

With a double-dip recession looking more likely, the forecast for the short-term does not look promising. Nonetheless, according to the results of the 2012 Global State of Information Security Survey®, the majority of executives are confident that their organisation is addressing and dealing with the information security threats relevant to them. They feel the appropriate strategies are in place and are being proactively managed, and it appears as a consequence of this, more organisations are able to identify the frequency and number of security breaches that they suffer. Yet, something is not quite right. Despite this confidence, some results indicate that certain security practices are in decline and the risks of third-party security breaches are on the rise.

So why are executives so confident, and where has progress been made in addressing information security threats from the prior year? What are the weaknesses and vulnerabilities that you need to be aware of and which opportunities do you need to consider preparing for the cyber threats that face your organisation?

Organisation approach

This year, we found that a very high percentage of respondents consider their organisation a 'frontrunner' in information strategy and execution. This is quite surprising and is certainly against the normal curve that we expected to see. See Figure 1.

Companies now consider they have control of the incidents that occur and this is having a knock-on effect into where their investment is being made. Not that long ago, almost half of the respondents could not answer clear questions about security-related breaches, now we find that approximately 80 percent could provide specific information on the nature and frequency of security events.

Advanced persistent threats

Whilst an Advanced Persistent Threat (APT) usually refers to a group such as a foreign state performing a long-term attack against a specific target, there is increasing evidence that organisations are becoming targets of these attacks.

Only 16 percent stated they had a policy in place to manage this threat. In addition, more than half of the responses indicated that the core strategies to mitigate this threat were not in place, such as penetration testing, identity management technology or centralised security information management processes. In fact, from the results it appears that organisations are reducing their safeguards from the prior year. See Figure 2.

Not all factors shown. Totals do not add up to 100%.

Security risks

Perhaps as a direct correlation to the economic downturn, there appears to be a worrying trend in the reduction of controls and processes to mitigate and manage information security risks. The degradation is apparent across key areas including business continuity which is fundamental to the operational effectiveness of ensuring the business as a 'going concern'. See Figure 3.

Not all factors shown. Totals do not add up to 100%.

It also appears that managing security risks related to third-parties such as vendors, partners and suppliers is getting worse and more of a challenge to the organisation.

The number of security breaches linked to customers or suppliers has risen for the third year running; however, the insider risk of current or former employees still remains the number one threat to an organisation's security.

But given the rise of the external threat what is most concerning is the apparent reduction in the efforts taken to manage the risks with these third-parties and again we see a year-on-year degradation. See Figure 4.

Not all factors shown. Totals do not add up to 100%.

Security in the cloud

On the positive side, more companies are reporting that cloud computing is improving security but report that they want better enforcement of security policies at their provider.

More than four out of ten respondents report that their organisation is using some form of cloud computing – and 54 percent report it has improved the level of information security. However, there still remain some uncertainties about the ability to audit and recover data in the cloud and how the providers enforce segregation between different organisations' data.

Global trends

For several years, it has been apparent that Asia has been investing heavily in information security. The results this year reveal just how far this region has advanced. As North American organisations continue to reduce spend and Europe's even further, Asia continues to grow and invest for the future.

Two years ago, in the middle of the crisis as much of the world froze or reduced spend on security, Asia began to invest in this critical area. There is an increased visibility of security incidents at levels unmatched elsewhere in the world. This has developed a new awareness of the value of information security with 74 percent of Asian respondents, higher than any other region in the world, agreeing that the economic downturn and the instability of the world's markets have elevated the role and importance of the security function.

The number of Asian respondents expecting security funding to increase over the next 12 months has leapt to 74 percent this year – an expectation rate far higher than any other region in the world. This indicates they are not prepared to sit back and rely on the efforts made so far. See Figure 5.

Not all factors shown. Totals do not add up to 100%.

In conclusion

The survey reveals concerning trends, security spend on the decrease, increased use of third-parties for key operational processes management, but reduced controls in place to manage them. It seems far too many of us are quite happy to

entrust management of critical business processes, tools and information to technology we don't understand or control, in the hands of poorly vetted and monitored strangers. To revert to my opening analogy, if you were Battle Field Commander, would you be content to let strangers tend to and feed your horses?

If we reflect on the context in which these results sit, we see a world where the volume of business information shared online is growing exponentially. The way we do business, drum up new business and manage our reputation, all happens online and, as such, everything to do with it is business critical. Ours is a digital way of life but Asia, it seems, is the only continent responding appropriately to the implications this has for business risk.

The 2012 Global State of Information Security Survey® is a worldwide security survey by PwC, CIO Magazine and CSO Magazine. The results are based on the responses of more than 9,600 CEOs, CFOs, CISOs, CIOs, CSOs, vice presidents and directors of IT and information security from 138 countries.

Matthew Parker is a Manager at PricewaterhouseCoopers ('PwC') in Guernsey, Channel Islands. He has nearly 20 years experience in the IT industry and specialises in IT controls, security and managing IT advisory services for PwC in the Channel Islands. Matthew is a frequent contributor to the media on information security matters and a Certified Information Security Systems Professional (CISSP), a Certified Information Systems Manager (CISM) and a Certified Ethical Hacker (CEH). Call Matthew on +44 1481 752026 or email matthew.parker@gg.pwc.com.

Figure 1

Organisational approach to Information Security

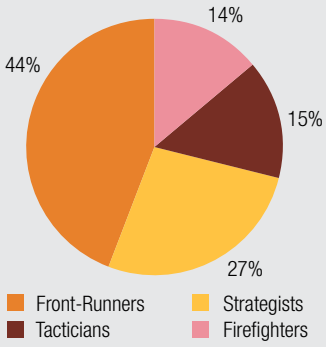


Figure 2

Percentage of respondents who report that their organisation has the following APT-related capabilities in place

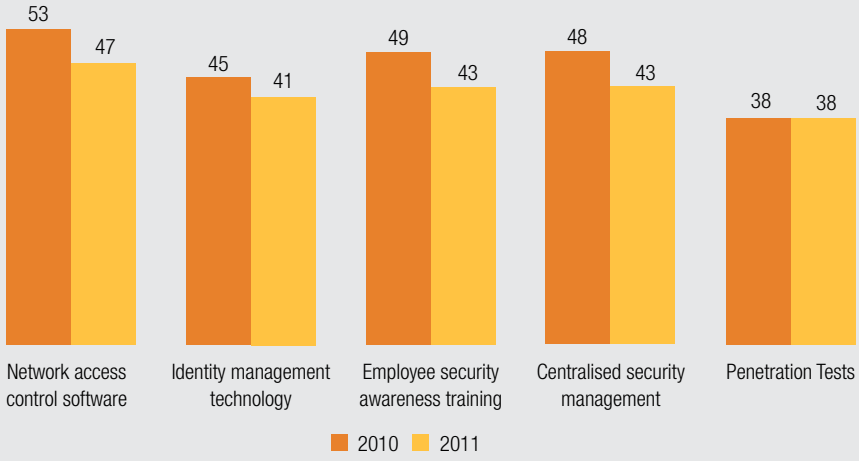


Figure 3

Percentage of respondents who report that they have Business Continuity/Disaster recover in place

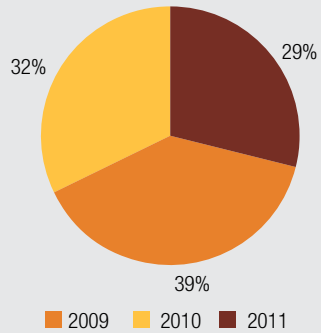


Figure 5

Percentage of respondents reporting security spending will increase over next 12 months

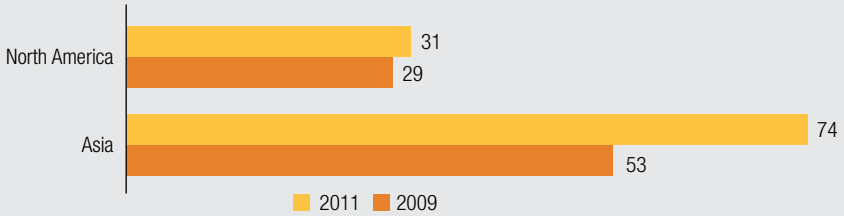
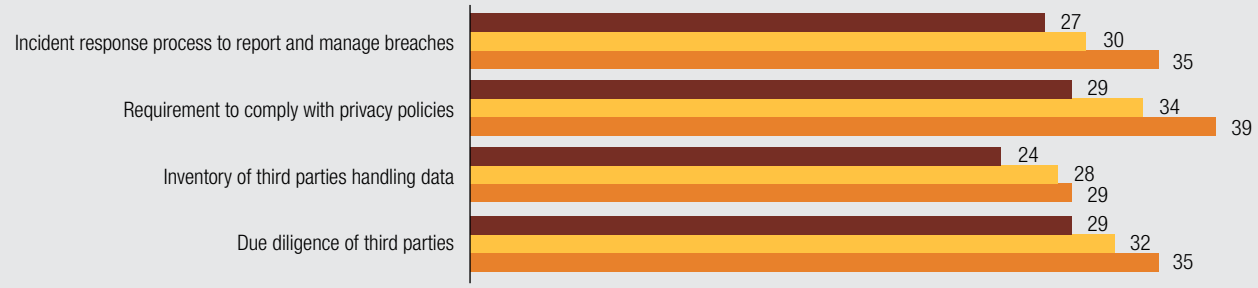


Figure 4

Percentage of respondents who report that their organisation has the following capabilities in place to counter the risks associated with third parties



Source: The 2012 Global State of Information Security Survey©