

10Minutes

on Information Security



How does your company manage today's information security risks?

Highlights

Security should be considered at the outset of new business initiatives as a way to mitigate risk.

Yet 35% of respondents in our survey say that they don't have an overall information security strategy.

Better security doesn't have to cost more. Automating management of user data and streamlining compliance can free up resources to focus on protecting critical data.

People are the key to security in a world where valuable corporate data is increasingly moving beyond a company's physical control.

Emerging technologies such as cloud computing and social media can provide benefits to your organization, but they pose new challenges in the form of information security risks.

At the same time, professional hackers are using more sophisticated techniques to try to steal valuable corporate data. One strategy involves making unwitting accomplices among employees—or employees of business partners—who allow intrusions into systems.

This *10Minutes* identifies 10 key questions to help CEOs and directors determine how well their companies manage information security risks in a hyper-connected world.

Increased adoption of technologies that connect people and organizations requires a new approach

1. Companies are embracing cloud computing, which allows them to cut costs and become more flexible and agile.¹ In the *2011 Global State of Information Security Survey* conducted by PwC, CIO magazine and CSO magazine, 49% of the 12,847 executives polled said their organizations use cloud services.
2. Employees are using their personal smart phones, computers and other mobile devices, often without the knowledge of security departments. In one study, 95% of 2,820 workers polled said they use at least one personal device for work.²
3. More employees are using social networking sites at work. In a survey of 1,600 employees in the US, UK, Germany and Japan, 24% said they visit the sites from corporate networks, up from 19% in 2008.³

1 PwC, *10Minutes on the Cloud*, June 2010.

2 Unisys *Consumerization of IT Benchmark Study*, 2010.

3 Trend Micro, *2010 Corporate End User Study*, July 2010.

At a glance

The old approach to security...

- Companies focus on securing the walls around their networks.
- Oversight of security is fragmented, leading to duplication of effort, often with inconsistent results.
- Security personnel focus on complying with company policies, even when they are outdated.
- User data are managed manually, exposing companies to human errors or allowing people who leave the company to continue to have access to some systems or applications.
- Security personnel are cautious to the point of refusing to support new business initiatives.

...versus the approach required to meet today's challenges.

- The goal is protecting valuable data wherever it resides.
- Chief information security officers (CISOs) set companywide priorities and function as trusted business advisers who weigh security risks against business needs and help companies grow.
- Benchmarking studies and other tools are used to assess the cost-effectiveness of security programs. Most companies don't need a Department-of-Defense level of security, but they do need to address the risks they face.
- Companies automate management of user data and handle compliance more efficiently, freeing up resources to focus on protecting critical data.

Where CEOs and boards should focus first

Question 1: Who is accountable for protecting our critical information?

Leading companies employ CISOs who focus on securing critical data across the organization. They ensure that security is a consideration at the outset of new business initiatives by lending security experts to business units. “If you partner with the business to meet industry needs and drive growth, they will bring you to the table to collaborate on best practices and innovative ways to address information security,” Equifax Chief Security Officer (CSO) Tony Spinelli told an industry conference this year.⁴

Organizations with CISOs also tend to lose less data than those without CISOs, according to studies and PwC’s experience working with a broad range of clients.

Question 2: How do we define our key security objectives and ensure that they remain relevant?

CEOs and boards help articulate these objectives as they pursue growth. Security can’t be an afterthought. In the power industry, for example, utilities need to incorporate security in the design of smart grids to protect all of the new points in networks where intrusions can occur.⁵

It’s also a good idea to review your overall security strategy. Weigh risks against business needs, set companywide priorities and use resources to protect data that, if lost, would cause the most damage. That can change over time as the business evolves. For example, allowing data to move beyond your company’s physical control—by outsourcing data storage, sharing inventory information with suppliers or running software on a cloud computing provider’s platform—poses new challenges.

Question 3: How do we evaluate the effectiveness of our security program?

Many firms don’t track metrics such as spending on security administration or actively monitor their logs for signs of breaches.

Leading firms that track indicators like these are able to benchmark their programs against peers. The benchmarking data along with internal assessments help them determine where to increase spending and where to cut.

Security on the radar

More and more CISOs are reporting to the CEO or the board

Percentage of CISOs who:	2007	2010
report to CEO	32%	36%
report to the board	21%	32%
report to the CIO	38%	23%

Sample: More than 12,840 CEOs, CFOs, CIOs, CSOs, and IT executives from 135 countries.

Source: PwC, 2011 Global State of Information Security Survey, September 2010.

⁴ CIO insight know it all blog, *RSA: CISOs as Entrepreneurial Business Partners*, March 4, 2010.

⁵ PwC, *Smart Grid Growing Pains*, May 2010.

Keeping the bad guys out

Unprepared for an increasingly connected world

Percentage of respondents

Don't have security policies addressing the use of social media or Web 2.0 technologies



Haven't implemented security technologies supporting Web 2.0 exchanges



0% 20% 40% 60% 80%

Sample: More than 12,840 CEOs, CFOs, CIOs, CSOs and IT executives from 135 countries.
Source: PwC, 2011 *Global State of Information Security Survey*, September 2010.

Question 4: How do we monitor our systems and prevent breaches?

Hackers were once motivated largely by ego, but they now target valuable data they can sell or use to steal money. Cases of state-sponsored espionage known as advanced persistent threats also target companies' intellectual property. Hackers' techniques have gotten more sophisticated, and they can hide evidence of attacks, going undetected for months or even years.

A study of confirmed breach cases in 2009 found that nearly 90% of victims had evidence of the breach in their log files.⁶ The companies just didn't effectively review the logs. Proactive breach analysis can find signatures of attacks, communications with external networks known to have been compromised and other suspicious activity.

Question 5: What is our plan for responding to a security breach?

An effective plan can mean the difference between a quick recovery and a serious blow to a company's reputation. Yet 63% of respondents

6 Verizon Business RISK team with US Secret Service, 2010 *Data Breach Investigations Report*, July 2010.

in PwC's 2011 *Global State of Information Security Survey* said their firms either don't have a contingency plan or have a plan that doesn't work. Independent assessments of IT operations have helped companies identify specific vulnerabilities and develop a more integrated approach to maintaining information security.⁷

Question 6: How do we train employees to view security as their responsibility?

Employees who aren't trained to think about security can disclose sensitive data on social networks or click on sites that hackers use to infiltrate corporate networks.⁸ Messages appearing to come from friends are often used to encourage employees to click.

Vigilant companies embrace social media and step up training. At Intel, which conducts security awareness training and has an internal portal devoted to security, the view is that "people are the new perimeter."⁹

7 PwC, *10Minutes on Trust and Transparency*, May 2010.

8 PwC, *Security for Social Networking*, February 2010.

9 IT World Canada, *Intel CISO: The Biggest Security Threat Today Is...*, July 7, 2010.

03

Keeping up with the pace of change in the business

Question 7: How do we take advantage of cloud computing and still protect our information assets?

As they do with all business partners, companies need to assess the ability of cloud providers to protect the confidentiality, availability and integrity of their data. They need to understand the risks related to how the cloud provider handles data from multiple clients or how it manages the third parties it uses. In contracts, they need to spell out requirements, including how providers will mitigate the risks and handle data when the contract ends. Certification or third-party audits can be required to ensure that providers do what they promise.¹⁰

A cloud model also requires changes in how companies manage user data, log activity and identify and investigate events. By centralizing the creation and removal of user accounts, for example, companies can enable an employee to use a single ID and password to access several cloud services such as email, human resources and customer relationship management applications. A well-managed central system increases security by guaranteeing that all systems are updated when employees leave or their access changes.

Question 8: Are we spending our money on the right things?

Instead of trying to lock down everything, firms can redeploy their resources to focus on protecting data that is most at risk. A recent Forrester study suggests companies may spend too much on compliance and not enough on securing corporate secrets.¹¹

Management of user data, which is handled manually at many companies, can be automated to free up resources. Automation can help reduce the vulnerability of companies to human errors inherent in manual management.

¹⁰ PwC, *Security Among the Clouds*, September 2009.

¹¹ *The Value of Corporate Secrets*, a commissioned study conducted by Forrester Consulting on behalf of Microsoft/RSA, March 2010.

Compliance and customer trust

Question 9: How can we ensure that we comply with regulatory requirements and industry standards in the most cost-effective, efficient manner?

Companies such as highly regulated financial services firms face overlapping requirements. Costs can be reduced by mapping these and conducting tests to demonstrate compliance with multiple regulations and standards. Independent evaluations can help streamline the process further.

But compliance with Sarbanes-Oxley or the Health Insurance Portability & Accountability Act doesn't mean their systems are secure. Major breaches have occurred at credit-card processors and merchants certified as compliant with Payment Card Industry standards.

Question 10: How do we meet expectations regarding data privacy?

Financial services firms and health-care providers are required by law to protect personal information about customers and patients. Some states require all businesses to do this, and most states require businesses to notify customers if their personal information is compromised. Companies also need to uphold promises they make in privacy policies; the Federal Trade Commission holds them to their word.

But firms have an opportunity to go beyond compliance and gain consumers' trust amid growing concern about the amount of electronic data companies collect, analyze and share. Smart grid operators can use privacy protection to gain credibility among customers and encourage them to participate. Online advertisers who target ads to people based on products they view could win their confidence by making it easier for people to opt out.

How PwC can help

**To have a deeper discussion about
managing information security risks,
please contact:**

Ciaran Kelly
Partner
PwC Dublin
Phone: +353 (1) 792 6408
Email: ciaran.kelly@ie.pwc.com

Kieran Mongan
Information Security Leader
PwC Dublin
Phone: +353 (1) 792 8632
Email: kieran.mongan@ie.pwc.com

Global contact:

Gary Loveland
US Security Leader
PwC
Phone: +1 949 427 5380
Email: gary.loveland@us.pwc.com

Tell us how you like 10Minutes and what topics
you would like to hear more about. Just send
an email to: 10Minutes@us.pwc.com