gyb

Growing your business™

Volume 64
2012

# *Cyber security*
# Why you can't afford to ignore it

pwc

# *Cyber security: Why you can't afford to ignore it*

Cyber criminals are increasingly targeting private companies in hopes of easy access. The cost to a business can be high, ranging from financial loss to reputational damage. With heightened awareness, private companies can fight back.

***Private businesses might not realize it, but they could be at extra risk.***

You've seen the headlines: *Hackers Steal Credit Card Data from Online Retailer. Cyber Attack Hits US Defense Contractors*. News of high-profile incidents like these inevitably rattles corporate nerves: Could that happen to us? What's our exposure? What's the IT department doing to protect us? Yet too often other issues take precedence, pushing security into the background—until a company is forced to do something about it.

That is precisely the problem, says Gary Loveland, PwC's Security practice leader: "Historically, security has been very reactive. Something bad happens and you go fix it. But that's not the best place to be."

The stakes are high: business interruption, stolen intellectual property, fraud, reputational damage, and financial loss. Private businesses might not realize it, but they could be at extra risk.

"Often midsize companies think they're under the radar and therefore don't need to worry about being a potential target," says Quentin Orr, a managing director in PwC's Security practice. "*We're secure because we're obscure* is the rationale. In fact, the opposite may be true. Midsize businesses make ideal targets. Unlike most large public companies, they tend to lack the sophisticated infrastructure to protect themselves and are not as sensitized to the threats."

Consider, for example, a fraud alert the FBI issued earlier this year. The alert warned small and midsize businesses about a new scheme: Cybercriminals were hacking into company computers, gaining access to authorized individuals' online banking logins and passwords, and then sending wire transfers to Chinese companies near the Russian border. Between March 2010 and April 2011, the FBI detected 20 such incidents. The attempted fraud amounted to $20 million, with actual losses totaling $11 million.[1]

1 http://www.ic3.gov/media/2011/ChinaWireTransferFraudAlert.pdf

*Increasingly, cyber criminals are reaching their primary targets via smaller vendors that do business with the main targets.*

Twenty incidents might not sound like a lot in the larger scheme of things, but according to PwC's *2012 Global State of Information Security Survey* (conducted in conjunction with *CIO Magazine* and *CSO Magazine*) more than 60% of US midsize businesses (those with revenue ranging from $100 million to $1 billion) said they were aware of having experienced one or more security incidents over the past 12 months.[2]

"It's not just companies in the business-to-consumer space that need to be concerned," notes Marty Janowiecki, a partner in PwC's Private Company Services practice. "Increasingly, cyber criminals are reaching their primary targets indirectly via smaller vendors that do business with the main targets. The expectation is that the data security at smaller companies may be easier to penetrate, providing a back door."

The need for greater vigilance is not lost on private companies. When recently surveyed for PwC's *Trendsetter Barometer,* leading private businesses ranked information security as their top area of planned IT investment.[3] Many of them also said they're planning investments in mobile devices and networks, social media, new data analysis tools, and cloud computing. By leveraging these technologies, private companies are finding they can do more with less, making it easier for them to compete with their better-resourced public counterparts. For those investments to pay off, however, the accompanying risks must be adequately addressed.

### *Finding the cracks in your security edifice*

Addressing the risks involves more than just installing antivirus protection. "A lot of people like to focus on the technical side of information security, but we find that it's often more about people and process," explains Loveland.

For example, on the people side, there may be issues around basic awareness of risk and policy, such as employees leaving their passwords visible (e.g., on a sticky note tacked to the wall of their cubicle) or failing to turn off their computers before going home—oversights that could be addressed with adequate companywide training. On the process side, a company might make the all-too-common mistake of installing software applications with default user names and passwords, or it may fail to roll out automated patches for its antivirus program.

Some companies enlist outside experts to assess their information security for these and other potential problems, particularly if they want to test the safety of their networks. Such experts employ "ethical hacking" to penetrate a company's network and pinpoint vulnerabilities. "We can get into a company's network nearly every time," says Loveland. "The trend we've seen is that clients have become much better about protecting themselves from the outside. But once we penetrate a client's internal network—by walking through the door in a suit and tie and then plugging into a network jack—we've always been able to get some level of access to information that the client wouldn't want a hacker to see."

2 Another 8% of respondents said they did not know if their business had experienced any security incidents.

3 *Trendsetter Barometer: Private Companies Rebuild IT Budgets*, PwC, July 2011

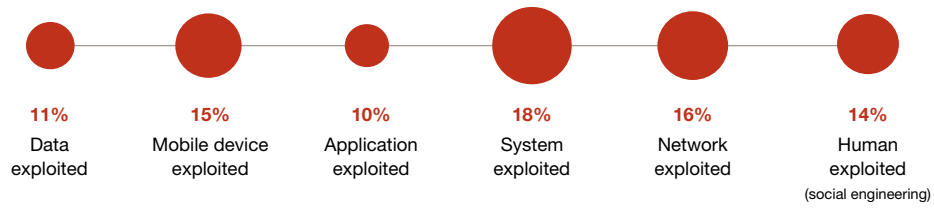
A security assessment might also reveal that the company's data defenses have not kept up with a changing IT environment. "As more businesses expand their use of smartphones and computer tablets to access internal email networks and systems, it's critical that top executives appreciate how such access dramatically increases their company's potential vulnerability," stresses Janowiecki.

Yet all too often businesses maintain the status quo rather than adequately address how novel technologies and new ways of working put the company at risk. Says Loveland, "It's like locking the main entrance of your home but then failing to put a lock on the door to your new back deck. If I'm looking to break into your house, I'm going through that unlocked door."

### *How they're getting in*

Points of access at midsize US companies

Types of security incidents experienced

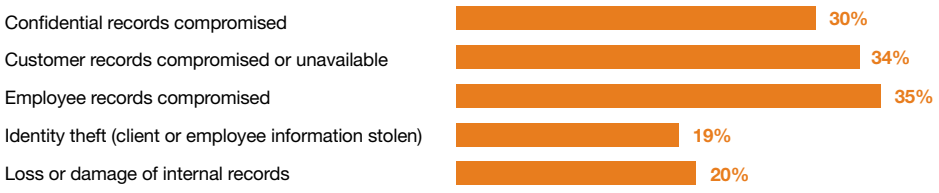



A small percentage of survey participants responded "unknown" (8%), "other" (2%), and "non-applicable" (6%).

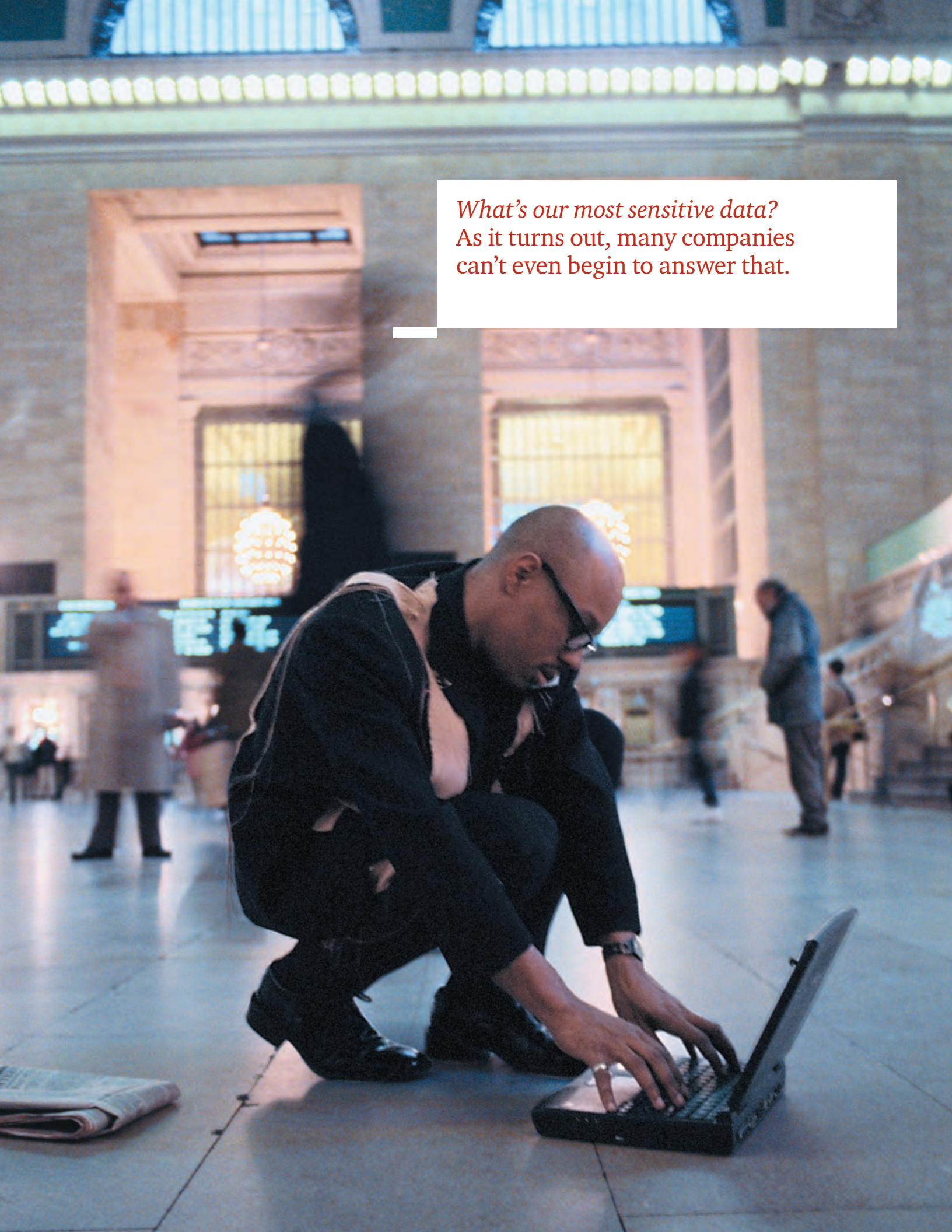
Source: *2012 Global State of Information Security Survey,* PwC, September 2011 (conducted jointly with *CIO Magazine* and *CSO Magazine*)
Midsize companies are defined here as those with $100 million to $1 billion in annual revenue.

### *What they're doing once they get in*

Data impact of security breaches at midsize US companies




Source: *2012 Global State of Information Security Survey,* PwC, September 2011



*What's our most sensitive data?* As it turns out, many companies can't even begin to answer that.

### *Taking action*

While tackling information security may seem daunting, it begins with a simple question: *What's our most sensitive data?* As it turns out, many companies can't even begin to answer that. "You've got the company's crown jewels on one side," says Orr, "and on the other side there's the information the company has a fiduciary responsibility to protect, such as data regarding customers, business partners, or employees."

Once you decide what the most sensitive data is, you have to figure out *where* it is—as well as where it's been, where it's going, how it's getting there, and why. For instance, is the information living in the organization, or is it stored elsewhere? Is it coming from outside and then being modified? When does it become special? Who's using it? How are they using it? Are they sending it to third parties? How are they sending it? Is it being sent securely?

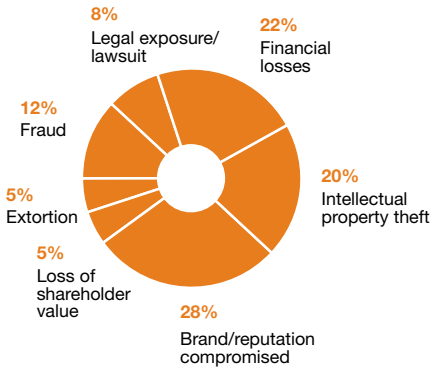
"All of these considerations have to be brought into the fold to fulfill your due diligence around managing risk associated with your company's most sensitive data," says Orr. "That's what security is all about. Everything you put in place—the security officer, policies, procedures, infrastructure, passwords—all of that is geared to protecting information."

To do that effectively, a company should have a security strategy or plan and then put someone in charge of it. "If you said that you didn't have an IT strategy to support the business, people would think you were crazy," says Orr. "You need to think about security in the same way."

That applies to private and public companies alike. However, not all private companies may find this easy to do initially. Many of them run lean IT shops, with security being just one among a number of responsibilities falling to the group. Oftentimes there is neither a chief financial officer (CIO) to elevate strategic security issues to the company's executive team nor an audit committee that could be tasked with raising questions—and seeking assurances—about a company's information security exposure.

### *The effect on your business*

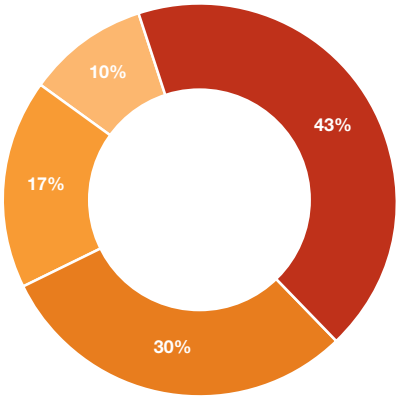
Where midsize US companies are feeling the pain




Source: *2012 Global State of Information Security Survey,* PwC, September 2011 (conducted jointly with *CIO Magazine* and *CSO Magazine*); midsize companies are defined here as those with $100 million to $1 billion in annual revenue.

### *Getting strategic about data security*

Most midsize companies have a strategy in place




**Front-runners**
We have an effective strategy in place and are proactive

**Strategists**
We are better at getting the strategy right than executing

**Tacticians**
We are better at getting things done than defining strategy

**Firefighters**
We do not have an effective strategy in place (reactive)

Source: *2012 Global State of Information Security Survey,* PwC, September 2011 (conducted jointly with *CIO Magazine* and *CSO Magazine*)
Midsize companies are defined here as those with $100 million to $1 billion in annual revenue.

# *Safeguarding technology investments*

As companies increasingly look to technology to gain a competitive advantage, they also need to be mindful of exposing the business to new information security risks. Enterprise mobility, social media, and cloud computing are among the top areas where private companies plan to invest their IT dollars over the next one to two years.* As they pursue those investments, here are some security issues they should keep in mind:

### *Cloud computing*

When businesses talk about cloud security, they first need to define what type of cloud deployment they are dealing with — public, private, or hybrid. Many of the security risks you hear about pertain to the public cloud, in which a service (and its underlying hardware and software) are shared by multiple organizations or customers.

Chief security questions: *Can the provider enforce the required security policies at its site? Is access control to the site adequately secured by the provider? Will your data be adequately segregated from that of other customers? Will the application and your company's data be available whenever you need them?*

Third-party assurance of the provider's security and controls, as well as detailed service-level agreements, can address these questions and help companies mitigate the security risks.**

### *Social media*

Given the free-flowing nature of social media, data leakage is a major security issue. Employees may post potentially sensitive information without realizing it. Phishing scams, whereby attackers try to elicit information from individuals, pose a significant threat as well.

Company networks are also at risk because hackers can easily and quickly spread malware via social networks. Just one click on a post that appears to come from a friend, and an employee might inadvertently launch a worm that infiltrates the network and puts sensitive information at risk. The best defenses? Employee education and awareness, combined with vigilant network monitoring.

### *Mobile devices*

As companies begin allowing employees to use smartphones and tablets — whether purchased by the company or via the "bring your own device" (BYOD) model — they face the challenge of managing access, usage, and security policies across different devices. A new type of software tool that manages mobile devices can ease the burden and also help protect corporate data stored on those devices. If a phone or tablet is lost or stolen, the corporate data can be erased remotely and the device locked.

**Trendsetter Barometer: Private Companies Rebuild IT Budgets,* PwC, July 2011

**For more on cloud computing and related security considerations, please see "Cloud Computing: Why It Matters to Your Business," *Growing Your Business,* vol. 62, PwC, 2011

When that's the case, a company might want to make one or more top executives responsible for overseeing IT activities or appoint members of senior management to an IT committee. Doing so would help ensure that information security threats aren't overlooked and protective measures don't languish.

"By making someone accountable for security —whether it's the chief information security officer at a Fortune 1000 company or the IT director who splits his time between security and network management—you provide a direct line of sight into potential issues," says Loveland.

This is critical, says Greg Burner, CIO of Wyle Laboratories, an aerospace and engineering services company that does a significant amount of work for the Department of Defense, including designing flight systems for the Navy and devising ways to remove air carbon from the space shuttle. He stresses the importance of involving company leadership so that they understand key IT issues and how they affect the business.

"Security-risk questions from chief executives are becoming more common as of late," observes Chip Lightfoot, a partner in PwC's Private Company Services practice. "Recent media stories reporting hacker attacks on major corporations—some resulting in costs exceeding tens of millions of dollars—are prompting executives to ask about the legal and financial implications of security breaches, particularly those involving customer data."

Because Burner works for a CFO who "gets" security, engaging leadership's attention was not as challenging for him as it has been for some of his counterparts at other companies. "Our CFO understands the issues very well and is really interested in talking about these kinds of things," says Burner. "I am pretty fortunate that I have an executive sponsor who will sit down and do that."

When developing the information security strategy for Wyle, Burner marked out a clear path: the starting point, the end point, and milestones along the way. Explains Burner, "You need to be able to document that path at a high level and get your executives to understand what each step in the path means to the company. And then you need to keep moving down that path— don't just do step one and then say that's good enough. You really have to go from start to finish."

Part of the conversation that Burner routinely has with the leadership team regards goals and expected outcomes. He stresses the importance of illustrating how the company's security investment in a particular project led to tangible risk reduction in the key areas that were identified at the project's outset: "If you can show leadership that success is measurable each step of the way, you're much more likely to keep them engaged and committed."

Along those lines, it's important that the person heading up security for the company be focused on the bigger picture of how information security aligns with the business. "Because technology touches nearly every area of a business these days, there's a growing understanding that information security has an increasingly important role to play in the financial wellbeing of a company," says Lightfoot. "This is evident in the Securities and Exchange Commission's recent disclosure guidance on cyber incidents, which although directed at public companies' disclosure considerations, sets the tone for businesses in general, including private companies."[4]

4 http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

## *M&A challenges*
## One IT security policy too many

Private companies that grow through mergers and acquisitions face the challenge of getting a handle on disparate IT security policies, processes, and systems that come with each merger or acquisition. That was the situation at Wyle, which made four major acquisitions in seven years.

"Because we grew by acquisition," explains Wyle's CIO Greg Burner, "we inherited different sets of policies and procedures for IT, including those covering information security and network security. I wanted to take a look at what we had out there and see whether there were any holes or conflicting policies, as well as possible redundancies."

His assessment helped Burner narrow down and prioritize the company's security issues. The result was that four inherited approaches to IT security were distilled into one coherent — and manageable — strategy, with tactical improvements made along the way.

## *Public profile*
## Is lax security compromising your reputation?

Beyond establishing a sound defense, there are other compelling reasons for making information security a high priority. For instance, enhanced security efforts can be a competitive differentiator for private companies if they identify the security controls they have in place and emphasize those to their customers or prospective business partners.

So far, this appears to be an area of missed opportunity for many companies: In PwC's *2012 Global State of Information Security Survey,* two-thirds of all respondents said they were not very confident or only somewhat confident in their partners' or suppliers' information security.

For private companies that are service providers, a security focus is especially important, as vendor risk management has become a pressing issue. Potential customers want to know how their information is being handled and protected, and they may ask prospective providers to field a questionnaire or specify data-handling processes in a contract. Companies that are ill prepared for such queries could jeopardize or slow down potential business deals.

As for businesses experiencing a security breach that results in the theft of confidential customer information, the reputational damage to the company could be considerable. With stakes as high as these, business leaders should ask themselves whether lax security is an option they can truly afford.

For some security departments, aligning information-protection efforts with the business overall may entail a mindset change. "Many security professionals do not behave as if they are a critical business function. Instead of discussing business risk, they discuss attack techniques and technologies," says Eric Cowperthwaite, chief security officer at Providence Health and Services, a not-for-profit healthcare provider. Cowperthwaite, one of the information security leaders interviewed by *CSO Magazine* about the *2012 Global State of Information Security Survey* results, emphasizes the importance of security leaders who think and act like leaders, rather than simply as tacticians.[5]

## *Conclusion*

Private companies are recognizing that investing in information security is about more than just protecting the business. While that is admittedly the most important objective, private-company leaders also understand that rigorous information security can better position their organization with business partners and customers, as well as enable the company to take safe advantage of newer technologies that will help grow the business. They also know that information security is just too important to relegate to the IT department alone.

Company executives are leading the charge to assess the threats, define their most sensitive data, assign accountability, devise a comprehensive strategy, and measure their progress. Shouldn't your company's leaders be doing the same?

## *More information*

Want to learn more about information security? Please contact someone on the PwC team, including:

*Marty Janowiecki*
Partner
Private Company Services
(267) 330-1588
marty.janowiecki@us.pwc.com

*Chip Lightfoot*
Partner
Private Company Services
(213) 217-3299
chip.lightfoot@us.pwc.com

*Gary Loveland*
Principal/Leader
Security Practice
(949) 437-5380
gary.loveland@us.pwc.com

*Quentin Orr*
Managing Director
Security Practice
(267) 330-2699
e.quentin.orr@us.pwc.com

5 *CSO Magazine,* "Laggard to Leader: What It Takes to Get There," October 2011, http://www.cio.com/article/691110/Laggard_to_Leader_What_it_Takes_to_Get_There?taxonomyId=3089

Moving beyond tomorrow's uncertainty and growing your business matters to you, and to us. Experience what it is like to work with professionals dedicated to serving private companies and their owners. Working with you on both day-to-day and more-complex issues such as compliance, controls, cash flow, expansion, succession, and personal financial matters — this is PwC's Private Company Services.

You talk, we listen and share insight. We are proud to serve as advisors to more than 60% of America's Largest Private Companies,[1] collaborating to help you achieve long-term success.

Experience the difference. Visit us online at pwc.com/us/pcs, email us at pcs@us.pwc.com, or call us at 800-844-4PCS to start the conversation.



1 2011 Forbes America's Largest Private Companies List