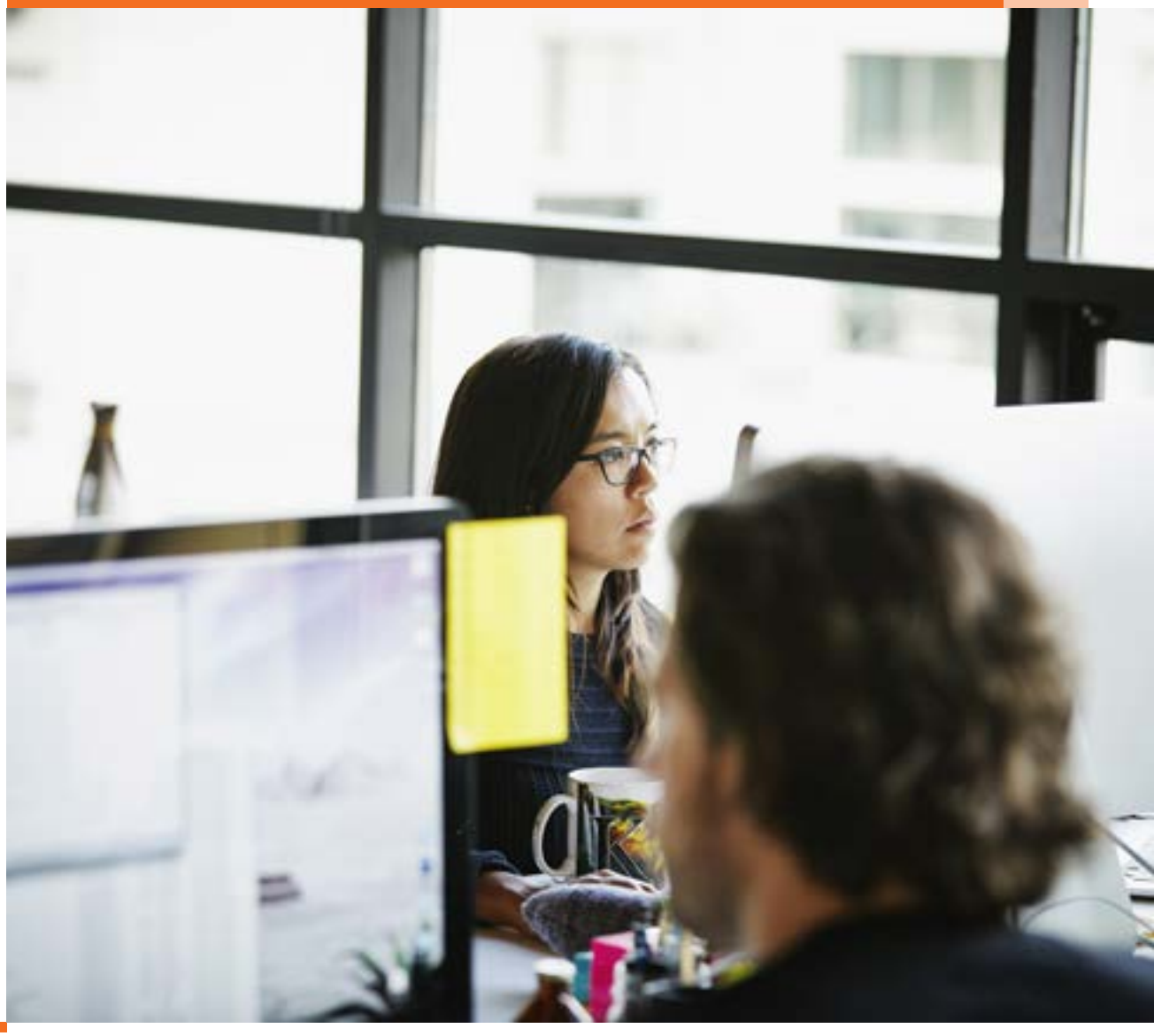
gyb

Growing your business™

Cyberattacks on the rise:
Are private companies doing enough to protect themselves?

Cybercriminals are targeting private companies in hopes of easy access. With heightened awareness, businesses can fight back.



pwc

Cyberattacks on the rise: Are private companies doing enough to protect themselves?

Cybercriminals are increasingly targeting midmarket companies and startups 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.

The headlines keep coming: *Hackers Steal Bank's Valuable Data. Big Box Store Says Millions of Credit Card Records May Have Been Snatched. US Indicts Chinese Army Officers for Hacking Industry Trade Secrets.*[1]

Cyberattacks of the past year have been rattling C-suites across the country, making executives and IT managers wonder how vulnerable their own networks might be. And the incidents are increasing. A recent global survey PwC conducted with *CIO Magazine* and *CSO Magazine* shows that the number of attacks reported by midsize companies (those with revenues of $100 million to $1 billion) has jumped 64% since a year ago.[2]

The fallout? Financial loss, disrupted business systems, regulatory penalties, and the erosion of customer confidence. A single data breach reportedly costs US companies more than $500,000 on average.[3] Corporate reputations suffer. Products are pirated. Research and development information is diverted. Designs and prototypes are stolen, as well as sensitive information about M&A plans and corporate strategy.

Regulated and large corporations tend to be more focused on these risks, as well as tend to have the budgets and personnel to constantly monitor security. But what about companies in the middle market?

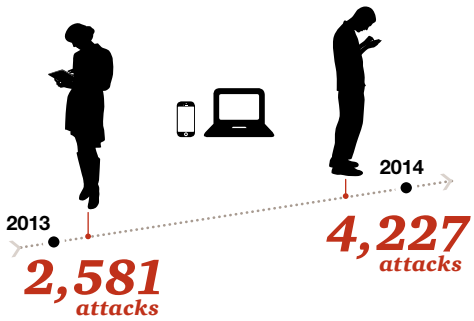
"Less regulation carries risk from a security perspective," says David Burg, PwC's global and US advisory cybersecurity leader, who notes that security considerations then have to be directed entirely by a company's own initiative.

But the rationale of an unregulated midsize company may be, *We're secure because we're obscure*. In fact, the opposite is often the case. Midsize businesses make ideal targets, often as a backdoor entrance to larger companies.

"Years ago government agencies were popular targets for threat actors," observes Laura Deaner, chief information security officer at PR Newswire. "And then it was financial services. Now it's smaller organizations that happen to have critical data. Plus there are simply more threat actors out there nowadays, and it's easier to go after the lowest hanging fruit. They see many private companies as easy targets."

Security-breach surge

Midsize companies detected dramatically more cyberattacks in 2014 than in 2013



Today's hackers are farsighted and more tenacious now when it comes to midsize companies.

The proof is in the numbers. Incidents detected by midsize US organizations in the past year have led to an estimated average financial loss of $1.8 million per company.[4] The true loss may be larger than that if the attacked business was a portal to other companies and if the number of attacks was higher than what these businesses actually detected.

Today's hackers are farsighted and more tenacious now when it comes to midsize and smaller companies, says Gary Loveland, a principal in PwC's Consumer, Industrial Products and Services group. "They might hack a high-tech startup, thinking, *When you get bought by a big company, the first thing you'll do is connect to their networks — and then, bam! I'm in*. You don't want your company to be that conduit."

So what should you do? Well, for starters, don't bury your head in the sand, says Burg. "We're beyond thinking, *Is cyber really a risk?* As one tech-company CEO famously put it, only the paranoid survive. But obviously it's not enough just to worry about security breaches. The best survival strategy for information protection is to make sure you have a cybersecurity strategy, and most companies don't."

So who are these new adversaries?

Wyle Laboratories is not among the companies without a strategy to combat this new breed of adversary. But to get the strategy right, you need to understand what the adversary wants. Greg Burner makes a point of doing just that. As the vice president and chief information officer of Wyle — an aerospace and engineering services company that is a contractor for the Department of Defense — Burner works on the front lines of digital defense. He says that in the past, hackers often were content to flaunt their ability to penetrate corporate defenses or to scout for intriguing or damaging information. They're playing for higher stakes now. Cybercriminals have grown both more sophisticated in their attacks and highly targeted in what they're going after. They're more financially motivated, too. And patient. "The amount of time and money the adversaries are putting into attacking you is the big change in recent years," says Loveland.

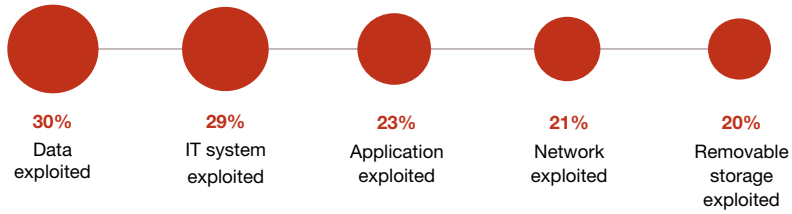
Most commonly employed software programs have known vulnerabilities, and hackers have long taken advantage of those weaknesses by running forensics on a company and using security holes to infiltrate it. What's new is that hackers are now designing highly tailored malicious software (malware) with specific company targets in mind, depositing the malware at the targeted company and then simply waiting. "They'll be successful in putting malware in a company's system but won't do anything beyond that for months," Burner says. Instead, they'll bide their time until the most valuable information shows up.

The bright side? Cyberdefense technology is getting better at detecting hackers as they enter a company's system — whereas not too long ago, the hackers generally weren't caught until they were on their way out, if intercepted at all. But too few companies are deploying these defenses; an oversight that could end up costing them dearly.

How they're getting in

Points of access at midsize US companies

Top types of security incidents experienced

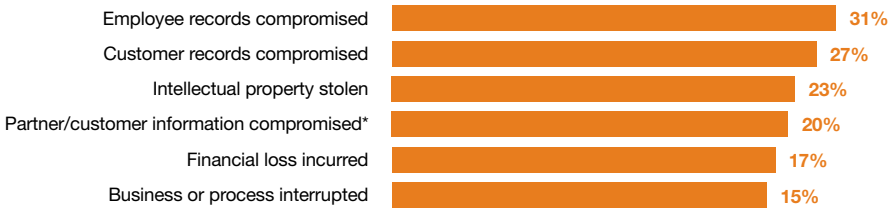


Multiple responses were allowed.

Source: *PwC, CSO magazine, CIO magazine, The Global State of Information Security® Survey 2015,* September 2014
Midsize companies are defined here as those with $100 million to $1 billion in annual revenue.

What they're doing once they get in

Where midsize companies are most feeling the pain



*Personally identifiable information

Source: *PwC, CSO magazine, CIO magazine, The Global State of Information Security® Survey 2015,* September 2014
Midsize companies are defined here as those with $100 million to $1 billion in annual revenue.

Hear no evil, see no evil: The cost of not defending yourself

"Companies need to assume a state of compromise," says Burg. "When clients hire us to do ethical hacking, we can get into their networks nearly every time." If it's a real hacker who's getting into your network, the costs can be considerable — not just in the loss of data or stolen intellectual property, but also in the interruption to business operations and the hit your company's reputation can take, possibly causing you to lose customers and clients. A breach can increase customer churn by nearly 4 percent.[5]

To avoid these losses, companies need to take a hard look at their defenses up front. Yet a big reason companies often fail to invest in cybersecurity is that they see it as discretionary spending, not a business imperative. "With profitability being top of mind, businesses tend to be more inclined to invest in growth activities than defensive measures," says Tyson Cornell, a PwC partner who works closely with private companies. But a company may in fact be hampering its growth by tabling cybersecurity. That's because, increasingly, good cybersecurity is a cost of doing business. Indeed, a full 89% of consumers say they avoid doing business with companies that they think do not protect their privacy online.[6]

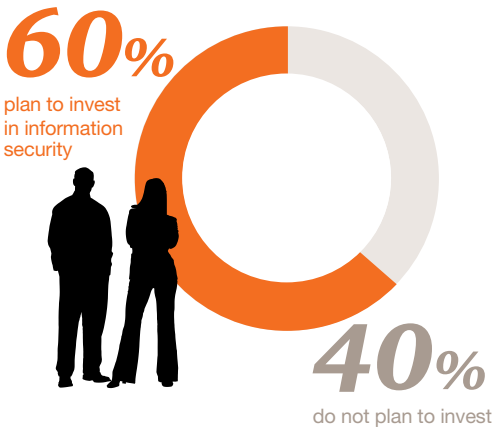
Business partners, too, want evidence that they are protected. More and more, good security has become a requirement for companies that seek to collaborate on or outsource work. Sixty percent of US companies overall have baseline standards they expect their external partners, suppliers, and vendors to meet, and nearly another one-quarter plan to establish such standards in the next 12 months. Getting the business means getting up to cybersecurity snuff.[7]

Acquisition can force a review as well. When a business performs due diligence on a target company, a security component is now part of the assessment, says Cornell: "Looking at a target company, the buyer asks, *What risk am I taking on, what would be the cost if there were a breach?*"

The demands of all of these stakeholders — consumers, partners, and purchasers — are reinforcing the importance of having a cybersecurity strategy. Leading US private companies are taking heed, with 60% of them saying they plan to invest in information security over the next couple of years.[8] The other 40% may find it difficult not to follow suit soon.

Cybersecurity vigilance

Some private companies are more invested than others



Reality check: Learn where your blind spots are

A business needn't have the equivalent of a large corporation's fulltime security team to assess and get its arms around the organization's cybersecurity weaknesses. Such an assessment is essential; without one, it's hard to forge a strategy to safeguard your assets. Here's a baseline of what every company, of any size, ought to be doing to size up its threat vulnerability.

Identify your most valuable data: Tackling information security begins with a simple question: *What's our most sensitive data?* As it turns out, many companies can't even begin to answer that. While certainly there are the company's crown jewels to guard, the data most valuable to a cyberthief might not be yours exclusively. He or she might be hacking you primarily to obtain one of your *client's* or *customer's* prize jewels. Once you've zeroed in on what's your most sensitive data (including the information you have a fiduciary responsibility to safeguard), then you can start to devise a strategy to protect that material.

Know where your prized information resides: Your most valuable data won't all be in just one place. For example, a midsize pharmaceutical company might have the formula for a new drug in a document that sits on a hard drive but that has also been shared among employees via email. So it's important to ask yourself, *Where has the information been? Where is it going? And how is it getting there?* For instance, is the information living in the organization, or is it stored elsewhere (e.g., on the cloud)? 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 (via email, a mobile device)? Is it being sent securely (does the company use email encryption)? Knowing the answers to these questions is essential if you're going to do an effective job of blocking and tackling the cybersecurity threats your organization is facing.

Understand your cyber ecosystem: It used to be that if you protected your four walls, you could keep the bad guys out. But in today's world of social, mobile, analytics, and cloud, there is now a hugely expanded ecosystem of information sharing. In PwC's recent *Trendsetter Barometer* survey of privately held companies, the majority of businesses said they plan to invest in each of these areas over the next couple of years, with the greatest number of them (nearly two-thirds of the companies surveyed) flagging cybersecurity as where they'll be putting their IT dollars.[9] To make smart use of this investment, companies should think about cybersecurity up front, rather than treat it as a bolt-on feature. Too often, though, cybersecurity ends up being an afterthought.

Embedding good security in your cyber ecosystem before you incorporate further elements simply makes good business sense, says Loveland, pointing out that "you wouldn't design a new car from top to bottom but fail to include locks. If you tried to install locks afterwards, it would be more expensive, and the car's overall design wouldn't work as well. You need to incorporate the security requirement at the outset. The same principle applies to any business."

Your cyber ecosystem
Putting security at the heart of it

Too often cybersecurity is treated as an afterthought — something to be bolted onto a new system or device. Smart companies are choosing to do just the opposite: embed security at the outset.

Fight back: The half-dozen defense tactics every company should employ

So what's the best way to go about protecting your company's information? As with any enterprise-wide initiative, it's important to set the tone at the top, making sure it resonates throughout all quarters of the organization. And then someone has to lead the charge — rally company employees and regularly update leadership. Easier said than done, but it's time and effort well spent if you want to reduce your risk of being the next cyber-attack casualty.

1. Get the C-suite involved: Many private companies run lean IT shops, with security being just one among a number of responsibilities falling to the group. And not all of them have a chief information officer (CIO). But that doesn't mean security has to slip through the cracks at those companies.

Instead, a company can have a top executive be responsible for overseeing IT activities or appoint members of senior management to an IT or security committee. Doing so would help ensure that cybersecurity threats aren't overlooked and protective measures don't languish.

"By making someone accountable for security — whether it's the CIO 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.

Getting the C-suite's buy-in and support is also critical. It's all well and good for a company to charge someone with overseeing information security, but it may end up being little more than a check-the-box approach if the appointed person doesn't actively engage the company's leaders. Actively engaging them in a clearly defined cybersecurity strategy requires focusing on the bigger picture of how information security aligns with the business. "Technology touches nearly every area of a business these days," notes Cornell. "Cybersecurity isn't just an IT issue, it's a business issue too."

Burg agrees. "One of the things that works well with the clients we advise is having the CEO say, *This is a strategic issue*." He urges CEOs to get on board the project wholeheartedly. "Don't question this. Embrace this. Make this a strategic priority so your team knows this is something to focus on not only at headquarters, but also across the portfolio."

And then once a security leader has the C-suite's buy-in and support, he or she needs to keep the leadership team updated on the company's cybersecurity goals and expected outcomes. That includes showing how the company's security investment led to tangible risk reduction in the key areas.

"It's really important for any information security leader to communicate regularly with leadership, to collaborate, and show metrics," says Deaner. "This is necessary for demonstrating that the investment in information security is important. It requires ownership by everyone."

2. Link hands across departments: Communication between departments is integral to a successful security strategy. Forty-four percent of US midsize companies have a cross-organizational team that meets regularly to discuss and coordinate information security issues.[10] Members include leaders from the IT, human resources, finance, risk, and legal departments. Unfortunately, more than half of US midsize companies have no such inter-departmental effort where cybersecurity is concerned, which makes those businesses especially vulnerable to information security breaches.

3. Raise employee awareness: While cyberattacks are growing increasingly sophisticated, the main reason for security breaches remains quite simple: lax security awareness among employees. The problems can be as basic 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 education.

Just slightly more than half of midsize US companies recognize and act on the importance of employee training when it comes to cybersecurity.[11] That leaves the other half vulnerable in this way. "Raising security awareness doesn't need to be a costly or logistically difficult undertaking," observes Cornell. "Effective use of office bulletin boards, for instance, and weekly emails to remind employees of basic security precautions can go far toward improving information protection across a company."

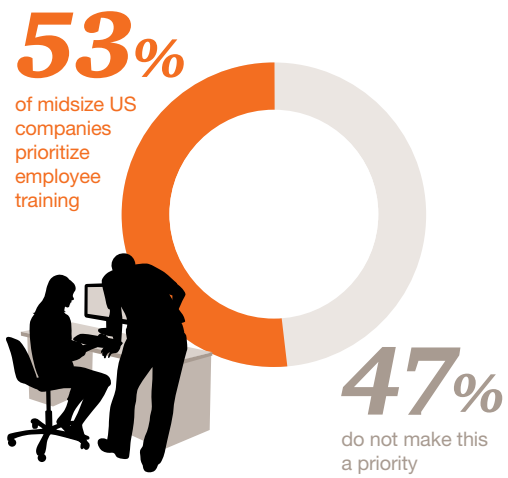
4. Do your due diligence on third-party security providers: Every question that you or a business partner would put to your own company about security standards should also be put to your third-party providers. Establish your standards up front so that you don't have to recreate a security questionnaire for each new arrangement. Spell out the security you want, make sure it's specified in the provider's fine print, and then check that it's actually being done.

5. Use the latest security protection to its fullest: Websense-type anti-spam systems can screen for vulnerable or malicious URLs, or better yet create a whitelist of websites that your employees may safely access. But these measures work best when they are kept up to date. Companies are often inclined to wait to push out new security patches during a slow week or over the weekend, but it's best to push them out as soon as soon they become available.

6. Have a crisis response ready: Every company should devise a plan for how to take immediate action if a security breach were to happen. Once a plan has been created, you should run an incident-response exercise with key members of your security team, as well as with your employees overall. Ask yourselves, *What actions should employees take to pinpoint and then mitigate the damage? Who should you contact in law enforcement? How should you go about informing all the stakeholders? Who should speak to the media, and what should they divulge?* Companies that don't scenario-plan for eventualities like these may end up looking like deer in the headlights, making a bad situation worse. Crisis-readiness can help ensure that won't happen.

Employee vigilance

Only half of midsize companies make this a cybersecurity priority



New, affordable technologies are offering stronger protections so that you can detect intruders sooner.

The good news

While tackling cyberthreats might seem daunting to many midsize private companies, it's hardly a doom-and-gloom scenario. Here are several encouraging things to bear in mind as you brace yourself for battle with cybercriminals:

You are lithe.
You might not have the big budget and staffing of larger corporations to fight cybercrime, but you can be agile in implementing a strategy (having less bureaucratic red tape to cut through) — key to battling a fast-evolving adversary.

The cost needn't be overwhelming.
New, affordable technologies are offering stronger protections so that you can detect intruders sooner — at the gate as they come in, rather than as they slip out (the difference between realizing there's been a breach and actually preventing one).

New cybersecurity innovations may deter attackers.
Private-sector efforts are afoot to identify and circumvent zero-day threats (unknown and unpatched code flaws) before hackers can exploit them. This could ultimately make cybercrime less lucrative by forcing hackers to invest more in technology and attack-process capabilities. Some hackers might end up deciding it just isn't worth it.

Hackers are human, too.
If one of the biggest worries from the defensive posture is human error, the good news is that the adversaries share the same frailty. They slip up, just like the rest of us, which makes catching them in the act far from impossible, as long as you have the right protections in place.

Conclusion

Leading private companies recognize that investing in information security is about more than just protecting the business. While that is admittedly the most important objective, strong cybersecurity can also better position an organization with its business partners and customers — not to mention let the company take safe advantage of newer technologies to help grow the business. So if you don't have a cybersecurity strategy, now's the time to start thinking about one. And not a moment too soon.

Endnotes

1 http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

2 *PwC, CSO magazine, CIO magazine, The Global State of Information Security® Survey 2015,* September 2014

3 *10Minutes on Data Privacy,* PwC, 2014

4 *PwC, CSO magazine, CIO magazine, The Global State of Information Security® Survey 2015,* September 2014 (reported losses ranged from "less than $10 thousand" to "$10 million to $19.9 million")

5 *10Minutes on Data Privacy,* PwC, 2014

6 Ibid

7 *PwC, CSO magazine, CIO magazine, The Global State of Information Security® Survey 2015,* September 2014

8 *Trendsetter Barometer,* PwC, 2014

9 Ibid

10 *PwC, CSO magazine, CIO magazine, The Global State of Information Security® Survey 2015,* September 2014

11 Ibid

More information

Want to learn more about cybersecurity? Please contact someone on the PwC team, including one of the following individuals:

David Burg
Leader
Global and US Advisory Cybersecurity
david.b.burg@pwc.com

Gary Loveland
Principal
Consumer, Industrial Products & Services
gary.loveland@pwc.com

Tyson Cornell
Advisory Partner
Private Company Services
tyson.cornell@pwc.com

GYB is published by PwC's Private Company Services (PCS) practice. Here we discuss the challenges privately owned businesses face and where the opportunities lie, suggesting how you can effectively make the most of both.

Please visit the *GYB* website at www.pwc.com/gyb for archives and local contacts. Contact our editor at gybeditor@us.pwc.com.

Located in all major U.S. markets, PwC's Private Company Services (PCS) is a national practice with more than 170 partners who provide tax, audit and advisory services especially for private companies, their owners and high net worth individuals. More than 60 percent of America's largest private companies are PCS clients.* They span a broad range of sectors and industries, from manufacturing to retail, and industrial to professional services.

A hallmark of PCS is thought leadership to give clients timely, thought-provoking information to help manage and grow their businesses and wealth.

Visit us online at pwc.com/us/pcs

MW-15-0397

* Forbes America's Largest Private Companies 2013